Andmejälgija turvaanalüüs  
Lisa 1 – ohud ja meetmed

X-tee andmejälgija analüüs ja disain

Versioon 1.0, 20.12.2015

Tellija: Riigi Infosüsteemi Amet

Täitja: Degeetia OÜ, Mindstone OÜ ja FocusIT OÜ



# Dokumendi ajalugu

|  |  |  |  |
| --- | --- | --- | --- |
| Versioon | Kuupäev | Autor | Märkused |
| 1.0 | 20.12.2015 | Janek Part | Esimene versioon |
|  |  |  |  |
|  |  |  |  |

# Sisukord

[1 Dokumendi ajalugu 2](#_Toc437897191)

[2 Sisukord 2](#_Toc437897192)

[3 Sissejuhatus 2](#_Toc437897193)

[4 Turvaserverist väljas oleva proxy variant 2](#_Toc437897194)

[5 Turvaserveri sees oleva proxy variant 27](#_Toc437897195)

# Sissejuhatus

Käesolev dokument sisaldab andmejälgijaga lisanduvate täiendavate ISKE tüüpmoodulite kohaste ohtude ja meetmete detailset loendit. Vaadeldud on kahte varianti – turvaserverist väljas oleva *proxy* varianti ja turvaserveri sees oleva *proxy* varianti. Turvaserveri sees oleva *proxy* variandis pole juba lahtikirjutatud meetmeid korratud, vaid on välja toodud aspektid, mille osas ta erineb turvaserverist väljas oleva proxy variandist.

Lisaks ISKE standardsete ohtude ja meetmete pealkirjadele on võtmeküsimustes lisatud ka kommentaare, millisest tahust või eripärast lähtuvalt tuleb andmejälgijas selle ohu mõju silmas pidada või millise eripäraga tuleb selle meetme rakendamisel arvestada.

# Turvaserverist väljas oleva proxy variant

Selle variandi korral eeldame nii ohtude kui ka turvameetmete spetsifitseerimisel, et andmejälgija asub samas füüsilise turbe keskkonnas kus turvaservergi. Täpsemalt – andmejälgija füüsilist turvet kajastavaid ohtusid ja meetmeid ei ole vaadeldud, kuna need on vaatluse all turvaserveri eksistentsi tõttu ja ei vaja täiendavat lahendamist andmejälgija projektis.

**Asjakohased ISKE moodulid**

* **B 1.3. Hädaolukorraks valmisoleku kontseptsioon** – mõned ohud ja meetmed, mis puudutavad andmejälgija taastet ja selle eritingimusi, enamik N/A
* **B 1.8 Turvaintsidentide käsitlus** – mõned spetsiifilised ohud ja meetmed, mis puudutavad andmejälgija turvaintsidente, enamik N/A
* **B 1.9 Riist- ja tarkvara haldus** - ohud ja meetmed peaaegu täies mahus (arvestades lahenduse spetsiifikat mõned ohud ja meetmed N/A)
* **B 1.14 Turvapaikade ja muudatuste haldus** - ohud ja meetmed täies mahus
* **B 3.101 Server**
* **B 3.304 Virtualiseerimine**
* **B 5.4 Veebiserver** - ohud ja meetmed peaaegu täies mahus (kuna andmejälgijal toimib veebirakendus)
* **B 5.7 Andmebaasid** - ohud ja meetmed peaaegu täies mahus (v.a. krüpteerimine, mis lisandub suuresti alles H-tasemel)
* **B 5.21 Veebirakendused** - ohud ja meetmed täies mahus
* **B 5.22 Logimine** - ohud ja meetmed täies mahus
* **B 5.E2 ID-kaart/PKI** - ohud ja meetmed, mis puudutavad EID vahendiga sisselogimist, muud jäävad välja

Toodud nimekirjale lisandub krüptokontseptsiooni tüüpmoodulist B 1.7 meede M 4.86, mida rakendatakse andmejälgija korral eritingimustel.

**B 1.3 Hädaolukorraks valmisoleku kontseptsioon**

**Ohud**

* **G 1.2 IT-süsteemi avarii.** Tuleb arvestada andmejälgija võimalike riketega.

Ülejäänud mooduli B 1.3 ohud on andmejälgija vaates N/A.

**Meetmed**

* **M 6.114 (L) Hädaolukorraks valmisoleku kontseptsiooni koostamine.** Kontseptsioonis tuleb arvestada mh. ka andmejälgija rikkeid.
* **M 6.115 (L) Kaastöötajate integreerimine hädaolukorra haldusprotsessi.** Töötajatele tuleb kohustuseks panna mh.ka andmejälgija võimalike riketega seonduvaid kohustusi.
* **M 6.117 (M) Testid ja valmisoleku harjutused.** Peavad hõlmama ka andmejälgija hädaolukordi.
* **M 6.118 (L) Hädaolukorra meetmete kontroll ja käigushoidmine.** Peavad hõlmama ka andmejälgija hädaolukordi. Andmejälgijast hakkab sõltuma turvaserveri töö.

Ülejäänud mooduli B 1.3 meetmed on andmejälgija vaates N/A.

**B 1.8 Turvaintsidentide käsitlus**

**Ohud**

* **G 2.62 Turvaintsidentide puudulik käsitlus.** Tuleb arvestada, et andmejälgijaga seotud turvaintsidendid on spetsiifilised. Eriti tuleks rõhk panna juhtumitele, kus keegi modifitseerib kuritahtlikult andmejälgija konfiguratsiooni, nii et jõustruktuuride poolt tehtud andmepäringud ja neis sisalduv teave jõuavad isikutele, kelleni need ei tohiks jõuda

**Meetmed**

* **M 6.62 (M) Prioriteetide kindlaksmääramine turvaintsidentide käsitlemiseks.** Prioriteetide kindlaksmääramisel tuleb arvestada ka andmejälgija turvaintsidente.
* **M 6.121 (L) Suuniste väljatöötamine turvaintsidentide käsitlemiseks.** Suuniste koostamisel tuleb mh. lähtuda ka andmejälgija võimalikest turvaintsidentidest. Tuleb arvestada juhtumitega, kus keegi modifitseerib kuritahtlikult andmejälgija konfiguratsiooni, nii et jõustruktuuride poolt tehtud andmepäringud ja neis sisalduv teave jõuavad isikutele, kelleni need ei tohiks jõuda**.** Eriline rõhk tasub panna sisemistele intsidentidele, kus asutuse töötajad kasutavad andmekogu andmeid vääriti ja kasutavad saadud infot oma hüvedest lähtuvalt või uudishimu rahuldamiseks.
* **M 6.67 (M) Turvaintsidentide avastamismeetmete rakendamine.** Tuleb rakendada ka andmejälgija korral. Peamine rõhk tuleb panna andmejälgija konfiguratsioonifaili volitamata muutmise avastamisele – selle korral peaks peaadministraator (või peakasutaja) saama vastava meili, milles on vana konfiguratsioonifaili räsi ja uue, muudetud konfiguratsioonifaili räsi.
* **M 6.123 (M) Ekspertmeeskonna moodustamine turvaintsidentide käsitlemiseks.** Ekspertmeeskond peab tundma muuhulgas andmejälgija spetsiifikat, kui asi puudutab andmejälgija turvaintsidente.
* **M 6.130 (L) Turvaintsidentide äratundmine ja mõistmine.** Turvaintsidentide hindamisel tuleb arvestada muuhulgas andmejälgija spetsiifikat.

Ülejäänud mooduli B 1.8 meetmed on andmejälgija vaates N/A.

**B 1.9 Riist- ja tarkvara haldus**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Vääramatu jõud**

* **G 1.1 Personali väljalangemine**
* **G 1.2 IT-süsteemi avarii**
* **G 1.4 Kahjutuli.** Andmejälgija vaates N/A, kuna andmejälgijat hoitakse eeldatavalt samas ruumis turvaserveriga, mille füüsiline turve on tagatud juba enne andmejälgija lisamist.
* **G 1.5 Vesi.** Andmejälgija vaates N/A, kuna andmejälgijat hoitakse eeldatavalt samas ruumis turvaserveriga, mille füüsiline turve on tagatud juba enne andmejälgija lisamist.
* **G 1.8 Tolm, saastumine.** Andmejälgija vaates N/A, kuna andmejälgijat hoitakse eeldatavalt samas ruumis turvaserveriga, mille füüsiline turve on tagatud juba enne andmejälgija lisamist.
* **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 2.6 Volitamata pääs ruumidesse.** Andmejälgija vaates N/A, kuna andmejälgijat hoitakse eeldatavalt samas ruumis turvaserveriga, mille füüsiline turve on tagatud juba enne andmejälgija lisamist.
* **G 2.7 Õiguste volitamata kasutamine**
* **G 2.9 Halb kohanemine IT-muutustega**
* **G 2.10 Probleemid andmekandjate kättesaadavusega.** Andmejälgija vaates N/A, kuna andmejälgija töös andmekandjaid vaja ei lähe.
* **G 2.15 Konfidentsiaalsusaugud *Unix* süsteemis**
* **G 2.21 Korraldamata kasutajavahetus.** Andmejälgija vaates N/A, kuna kasutajavahetus ei mängi arhitektuurist lähtuvalt rolli.
* **G 2.22 Logiandmete analüüsimata jätmine**
* **G 2.24 Kaitsetus välisvõrgu vastu.** Andmejälgija vaates N/A, kuna andmejälgija arhitektuurist lähtuvalt pole seda ohtu vaja käsitleda.
* 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.** Vaadelda tuleb andmejälgija vaates neid liine, mis ühendavad andmejälgijat turvaserveriga.
* **G 3.6 Koristajad jm väljastpoolt tellitud töötajad.** Andmejälgija vaates N/A, kuna andmejälgijat hoitakse eeldatavalt samas ruumis turvaserveriga, mille füüsiline turve on tagatud juba enne andmejälgija lisamist.
* **G 3.8 IT-süsteemi väär kasutamine**
* **G 3.9 IT-süsteemi väär haldus**
* **G 3.11 Sendmaili väär konfiguratsioon.** Eriline risk on räsisid sisaldava teavitusmeili saatmise nurjumisel, mis saadetakse konfiguratsioonifaili muutmisel.
* **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-süsteemidesse**
* **G 4.13 Salvestatud andmete hävimine**
* **G 4.22 Tüüptarkvara turvaaugud või vead**
* **G 4.31 Võrgukomponendi avarii või rike**
* **G 4.35 Ebaturvalised krüptoalgoritmid.** Andmejälgija vaates N/A, kuna tugevust kaotada võivaid krüptoalgoritme neile sisse ehitatud ei ole
* **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.** Andmejälgija vaates N/A, kuna krüptomoodulit neis pole.
* **G 5.83 Krüptograafiliste võtmete paljastamine.** Andmejälgija vaates N/A, kuna andmejälgija krüptovõtmeid ei kasuta.
* **G 5.84 Võltsitud sertifikaadid**
* **G 5.87 Veebilehe võltsimine**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija suhtes spetsiifilistele aspektidele.

**Planeerimine ja kontseptsioon**

* + - **M 2.3 (L) Andmekandjate haldus**
    - **M 2.9 (L) Aktsepteerimata riist- ja tarkvara kasutuse keeld**
    - **M 2.11 (L) Paroolide kasutamise reeglid**
    - **M 2.12 (M) IT-kasutajate nõustamine**
    - **M 2.24 (M) IT-passi juurutamine**
    - **M 2.30 (L) Kasutajate ja kasutajarühmade määramise protseduurid**
    - **M 2.214 (L) IT-kasutuse kontseptsioon**
    - **M 2.216 (L) IT-komponentide kinnitamise protseduur**
    - **M 2.218 (L) Andmekandjate ja IT-komponentide kaasavõtmise protseduurid.** Andmejälgija vaates N/A, kuna andmekandjaid ei kasutata ja andmejälgija on kohtkindlalt paigas.
    - **M 2.220 (L) Pääsu reguleerimise suunised**
    - **M 2.221 (L) Muudatuste haldus**
    - **M 2.223 (L) Tüüptarkvara kasutamise turvaeesmärgid**
    - **M 4.133 (M) Sobivate autentimismehhanismide valimine.**
    - **M 4.134 (L) Sobivate andmevormingute valimine**
    - **M 5.68 (M) Krüpteerimisprotseduuride kasutamine võrgusuhtluses.** Andmejälgija vaates N/A, kuna andmejälgija võrgusuhtluses spetsiaalseid krüpteerimisprotseduure ei kasutata.
    - **M 5.77 (M) Alamvõrkude rajamine.** Andmejälgija vaates N/A, kuna andmejälgija korral alamvõrke ei kasutata.

**Soetamine**

* + - **M 2.62 (L) Tarkvara vastuvõtuprotseduurid**

**Rakendamine**

* **M 1.29 (L) IT-süsteemi õige paigutus.** Andmejälgija vaates N/A, kuna andmejälgijat hoitakse eeldatavalt samas ruumis turvaserveriga, mille füüsiline turve on tagatud juba enne andmejälgija lisamist.
  + - **M 1.32 (M) Printerite ja koopiamasinate turvaline paigutus.** Andmejälgija vaates N/A, kuna printereid ja koopiamasinaid seal ei kasutata.
    - **M 2.25 (L) Süsteemi konfiguratsiooni dokumenteerimine**
    - **M 2.26 (L) Süsteemiülema ja ta asetäitja määramine**
    - **M 2.38 (M) Administraatorirollide jagamine**
    - **M 2.69 (M) Tüüpsete tööjaamade rajamine**
    - **M 2.111 (L) Juhendite hoidmine käepärast**
    - **M 2.138 (L) Struktureeritud andmetalletus**
    - **M 2.204 (L) Ebaturvalise võrkupääsu tõkestamine**
    - **M 4.1 (L) PC ja serveri paroolkaitse**
    - **M 4.7 (L) Algparoolide muutmine**
    - **M 4.65 (L) Uue riist- ja tarkvara testimine**
    - **M 4.84 (L) BIOSi turvamehhanismide kasutamine**
    - **M 4.135 (L) Süsteemifailide pääsuõiguste andmise kitsendused**
    - **M 5.87 (M) Leping kolmandate poolte võrkudega ühendamise kohta.** Andmejälgija vaates N/A, kuna andmejälgija korral reguleerib teabevahetust seadus, mitte lepingud.
    - **M 5.88 (M) Leping andmevahetuse kohta kolmandate pooltega.** Andmejälgija vaates N/A, kuna andmejälgija korral reguleerib teabevahetust seadus, mitte lepingud.

**Kasutamine**

* + - **M 1.46 (M) Vargusetõrjevahendid**
    - **M 2.10 (L) Riistvara ja tarkvara inventuur.** Peab hõlmama ka andmejälgija vahendeid.
    - **M 2.22 (L) Paroolide deponeerimine.** Andmejälgija vaates N/A, kuna sisselogimine hakkab toimuma EID vahenditega.
    - **M 2.31 (L) Volitatud kasutajate ja õiguseprofiilide dokumenteerimine**
    - **M 2.34 (L) IT-süsteemi muutuste dokumenteerimine**
    - **M 2.35 (L) Teabe hankimine turvaaukude kohta**
    - **M 2.64 (L) Logifailide kontroll**
    - **M 2.65 (L) IT-süsteemi kasutajate eraldatuse kontroll**
    - **M 2.110 (M) Andmeprivaatsuse suunised logimisprotseduurides.** Andmejälgija vaates N/A, kuna isikuandmete kogumine on projekti eesmärgiks ja logides neid nagunii vältida ei saa, selleks et nad täidaks oma eesmärki.
    - **M 2.182 (L) IT-turvameetmete regulaarne läbivaatus**
    - **M 2.215 (L) Tõrkekäsitlus**
    - **M 2.219 (L) Infotöötluse pidev dokumenteerimine**
    - **M 2.273 (L) Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine**
    - **M 2.402z (L) Paroolide lähtestamine**
    - **M 4.78 (L) Konfiguratsioonimuudatuste hoolikas teostamine**
    - **M 4.107 (L) Tootja ressursside kasutamine.** Andmejälgija vaates N/A, kuna tootja ressurssidega pole lahenduse spetsiifika tõttu midagi olulist peale hakata.
    - **M 4.109 (L) Tööjaamade tarkvara reinstalleerimine**
    - **M 4.254 (M) Juhtmeta klaviatuuri ja hiire turvaline kasutuselevõtt.** Andmejälgija vaates N/A, kuna haldus toimub kaugpöördusega, reeglina ilma lokaalse klavatuuri ja hiireta.
    - **M 4.306z (M) Paroolide salvestusseadeldise kasutamine.** Andmejälgija vaates N/A, kuna arhitektuuri eripära tõttu (sisselogimine EID vahenditega) pole paroolihaldust vaja rakendada.
    - **M 4.345 (M) Kaitse soovimatu infoäravoolu eest**
    - **M 5.150 (M) Penetratsioonitestide läbiviimine.** Andmejälgija veebiliidese korral tuleks läbi viia penetratsioonitest OWASP Top 10 metoodika põhjal. Siin on asutusel mõistlik hinnata ohu suurust ning tekkivat kahju, kui andmed peaksid lekkima „halva“ (OWASP Top10 metoodika põhist testi mitteläbiva) veebiliidese kaudu – mis andmed lekivad ja mis on võimalik kahju.

**Väljavahetamine**

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

**Valmisolek hädaolukorraks**

* + - **M 6.27 (L) BIOS-süsteemi turvaline värskendamine**

**B 1.14 Turvapaikade ja muudatuste haldus**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Organisatsioonilised puudused:**

* + **G 2.1 Reeglite puudumine või puudulikkus**
  + **G 2.9 Halb kohanemine IT-muutustega**
  + **G 2.17 Andmekandjate puudulik märgistus.** Andmejälgija vaates N/A, kuna andmekandjaid selle arhiketruuri eripärade tõttu ei kasutata.
  + **G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja evitusprotseduurid**
  + **G 2.27 Ebapiisav või puuduv dokumentatsioon**
  + **G 2.28 Autoriõiguse rikkumine.** Andmejälgija vaates N/A, kuna autoriõiguse rikkumine pole siin teemaks.
  + **G 2.132 Tööprotsesside puudulik arvestamine turvapaikade ja muudatuste haldamisel**
  + **G 2.133 Turvapaikade ja muudatuste haldamise vastutusalade puudulik**
* **kindlaksmääramine**
  + **G 2.134 Ebapiisavad ressursid turvapaikade ja muudatuste haldamisel**
  + **G 2.135 Puudulik kommunikatsioon 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.** Andmejälgija vaates N/A, kuna mobiilseid terminale haldusel ei kasutata (kuigi kaughaldus toimub TLS-põhise https-protokolli vahendusel).

* + **G 2.140 Ebapiisav hädaolukorraks valmisoleku kontseptsioon 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.** Üks kriitilisemaid intsidente andmejälgija juures on selle pahatahtlik manipuleerimine. Ohtlikumad on selline terviklusrünne, kus kellegi andmete vaatamisi kuritahtlikult ei salvestata-registreerita, ja selline konfidentsiaalsusrünne, kus riigi jõustruktuuride päringud koos päringusubjektidega edastatakse kellelegi lubamatult.
  + **G 5.145 Andmete ja utiliitide manipuleerimine turvapaikade ja muudatuste haldamisel**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine:**

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

**Soetamine**

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

**Rakendamine**

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

**Kasutamine**

* **M 2.219 (L) Infotöötluse pidev dokumenteerimine**
* **M 2.426 (M) Turvapaikade ja muudatuste halduse integreerimine äriprotsessidesse**
* **M 2.427 (M) Muudatustaotluste kooskõlastamine**
* **M 2.428z (M) Skaleeritavus paikade ja muudatuste haldamisel**. Andmejälgija vaates N/A, kuna skaleeritavus ei oma andmejälgija arhitektuuri tõttu siin rolli.
* **M 2.429z (M) Muudatusnõuete tulemuslikkuse mõõtmine**
* **M 4.78 (L) Konfiguratsioonimuudatuste hoolikas teostamine**
* **M 4.177 (L) Tarkvarapakettide tervikluse ja autentsuse tagamine**
* **M 4.323z (M) Sünkroniseerimine turvapaikade ja muudatuste halduse raames.** Andmejälgija vaates N/A, kuna sünkroniseerimine ei oma andmejälgija arhitektuuri tõttu siin rolli.
* **M 4.324 (M) Automaatsete uuendusmehhanismide konfiguratsioon turvapaikade ja**
* **muudatuste haldamisel**

**B 3.101 Server**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**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.** Kriitilisim tagajärg, mida niiviisi talitades saabuda saab, on andmejälgija konfiguratsiooni lubamatu muutmine, mis võib viia olulise terviklus- või konfidentsiaalsuskaoni.
* **G 5.21 Trooja hobused**
* **G 5.23 Viirused**
* **G 5.26 Sõnumivoo analüüsimine**
* **G 5.40 Pealtkuulamine ruumis arvuti mikrofoni kaudu.** N/A. Andmejälgija koosseisu mikrofone ei plaanita.
* **G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu**
* **G 5.75 Ülekoormus siseneva meili tõttu**
* **G 5.85 Tundliku informatsiooni tervikluse kadu**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine ja kontseptsiooni loomine**

* **M 1.28 (L) Puhvertoiteallikas (UPS)**
* **M 2.314 (M) Kõrgkäideldava serveriarhitektuuri kasutamine**
* **M 2.315 (L) Serveri kasutuselevõtu planeerimine**
* **M 2.316 (L) Serveri turvapoliitika kehtestamine**
* **M 4.250 (M) Keskse võrgupõhise autentimisteenuse valimine**
* **M 5.10 (L) Piiratud õiguste andmine**
* **M 5.138 (M) RADIUS serverite kasutamine.** N/A. Kuna mobiilsidet andmejälgijas ei kasutata, pole RADIUS serveril rolli ega mõtet.

**Soetamine**

* **M 2.317 (L) Serveri soetamise kriteeriumid**

**Rakendamine**

* **M 2.32 (M) Piiratud kasutajakeskkonna loomine**
* **M 2.204 (L) Ebaturvalise võrkupääsu tõkestamine**
* **M 2.318 (L) Serveri turvaline installeerimine**
* **M 4.7 (L) Algparoolide muutmine**
* **M 4.15 (L) Turvaline sisselogimine**
* **M 4.16 (L) Konto- ja/või terminalipääsu piirangud**
* **M 4.17 (L) Tarbetute kontode ja terminalide blokeerimine**
* **M 4.40 (M) Arvuti mikrofoni volitamata kasutamise vältimine.** N/A. Andmejälgijaks kasutatavas arvutis mikrofoni olemasolu ei plaanita.
* **M 4.237 (L) IT-süsteemi turvaline aluskonfiguratsioon**
* **M 4.305 (L) Salvestusvõimaluste piiramine (Quotas-kvoodid)**

**Kasutamine**

* **M 2.22 (L) Paroolide deponeerimine**
* **M 2.273 (L) Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine**
* **M 4.24 (L) Järjekindla süsteemihalduse tagamine**
* **M 4.93 (L) Regulaarne tervikluse kontroll**
* **M 4.238 (M) Lokaalse paketifiltri rakendamine.** N/A. Andmejälgija arhitektuurist lähtuvalt pole sellise paketifiltri rakendamine ostatarbekohane.
* **M 4.239 (M) Serveri turvaline käitus**
* **M 4.240 (M) Serveri testimiskeskkonna rajamine**
* **M 5.8 (M) Võrgu regulaarne turvakontroll**
* **M 5.9 (L) Serveri logi**

**Väljavahetamine**

* **M 2.319 (L) Serveri üleviimine**
* **M 2.320 (L) Serveri korrakohane kasutuselt kõrvaldamine**

**Ootamatuseplaan**

* **M 6.24 (L) Rikkejärgse buutimismeedia olemasolu**
* **M 6.96 (L) Serveri avariiplaan.** Olemas peab olema kogu andmejälgija süsteemi avariiplaan kõikide tõenäolisimate turvarikete puhuks.

**B 3.304 Virtualiseerimine**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**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 puudulik 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**. N/A. Andmejälgija juures SAN-võrke ei kasutata.
* **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.** N/A. Kui andmejälgijas virtualiseerimist rakendatakse, ei kasutata spetsiaalseid haldusservereid.
* **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**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine ja kontseptsioon**

* **M 1.74 (L) Virtuaalse taristu planeerimine**
* **M 2.82 (M) Tüüptarkvara testimisplaani väljatöötamine**
* **M 2.392 (L) Virtualiseerimisserverite ja virtuaalsete IT-süsteemide modelleerimine**
* **M 2.444 (L) Virtuaalsete IT-süsteemide ressursside planeerimine**
* **M 3.70 (L) Sissejuhatus virtualiseerimisse**
* **M 3.71 (M) Virtuaalkeskkondade administraatorite koolitamine**
* **M 5.153 (M) Võrgu planeerimine virtuaalsete taristute jaoks**

**Soetamine**

* **M 2.445 (L) Sobiva riistvara valimine virtualiseerimiskeskkondade jaoks**

**Rakendamine**

* **M 2.83 (M) Tüüptarkvara testimine**
* **M 2.446 (M) Haldustoimingute jaotus virtualiseerimisserverite puhul**
* **M 2.447 (L) Virtuaalsete IT-süsteemide turvaline kasutamine**
* **M 3.72 (M) Virtualiseerimistehnika põhimõisted**
* **M 4.97z (M) Ainult üks teenus serveri kohta**
* **M 4.346 (L) Virtuaalsete IT-süsteemide turvaline konfigureerimine**
* **M 5.154 (M) Virtuaalse taristu võrgu turvaline konfiguratsioon**

**Kasutamine**

* **M 2.448 (M) Virtuaalsete taristute funktsiooni ja konfiguratsiooni kontroll**
* **M 4.348 (M) Aja sünkroniseerimine virtuaalsetes IT-süsteemides**
* **M 4.349 (L) Virtuaalse taristu turvaline kasutamine**

**Valmisolek hädaolukorraks**

* **M 6.138 (M) Hädaolukorraks valmisoleku plaani koostamine virtualiseerimiskomponentide tõrke puhuks.** Ka need komponendid peavad sisalduma andmejälgija hädaolukorra plaanides, kui see realiseeritakse virtuaalserverina.

**B 5.4 Veebiserver**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**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 Autoriõiguse rikkumine.** Andmejälgija vaates N/A, kuna autoriõigused ei ole andmejälgija sisu ja äriloogika juures probleemiks.
* **G 2.32 Võrgu ebapiisav võimsus.** Andmejälgija vaates N/A, kuna võrgu võimsus on nagunii ära määratud X-tee turvaserveri poolt ja andmejälgija tekitatud koormus on marginaalne.
* **G 2.37 Sideliinide kontrollimatu kasutamine**
* **G 2.96 Aegunud või väär teave veebisaidil**
* **G 2.100 Interneti domeeninimede taotlemise või haldamise vead.** Andmejälgija vaates N/A, kuna domeeninimi ei mängi andmejälgija juures rolli.

**Inimvead:**

* **G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu.** Andmejälgija vaates N/A, kuna kasutaja ei saa üle veebiliidese andmejälgija äriloogikat muuta (v.a. juhud, kus modifitseeritakse konfiguratsioonifaili).
* **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**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine ja kontseptsioon**

* **M 2.172 (L) Veebilehe kasutamise kontseptsiooni väljatöötamine**
* **M 2.173 (L) Veebiserveri turbestrateegia väljatöötamine**
* **M 2.272z (L) Veebitoimetajate meeskonna loomine**
* **M 4.34z (M) Krüpteeringu, kontrollsummade või digitaalallkirjade rakendamine.** Andmejälgija vaates N/A, kuna halduseks kasutatav veebiliides mingit spetsiifilist krüpteeringut või digiallkirja ei sisalda (haldust kaitseb TLS-protokoll).
* **M 4.176 (L) Autentimismeetodite valimine veebilehtede jaoks**
* **M 5.64z (M) Secure Shell**
* **M 5.66z (M) TLS-i/SSL-i kasutamine.** Andmejälgija vaates peab kogu veebipõhine kaughaldus toimuma üle TLSile toetuva https-protokolli.
* **M 5.159 (W) Veebiserveri protokollide ja kommunikatsioonistandardite ülevaade**
* **M 5.160 (W) Autentimine veebiserveril**

**Soetamine**

* **M 2.176 (M) Sobiva internetiteenuse pakkuja valimine.** Andmejälgija vaates N/A, kuna tegu on turvaserveri lisaga, mis kasutab sama teenusepakkujat.

**Rakendamine**

* **M 2.175 (L) Veebiserveri ülesseadmine**
* **M 4.64 (L) Ülekantavate andmete kontrollimine enne edastamist/peidetud info**
* **kõrvaldamine**
* **M 4.94 (M) Veebiserveri failide turve**
* **M 4.95 (L) Minimaalne operatsioonisüsteem**
* **M 4.98 (L) Side piiramine miinimumini paketifiltritega**
* **M 4.360 (M) Veebiserveri turvaline konfiguratsioon**

**Kasutamine**

* **M 2.174 (L) Veebiserveri turvaline kasutamine**
* **M 2.273 (L) Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine**
* **M 4.33 (M) Viirusetõrjeprogrammi kasutamine andmekandjate vahetamisel ja andmete**
* **edastamisel.** Andmejälgija vaates N/A, kuna veebiliideses viiruseid sisaldada võivaid andmevorminguid ei edastata ja teiseldatavaid andmekandjaid ei kasutata.
* **M 4.78 (L) Konfiguratsioonimuudatuste hoolikas teostamine**
* **M 4.177 (L) Tarkvarapakettide tervikluse ja autentsuse tagamine**
* **M 5.59 (L) DNS võltsimise tõrje**

**Valmisolek hädaolukorraks**

* **M 6.88 (L) Veebiserveri hädaolukorraks valmisoleku plaani koostamine.** St andmejälgija hädaolukorraks valmisoleku plaani üks osa.

**B 5.7 Andmebaasid**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Organisatsioonilised puudused:**

* **G 2.22 Logiandmete analüüsimata jätmine**
* **G 2.26 Ebapiisavad või puuduvad tarkvara katsetamis- ja evitusprotseduurid**
* **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.** Andmejälgija vaates N/A, kuna väliseid andmekandjaid ei kasutata.
* **G 2.110 Andmebaasi versiooniuuenduste ja üleviimise puudulik organiseerimine**
* **Inimvead:**
* **G 3.6 Koristajad jm väljastpoolt tellitud töötajad.** Andmejälgija vaates N/A, kuna väliseid töötajaid turvaserveri ja andmejälgija serveri ligi ei lasta.
* **G 3.16 Väär pääsuõiguste haldus**
* **G 3.23 Andmebaasisüsteemi hooletu haldus**
* **G 3.24 Andmete juhuslik manipuleerimine**
* **G 3.80 Andmebaaside sünkroniseerimisvead.** Andmejälgija vaates N/A, kuna sünkroniseerimist ei toimu

**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**

**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**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine ja kontseptsioon**

* **M 2.80 (M) Tüüptarkvara nõuete kataloogi koostamine**
* **M 2.126 (L) Andmebaasi turvakontseptsioon**
* **M 2.132 (L) Andmebaasi kasutajate ja kasutajagruppide konfigureerimise reeglid**
* **M 2.134 (L) Andmebaasipäringute suunised**
* **M 2.363 (L) SQL-injektsiooni kaitse**
* **M 5.58 (M) Andmebaasiliidese draiverite valik ja installeerimine**

**Soetamine**

* **M 2.124 (L) Sobiva andmebaasitarkvara valimine**

**Rakendamine**

* **M 2.125 (L) Andmebaasi installeerimine ja konfigureerimine**
* **M 2.135 (L) Andmete turvaline teisaldus andmebaasi.**
* **M 4.7 (L) Algparoolide muutmine**
* **M 4.71 (L) Andmebaasi linkide kasutamise kitsendamine**
* **M 4.73 (M) Valitavate andmehulkade ülempiiride määramine**

**Kasutamine**

* **M 2.31 (L) Volitatud kasutajate ja õiguseprofiilide dokumenteerimine**
* **M 2.34 (L) IT-süsteemi muutuste dokumenteerimine**
* **M 2.65 (L) IT-süsteemi kasutajate eraldatuse kontroll**
* **M 2.127 (M) Tuletamise vältimine andmebaasis**
* **M 2.128 (L) Andmebaasisüsteemi pääsu reguleerimine**
* **M 2.129 (L) Andmebaasiinfo pääsu reguleerimine**
* **M 2.130 (L) Andmebaasi tervikluse tagamine**
* **M 2.131 (L) Haldusülesannete lahusus andmebaasisüsteemides**
* **M 2.133 (L) Andmebaasisüsteemi logifailide kontroll**
* **M 3.18 (L) PC kasutajate väljalogimiskohustus.** Andmejälgija vaates N/A, kuna andmejälgija arvutit töökohaarvutina ei kasutata.
* **M 4.67 (L) Tarbetute andmebaasikontode lukustus ja kustutus**
* **M 4.68 (L) Järjekindla andmebaasi halduse tagamine**
* **M 4.69 (L) Andmebaasi regulaarne turvakontroll**
* **M 4.70 (L) Andmebaasiseire teostamine**
* **M 4.72 (L) Andmebaasi krüpteerimine.** Andmejälgija vaates N/A, kuna andmejälgija arhitektuurist lähtuvalt pole andmebaasi vaja krüpteerida.
* **M 5.117 (M) Andmebaasiserveri integreerimine turvalüüsi koostisse.** Andmejälgija vaates N/A, kuna andmejälgija arhitektuur on turvaserveri arhitektuurist lähtuvalt veidi teistsugune ja keerukam.

**Valmisolek hädaolukorraks**

* **M 6.48 (L) Protseduurid andmebaasi tervikluse kao puhuks.** Peavad sisalduma andmejälgija hädaolukorraks valmisoleku plaanides.
* **M 6.49 (L) Andmebaasi varundamine**
* **M 6.50 (L) Andmebaasi arhiveerimine**
* **M 6.51 (L) Andmebaasi taastamine**

**B 5.21 Veebirakendused**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**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 või ebapiisav analüüs**
* **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 Pääsuõiguste väär 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 Halb või puuduv autentimine**
* **G 4.35 Ebaturvalised krüptoalgoritmid**
* **G 4.84 Veebirakenduste sisendi- ja väljundiandmete ebapiisav valideerimine**
* **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.** Eritähelepanu tuleks pöörata sellele, et ei tekiks riigi jõustruktuuride poolt tehtud päringute (sh nende parameetrite) konfidentsiaalsuskadu.

**Ründed**

* + **G 5.18 Süstemaatiline paroolide mõistatamine**
  + **G 5.19 Kasutajaõiguste väärkasutus**
  + **G 5.20 Administraatoriõiguste väärkasutus**
  + **G 5.28 Teenuse halvamine**
  + **G 5.87 Veebilehe võltsimine**
  + **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 klientsüsteemides**
  + **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 pahavara koodi smugeldamine veebirakendustesse**
  + **G 5.174 Injektsiooniründed**
  + **G 5.175 Klõpsurööv (clickjacking)**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine ja kontseptsioon**

* **M 2.1 (L) IT kasutajate vastutuse ja reeglite kehtestamine**
* **M 2.11 (L) Paroolide kasutamise reeglid**
* **M 2.63 (L) Pääsuvolituste kehtestamine**
* **M 2.80 (L) Tüüptarkvara nõuete kataloogi koostamine**
* **M 2.363 (L) SQL-injektsiooni kaitse**
* **M 2.486 (L) Veebirakenduste arhitektuuri dokumenteerimine**
* **M 2.487 (L) Veebirakenduste arendamine ja laiendamine**
* **M 2.488 (W) Web tracking**
* **M 4.176 (L) Autentimismeetodi valimine veebilehtede jaoks**
* **M 4.404 (L) Veebirakenduste turvalise loogika kavandamine**
* **M 5.66 (L) TLS-i/SSL-i kasutamine**
* **M 5.168 (L) Taustsüsteemide turvaline sidumine veebirakendustega**
* **M 5.169 (L) Veebirakenduse süsteemiarhitektuur**

**Soetamine**

* **M 2.62 (L) Tarkvara vastuvõtu protseduurid**
* **M 4.400 (L) Turbe seisukohalt oluliste andmete väljastamine veebirakendustes**

**Rakendamine**

* **M 4.392 (L) Autentimine veebirakendustes**
* **M 4.393 (L) Sisestuste ja väljastuste põhjalik valideerimine**
* **veebirakendustes**
* **M 4.394 (L) Seansihaldus veebirakendustes**
* **M 4.395 (L) Tõrkekäsitlus veebirakendustes**
* **M 4.396 (L) Veebirakenduste kaitsmine keelatud automaatkasutuse eest**
* **M 4.398 (L) Veebirakenduste turvaline konfiguratsioon**
* **M 4.399 (L) Andmete ja sisu kontrollitud lisamine veebirakendustesse**
* **M 4.401 (L) Konfidentsiaalsete andmete kaitse veebirakendustes**
* **M 4.402 (L) Juurdepääsukontroll veebirakendustes**
* **M 4.403 (M) Cross-Site Request Forgery (CSRF, XSRF, Session Riding)**
* **tõkestamine**
* **M 4.405 (M) Ressursside blokeerimise (DoS-rünnete) tõkestamine veebirakendust**
* **M 4.406 (Z) Clickjacking-rünnete tõkestamine**

**Kasutamine**

* **M 2.8 (L) IT-rakendustele ja andmetele pääsuõiguste andmine**
* **M 2.31 (L) Volitatud kasutajate ja õiguseprofiilide dokumenteerimine**
* **M 2.34 (L) IT-süsteemi muutuste dokumenteerimine**
* **M 2.35 (L) Teabe hankimine turvaaukude kohta**
* **M 2.64 (M) Logifailide kontroll**
* **M 2.110 (M) Andmeprivaatsuse suunised logimisprotseduurides**
* **M 2.273 (L) Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine**
* **M 3.5 (L) Turvameetmete koolitus**
* **M 4.78 (L) Konfiguratsioonide hoolikas teostamine**
* **M 4.397 (M) Veebirakenduste turvet puudutavate sündmuste logimine**
* **M 5.150 Penetratsioonitestide läbiviimine.** Andmejälgija veebiliidese korral tuleks läbi viia penetratsioonitest OWASP Top 10 metoodika põhjal.

**B 5.22 Logimine**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**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 või ebapiisav analüüs**
* **G 2.61 Isikuandmete volitamatu kogumine.** Andmejälgija vaates N/A, kuna andmejälgija on just ellu kutsutud isikuandmete kasutamise analüüsiks ja neid töödeldakse siin õiguspäraselt.
* **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.** Andmejälgija vaates N/A, kuna andmejälgija fikseerib isikuandmete kasutamise aja turvaserveris ja täiendav aja sünkroniseerimine pole vajalik.

**Tehnilised rikked**

* **G 4.89 Logimise puuduv või ebapiisav hoiatamiskontseptsioon**

**Ründed**

* **G 5.20 Administraatoriõiguste väärkasutus.** Kriitilisim on siin andmejälgija konfiguratsioonifaili volitamata muutmine, mis mõjutab otseselt kogutavate andmete (logide) hulka või nende edasist edastamist/käitlemist.
* **G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu.** Kriitilisim on siin konfidentsiaalsuskadu, kus riigi jõustruktuuride päringud koos päringusubjektidega edastatakse andmejälgijast kellelegi lubamatult.
* **G 5.85 Tundliku informatsiooni tervikluse kadu.** Kriitilisim on siin konfidentsiaalsuskadu, kus kellegi andmesubjekti kohta tehtud päringud koos päringusubjektidega jäetakse volitamatult logidest (jälgimise alt) välja.
* **G 5.143 Man-in-the-Middle-rünne.**
* **G 5.176 Logiandmete edastuse kompromiteerimine tsentraalses logimises.**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Planeerimine ja kontseptsioon**

* **M 2.1 (L) IT kasutajate vastutuse ja reeglite kehtestamine**
* **M 2.497 (L) Logiserveri korrakohane kasutusest kõrvaldamine**
* **M 2.499 (L) Logimise planeerimine**
* **M 2.500 (L) IT-süsteemide logimine**
* **M 3.90 (W) Tsentraalse logimise põhitõed**
* **M 5.66 (L) TLS-i/SSL-i kasutamine**
* **M 5.68 (M) Krüpteerimisprotseduuride kasutamine võrgusuhtluses**

**Rakendamine**

* **M 2.498 (M) Reageerimine hoiatus- ja veateadetele**
* **M 3.10 (L) Usaldusväärse administraatori ja tema asetäitja valimine**
* **M 3.89 (L) Logimisprotsessi haldamise koolitus**
* **M 6.151 (L) Logimise häirepoliitika**

**Kasutamine**

* **M 2.8 (L) IT-rakendustele ja andmetele pääsuõiguste andmine**
* **M 2.64 (L) Logifailide kontroll**
* **M 2.110 (L) Andmeprivaatsuse suunised logimisprotseduurides**
* **M 4.277 (M) Windowsi serverite SMB-, LDAP- ja RPC-kommunikatsiooni kaitse**
* **M 4.430 (L) Logiandmete analüüs**
* **M 4.431 (L) Logimise jaoks oluliste andmete valik ja töötlemine**
* **M 5.9 (L) Serveri logi**
* **M 5.171 (L) Turvaline andmeside keskse logiserveriga**
* **M 5.172 (L) Turvaline aja sünkroniseerimine keskse logimise korral.** Andmejälgija vaates N/A, kuna ajaarvestus toimub turvaserveri aja järgi ja keskset logimist ei toimu.
* **Kasutusest kõrvaldamine**
* **M 2.167 (L) Andmete kustutamine või hävitamine**
* **M 2.496 (L) Logiserveri korrakohane kasutusest kõrvaldamine**

**Valmisolek hädaolukorraks**

* **M 6.96 (M) Serveri avariiplaan.** St andmejälgija hädaolukorraks valmisoleku plaani üks osa.

**B 5.E2 ID-kaart/PKI**

**Ohud**

Edasises on ära tähistatud need ohud, mis on andmejälgija vaates N/A, ja ka need ohud, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

**Vääramatu jõud:**

* **G 1.2 IT-süsteemi avarii**
* **G 1.19 Teenusepakkuja või tarnija väljalangemine**

**Organisatsioonilised puudused:**

* **G 2.1 Reeglite puudumine või puudulikkus**
* **G 2.2 Reeglite puudulik tundmine**
* **G 2.3 Puuduvad, puudulikud või ühildamatud ressursid**
* **G 2.4 Turvameetmete ebapiisav järelevalve**
* **G 2.8 Ressursside kontrollimatu kasutamine**
* **G 2.19 Halb krüpteerimise korraldus.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse ja selle juures standardlahendusi.
* **G 2.47 Failide ja andmekandjate ebaturvaline transport.** Andmejälgija vaates N/A, kuna CDOCi ega andmete edastamist andmekandjatel ei kasutata.
* **G 2.77 Paberdokumentide elektroonilise arhiveerimise puudused.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 2.90 Välise teenusetarnijaga seotud nõrkused**
* **G 2.102 Infoturbe puudulik teadvustamine**
* **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.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 2.E8 Digiallkirjastatud dokumendi vormingureeglite mitmetimõistetavus.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 2.E9 Digitempli andmise seadme kasutuseõiguse väljumine asutuse poolt määratud subjektide ringist.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 2.E10 Juurdepääsutõendiga määratud digiallkirjade mahu ammendumine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 2.E11 Signeerimistarkvara puudus, mis võimaldab anda digiallkirja autentimisvõtmepaari ja PIN1-koodi kasutades.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 2.E12 Pin-pad'i mittekasutamine**

**Inimvead:**

* **G 3.1 Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu**
* **G 3.2 Seadme või andmete tahtmatu hävitamine**
* **G 3.3 Hooletus turvameetmete suhtes**
* **G 3.33 Krüptomoodulite väär kasutamine**
* **G 3.44 Teabe hooletu kasutamine**
* **G 3.77 Infoturbe puudulik aktsepteerimine**
* **G 3.105 Väliste teenuste volitamata kasutamine.** Andmejälgija vaates N/A, kuna digitempleid ja juurdepääsutõendeid ei kasutata, EID-vahenditega toimub vaid autentimine.
* **G 3.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 tõrge**
* **G 4.35 Ebaturvalised krüptoalgoritmid**
* **G 4.36 Vead kodeeritud andmetes.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digidokumenti.
* **G 4.41 Mobiilsidevõrgu käideldamatus**
* **G 4.42 Mobiiltelefoni või PDA tõrge**
* **G 4.47 Vananenud krüptomeetodid**
* **G 4.48 Välise teenusetarnija süsteemide tõrge**
* **G 4.E1 Teenusekatkestuste oht SSOga ühismöllimisel.** Andmejälgija vaates N/A, kuna SSOsid ja ühismöllimist ei kasutata.

**Ründed:**

* **G 5.1 IT-seadmete või tarvikutega manipuleerimine või nende hävitamine.** Puudutab EID-vahendeid.
* **G 5.2 Andmete või tarkvara manipuleerimine**
* **G 5.4 Vargus.** Puudutab EID-vahendeid.
* **G 5.5 Vandalism.** Puudutab EID-vahendeid.
* **G 5.6 Füüsiline rünne.** EID-vahendi rööv või rikkumine
* **G 5.9 IT-süsteemide volitamata kasutamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digitempleid.
* **G 5.16 Ohud hoolde- ja haldustööde ajal.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digitempleid.
* **G 5.22 Mobiilsüsteemi vargus.** Halvab mobiil-ID kasutamise.
* **G 5.28 Teenuse halvamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte digiallkirja ega digitempleid.
* **G 5.40 Ruumi pealtkuulamine mikrofoni abil.** PIN-koodide varguse eesmärgiga.
* **G 5.42 Inimestega manipuleerimine**
* **G 5.69 Varguseoht kodutöökohas.** Puudutab EID-vahendeid.
* **G 5.70 Pereliikmete või külaliste manipulatsioonid kodutöökohas.** EID-vahendite ja/või nende PIN-koodide kuritahtlik muutmine.
* **G 5.71 Tundliku informatsiooni konfidentsiaalsuse kadu.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist
* **G 5.81 Volitamatu krüptomooduli kasutamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist
* **G 5.82 Krüptomooduli manipulatsioon.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **G 5.83 Krüptovõtmete paljastamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **G 5.84 Sertifikaadipettus**
* **G 5.94 SIM-kaartide kuritarvitamine.** Mõjutab mobiil-ID vahendeid
* **G 5.95 Mobiiltelefoniga pealtkuulamine siseruumis.** PIN-koodide varguse eesmärgiga
* **G 5.96 Mobiiltelefoni ehituse muutmine.** PIN-koodide varguse eesmärgiga või kasutaja teadmata toimuva mobiil-ID osa kasutamise eesmärgiga
* **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**

**Meetmed**

Edasises on ära tähistatud need meetmed, mis on andmejälgija vaates N/A, ja ka need meetmed, kus tuleb tähelepanu pöörata andmejälgija spetsiifilistele aspektidele.

Plaanimine ja kontseptsioon:

* **M 2.1 (L) IT kasutajate vastutuse ja reeglite kehtestamine**
* **M 2.46 (L) Krüpteerimise õige korraldus.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.161 (L) Krüptokontseptsiooni väljatöötamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.162 (M) Krüptoprotseduuride ja -toodete vajaduse määramine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.163 (M) Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.164 (L) Sobiva krüptoprotseduuri valimine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.165 (L) Sobiva krüptotoote valimine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.173 (M) Veebiserveri turbestrateegia väljatöötamine**
* **M 4.85 (L) Sobiv krüptomoodulite liideste disain.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 4.88 (M) Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.E12 (M) E-ID rakendusjuhiste järgimine**
* **M 2.E13 (L) Asutusesisesed reeglid ID-kaardi/PKI kasutamiseks**
* **M 2.E14 (L) Digitempli turvaline evitamine asutuses.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.

**Rakendamine:**

* **M 2.9 (L) Aktsepteerimata riist- ja tarkvara kasutuse keeld. Andmejälgija vaates veebiliidesesse sisenemise seadme nõuded**
* **M 2.12 (L) IT-kasutajate nõustamine**
* **M 2.86 (L) Tarkvara tervikluse tagamine**
* **M 2.166 (M) Krüptomoodulite kasutamist reguleerivad sätted**
* **M 3.1 (L) Uute töötajate esmane juhendamine ja väljaõpe**
* **M 3.2 (L) Uute töötajate kohustamine eeskirju järgima**
* **M 3.4 (L) Väljaõpe enne programmi tegelikku kasutamist**
* **M 3.5 (L) Turvameetmete koolitus**
* **M 3.23 (M) Sissejuhatus krüptograafia põhimõistetesse**
* **M 4.7 (L) Algparoolide muutmine.** ID-kaardi ja mobiil-ID PIN- ja PUK-koodide korral.
* **M 4.34 (L) Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 4.87 (L) Krüptomoodulite füüsiline turve.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 4.88 (M) Nõuded operatsioonisüsteemide turvalisusele krüptomoodulite kasutamise korral.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 4.114 (L) Mobiiltelefonide turvamehhanismide rakendamine**
* **M 4.177 (M) Tarkvarapakettide tervikluse ja autentsuse tagamine**
* **M 4.228 (L) Pihuarvutite turvamehhanismide rakendamine. Nendes seadmetes, kus kasutatakse mobiil-ID lahendusi.**
* **M 5.150 (M) Penetratsioonitestide läbiviimine.** EID vahendiga autenditavas veebiliideses
* **M 3.E2 (L) Töötajate koolitus ID-kaardi/PKI lahenduste kasutamise osas**
* **M 4.E1 (L) ID-kaardi/PKI lahenduste turvaline seadistamine**
* **M 4.E5 (M) Nõuded ID-kaardi/PKI lahendusi kasutavale turvalisele autentimisele**
* **M 4.E6 (L) Keeld anda digiallkirja autentimisvõtmepaari ja PIN1-koodi kasutades**

**Kasutamine:**

* **M 2.22 (L) Paroolide deponeerimine**. EID PUK-koodide korral
* **M 2.111 (M) Juhendite hoidmine käepärast**
* **M 2.224 (L) Trooja hobuste tõrje**
* **M 2.264 (M) Krüpteeritud andmete regulaarne regenereerimine arhiveerimisel.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.265 (M) Digitaalallkirjade õige kasutamine arhiveerimisel.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit
* **M 4.3 (L) Viirustõrjeprogrammi regulaarne kasutamine**
* **M 4.229 (L) Pihuarvutite turvaline kasutamine**
* **M 2.E15 (L) ID-kaardi või sarnase seadme PIN-ja PUK-koodide turvaline käitlemine**
* **M 2.E16 (L) Transpordikrüpto vormingute kasutuskeeld andmete säilitamiseks.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 2.E17 (L) ID-kaardi või sarnase seadme kasutuskeeld tundmatute turvasätetega keskkonnas**
* **M 2.E18 (L) ID-kaardi või digi-ID edasiandmiskeeld teisele isikule**
* **M 2.E19 (W) ID-kaardi või digi-ID kaasavõtmiskohustus arvuti juurest lahkumisel**
* **M 2.E20 (L) Nõuded digiallkirjastatava dokumendi vormingule.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.
* **M 4.E2 (L) ID-kaardi baastarkvara uuendamine**
* **M 4.E3 (L) ID-kaardi, digi-ID ja mobiil-ID ning nende sertifikaatide õigeaegne uuendamine**
* **M 4.E4 (M) Juurdepääsutõendiga määratud signeerimisressursi seire ja uuendamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.

**Likvideerimine:**

* **M 2.E21 (M) Digitembeldussüsteemi tegevuse lõpetamine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit

**Valmisolek hädaolukorraks:**

* **M 5.E1 (L) Sertifikaatide õigeaegne peatamine.**
* **M 5.E2 (M) Varem antud digiallkirjade õigeaegne ülesigneerimine.** Andmejälgija vaates N/A, kuna EID-vahenditest kasutatakse ainult autentimist veebiliidesesse, mitte aga CDOC-krüpteerimist ega digitemplit.

**Meede M 4.86 krüptokontseptsiooni tüüpmoodulist B 1.9**

**M 4.86 (M) Rollide turvaline lahutamine ja krüptomoodulite konfiguratsioon.** Kuigi meede puudutab krüptomooduli haldamist, on seal kirjeldatud kasutaja- ja administraatorirollid ja nende lahususe nõuded üle kantavad ka andmejälgija kasutaja- ja administraatorirollidele. Andmejälgija juures tuleb lähtuda meetmes kirjeldatud rollidest ja nende lahutusest.

# Turvaserveri sees oleva proxy variant

Turvaserveri sees oleva proxy põhine lahendus erineb turvaserverist väljas olevast lahendusest selles osas, et mitmed ISKE tüüpmoodulid jäävad vaatluse alt välja. Nendeks on tüüpmoodulid "Server" (B 3.101), ja " Andmebaasid" (B 5.7). Käsitluse alla jäävad seal igal juhul järgmised ISKE tüüpmoodulid:

* **B 1.3. Hädaolukorraks valmisoleku kontseptsioon** – mõned ohud ja meetmed, mis puudutavad andmejälgija taastet ja selle eritingimusi, enamik N/A
* **B 1.8 Turvaintsidentide käsitlus** – mõned spetsiifilised ohud ja meetmed, mis puudutavad andmejälgija turvaintsidente, enamik N/A
* **B 1.9 Riist- ja tarkvara haldus** - ohud ja meetmed peaaegu täies mahus (arvestades lahenduse spetsiifikat mõned ohud ja meetmed N/A)
* **B 1.14 Turvapaikade ja muudatuste haldus** - ohud ja meetmed täies mahus
* **B 5.4 Veebiserver** - ohud ja meetmed peaaegu täies mahus (kuna andmejälgijal toimib veebirakendus
* **B 5.21 Veebirakendused** - ohud ja meetmed täies mahus
* **B 5.22 Logimine** - ohud ja meetmed täies mahus
* **B 5.E2 ID-kaart/PKI** - ohud ja meetmed, mis puudutavad EID vahendiga sisselogimist, muud jäävad välja

Tüüpmoodul "Virtualiseerimine" (B 3.304) jääb vaatluse alt välja siis, kui turvaserver ei ole realiseeritud virtuaalserverina. Kui turvaserver on realiseeritud virtuaalserverina, siis jääb see tüüpmoodul vaatluse alla turvaserveri arhitektuuriliste eripärade tõttu.

Sarnaselt variandile A lisandub toodud nimekirjale krüptokontseptsiooni tüüpmoodulist B 1.7 meede M 4.86, mida rakendatakse andmejälgija korral eritingimustel.

Nendele tüüpmoodulitele vastavate ohtude nimekirjad langevad täies mahus kokku turvaserverist väljas oleva proxy variandiga (toodud jaotises A), mistõttu neid siin korratud ei ole.