Ohje turvallisuusluokan I tiedon sähköisestä käsittelystä

1 Johdanto

Kansainvälisistä tietoturvallisuusvelvoitteista, turvallisuusselvityksistä sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien[1] mukaan Liikenne- ja viestintävirasto Traficomin tehtäviin kuuluvat erilaiset tietojärjestelmien turvallisuusarvioinnit ja -hyväksynnät. Edellä mainittujen tehtävien lisäksi Traficomin Kyberturvallisuuskeskus tarjoaa tietoturvallisuuden neuvontapalvelua turvallisuusluokiteltua tietoa käsitteleville organisaatioille.

Katakri on viranomaisten ja elinkeinoelämän yhteistyössä laatima työkalu[2], johon on koottu keskeiset kansallisen ja kansainvälisen turvallisuusluokitellun tiedon suojaamiseen kohdistuvat vaatimukset turvallisuusluokkien IV, III ja II osalta. Katakri-työkalua voidaankin hyödyntää sekä kansallisen, että myös kansainvälisen turvallisuusluokitellun tiedon suojausten suunnittelussa ja arvioinnissa. Katakrin tuettuja käyttötapauksia ovat yritysturvallisuusselvitykset (L 726/2014) sekä viranomaisten tietojärjestelmien arvioinnit (L 1406/2011). Kyberturvallisuuskeskus saa säännöllisesti tiedusteluja myös siitä, kuinka turvallisuusluokan I tietojen sähköinen käsittely olisi suositeltavaa suojata.

Tässä ohjeessa kuvataan Kyberturvallisuuskeskuksen keskeiset suositukset turvallisuusluokan I tietojen sähköisen käsittelyn suojaamiseen. Ohje on laadittu siten, että se täydentää Katakriin koottuja turvallisuusluokan II suojauksia turvallisuusluokan I lisäsuojauksilla siltä osin, kun ne liittyvät sähköiseen, tietojärjestelmissä tapahtuvaan tietojenkäsittelyyn. Ohjeessa ei käsitellä turvallisuusluokan I tietojen käsittelyn asettamia mahdollisia lisäsuojaustarpeita organisaatioiden hallinnolliselle turvallisuudelle, henkilöstöturvallisuudelle tai fyysiselle turvallisuudelle.

2 Tietoliikenneturvallisuus

2.1 Tietojenkäsittely-ympäristöjen erottelu

Katakri 2020:n kohtaan I-01 on koottu turvallisuusluokan II tietojenkäsittely-ympäristön erottelulle kohdistuvat suojausvaatimukset. Turvallisuusluokan I tietojenkäsittely-ympäristöjen erottelussa tulee lisäksi huomioida erityisesti seuraavat:

- Lähtökohtaisesti turvallisuusluokan I tietojenkäsittely-ympäristöt suositellaan pidettäväksi fyysisesti eriytettyinä kaikista muista ympäristöistä. Tyypillisenä toteutustapana on fyysisellä turva-alueella, hajasäteilysuojatussa tilassa tapahtuva kaikista muista ympäristöistä fyysisesti eriytetty[3] tietojenkäsittely tähän tarkoitukseen varatulla

[1] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Turvallisuusselvityslaki (726/2014). Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011).

[2] Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille. 2020. URL: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf.

[3] Fyysinen eriyttäminen pienentää useita tietojenkäsittelyn luottamuksellisuuteen ja eheyteen liittyviä riskejä. Fyysinen eriyttäminen ei tyypillisesti pysty kuitenkaan korvaamaan muita päätelaitteen suojauksessa tarpeellisia menettelyjä, esimerkiksi vähimpien oikeuksien periaatteen mukaisia käyttöoikeuksia (Katakri 2020 / I-06) ja vain välttämättömän toiminnallisuuden mahdollistavia kovennuskäytäntöjä (Katakri 2020 / I-08).

päätelaitteella. Toteutustapana voi olla myös vastaavasti turva-alueella hajasäteilysuojattuun tilaan fyysisesti sijoitettu ja muista ympäristöistä fyysisesti eriytetty päätelaitteista, niitä yhdistävästä paikallisesta verkosta ja tähän tarkoitukseen varatusta erillistulostimesta koostuva tietojenkäsittely-ympäristö.

- Tiedonsiirto fyysisesti eriytettyihin ympäristöihin tulee toteuttaa siten, että riski turvallisuusluokan I tiedon kulkeutumiseen matalamman turvallisuusluokan ympäristöön saatetaan mahdollisimman pieneksi. Tyypillisenä toteutustapana on kertakäyttöisten optisten medioiden hyödyntäminen tiedonsiirroissa matalamman turvallisuusluokan ympäristöstä ylemmän turvallisuusluokan ympäristöön.

- Mikäli kansallisen turvallisuusluokan I tietojenkäsittely-ympäristö on toiminnallisten tarpeiden näkökulmasta ehdottoman välttämätöntä yhdistää matalamman turvallisuusluokan ympäristöön, tulisi yhdistäminen tapahtua turvallisuusluokalle I hyväksytyn yhdyskäytäväratkaisun kautta. Turvallisuusluokan I tietojenkäsittely-ympäristöjen erotteluun hyväksyttyjä yhdyskäytäväratkaisuja on saatavilla rajoitetusti, keskittyen tyypillisesti vain yksisuuntaisen liikennöinnin (TL II → TL I) mahdollistavien datadiodiratkaisujen moniportaisiin ratkaisumalleihin. Yhdyskäytäväratkaisuja on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen yhdyskäytäväratkaisuohjeessa[4].

- Kansainvälisen turvallisuusluokan I tietojenkäsittely-ympäristön yhdistäminen matalamman turvallisuusluokan ympäristöihin voi olla kiellettyä. Esimerkiksi EU:n turvallisuusluokitellun tiedon osalta EU TOP SECRET -turvallisuusluokiteltujen tietojen käsittelyyn hyväksytyn tietojärjestelmän välitön tai porrastettu yhteenliitäntä suojaamattoman tai julkisen verkon kanssa on kiellettyä (2013/488/EU, liite IV, kohta 36).

2.2 Salaus fyysisten turva-alueiden ulkopuolella tai matalamman turvallisuusluokan verkon kautta liikennöitäessä

Katakri 2020:n kohta I-01 ottaa kantaa turvallisuusluokan II tietojenkäsittely-ympäristöjen yhdistämiseen turvattoman verkon yli liikennöitäessä. Kohta I-15 ottaa kantaa puolestaan muuhun tiedon sähköiseen välittämiseen turva-alueiden ulkopuolella tai matalamman turvallisuusluokan verkon kautta liikennöitäessä. Sekä I-01 että I-15 huomioivat erityisesti riittävän luotettavan, hyväksytyn salausratkaisun (vrt. Katakri 2020 / I-12) merkityksen.

Lähtökohtaisesti turvallisuusluokan I tietojenkäsittely-ympäristöt suositellaan pidettäväksi fyysisesti eriytettyinä kaikista muista ympäristöistä ja rajattuina fyysisille turva-alueille. Mikäli kansallisen turvallisuusluokan I tietojenkäsittely-ympäristö on toiminnallisten tarpeiden näkökulmasta ehdottoman välttämätöntä yhdistää toiseen turvallisuusluokan I tietojenkäsittely-ympäristöön verkon kautta, tulee yhdistämisessä huomioida, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla erittäin rajoitetusti. Riittävän luotettavien salausratkaisujen puuttuminen voi estää myös muun turvallisuusluokan I tiedon sähköisen välittämisen verkon kautta. Tämä voi edellyttää turvallisuusluokan I tietojen siirtämiseen turvallisuusluokalle I hyväksytyn kuriirimenettelyn käyttöä tilanteissa, joissa turvallisuusluokan I tietoa on tarve siirtää fyysisten turva-alueiden välillä. On lisäksi huomioitavaa, että vaikka joitakin salauksen luotettavuuteen liittyviä riskejä voi olla mahdollista pienentää käyttämällä eri valmistajien turvallisuusluokalle II hyväksyttyjä salausratkaisuja sisäkkäin, tällainen menettely ei välttämättä tuota turvallisuusluokan I tiedoille riittävää suojausta siihen kohdistuvia riskejä vastaan.

[4] Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf.

3 Tietojärjestelmäturvallisuus

3.1 Jäljitettävyys ja poikkeamien havainnointikyky

Katakri 2020:n kohta I-10 ottaa kantaa turvallisuusluokan II tietojenkäsittelyn turvallisuuteen liittyvien tapahtumien jäljitettävyyteen ja kohta I-11 puolestaan poikkeamien havainnointikykyyn ja toipumiseen. Turvallisuusluokan I tietojen käsittelyssä suositellaan riskiperustaisesti turvallisuusluokkaa II pidempiä säilytysaikoja lokitiedoille (esimerkiksi vähintään 10 vuotta), sekä tehostettua poikkeamien havainnointikykyä, painottaen muun muassa tietojenkäsittely-ympäristön käyttäjien ja ylläpitäjien toiminnan seurantaa.

Turvallisuusluokan I tietojenkäsittely-ympäristöt ovat tyypillisesti suppeita, koostuen esimerkiksi kaikista verkoista pysyvästi irtikytketyistä päätelaitteista. Toisaalta esimerkiksi 10 vuoden lokikertymän säilyvyys on haastava toteuttaa uskottavasti vain päätelaitteilla, joten tällaisten päätelaitteiden lokienkeräys sekä kerättyjen lokitietojen varmistukset edellyttävätkin yleensä suunniteltua säännöllistä prosessia. Käytännön toteutustapana voi olla esimerkiksi lokitietojen säännöllinen kerääminen irtomedialle, jota käsitellään ja säilytetään sen elinkaaren ajan kuin turvallisuusluokan I tietoa. Lisäksi huomioitava, että mikäli tietojärjestelmän pääsynhallinta tai esimerkiksi toimien jäljitettävyys nojautuu fyysisen turvallisuuden menettelyihin, myös näistä syntyviä tallenteita saattaa olla perusteltua säilyttää ja hallinnoida turvallisuusluokan I mukaisilla menettelyillä.

3.2 Salausratkaisut

Katakri 2020:n kohta I-12 ottaa kantaa turvallisuusluokan II tietojenkäsittely-ympäristössä käytettäviin salausratkaisuihin. Fyysisten turva-alueiden ja matalamman turvallisuusluokan verkkojen yli liikennöinti on käsitelty luvussa 2.2.

Muissa tilanteissa, joissa turvallisuusluokan I tietojen suojaamiseen käytetään salausratkaisuja, esimerkiksi päätelaitteiden kiintolevyjen salaukseen tai eri tiedon omistajien tietojen erotteluun, suositellaan huomioitavaksi, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla äärimmäisen rajoitetusti. Tällaisissa tilanteissa salausratkaisut ovatkin lähtökohtaisesti vain tukevassa roolissa muille suojauksille, erityisesti fyysiselle pääsynhallinnalle.

3.3 Hajasäteilyltä suojautuminen

Katakri 2020:n kohta I-14 ottaa kantaa turvallisuusluokan II sähköisen tietojenkäsittelyn hajasäteilyyn (TEMPEST) ja elektroniselta tiedustelulta suojautumiseen. Turvallisuusluokan I tietojen suojaamisessa tulee huomioida turvallisuusluokan II tiedoista eroavat riskit ja suhteutettava nämä toteutettaviin turvatoimiin. Hajasäteilyä ja siltä suojautumisen periaatteita on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen hajasäteilyltä suojautumisen ohjeessa[5], jonka päivitetty versio pyritään julkaisemaan syksyn 2021 aikana.

4 Käyttöturvallisuus

4.1 Tiedon sähköinen välitys

Käsitelty luvuissa 2.2 ja 3.2. Erityisesti huomioitava, että turvallisuusluokan I tietojen suojaamiseen riittävän luotettavia, hyväksyttyjä salausratkaisuja on saatavilla erittäin rajoitetusti. Tämä edellyttääkin tyypillisesti turvallisuusluokan I tietojen siirtämistä turvallisuusluokalle I hyväksytyllä kuriirimenettelyllä tilanteissa, joissa turvallisuusluokan I tietoa on tarve siirtää fyysisten turva-alueiden välillä.

[5] Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kansallinen-TEMPEST.pdf.

4.2 Fyysinen turvallisuus ja etäkäyttö

Katakri 2020:ssa fyysisen turvallisuuden hallinnolliselle alueelle, turva-alueille sekä esimerkiksi kassakaapeille asetettavat vaatimukset on kuvattu F-osa-alueessa (ks. F-02, F-03 ja F-04). I-osa-alueessa kuvataan puolestaan sidonta sähköisen käsittelyn mahdollisuuksista F-osa-alueessa kuvatut vaatimukset täyttävillä turvallisuusalueilla, sekä niiden ulkopuolella etäkäytössä (ks. I-18).

Turvallisuusluokan I tietojen sähköisessä käsittelyssä tulee lisäksi huomioida, että turvallisuusluokan I tietoa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla (1101/2019[6], 10 §), mikä asettaa rajoitteet myös etäkäytön mahdollisuuksille.

4.3 Sähköisessä muodossa olevan tiedon tuhoaminen

Turvallisuusluokan I sähköisessä muodossa olevan tiedon tuhoamisessa voidaan hyödyntää Katakri 2020:een koottuja turvallisuusluokan II silppukokoja, mikäli suojausta täydennetään viranomaisen hyväksymillä menettelyillä. Tällaisia menettelyihin sisältyvät tyypillisesti muun muassa silpun jatkokäsittely valvotusti polttamalla tai sulattamalla.

5 Lisätietoa

1. Laki julkisen hallinnon tiedonhallinnasta (906/2019). URL: https://www.finlex.fi/fi/laki/ajantasa/2019/20190906.

2. Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). URL: https://www.finlex.fi/fi/laki/ajantasa/2019/20191101.

3. Neuvoston päätös EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU). URL: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32013D0488.

4. Kansallinen turvallisuusviranomainen. 2020. Katakri 2020 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf.

5. Tiedonhallintalautakunta. 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. URL: http://urn.fi/URN:ISBN:978-952-367-500-1.

6. Kyberturvallisuuskeskus. 2018. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf.

7. Kyberturvallisuuskeskus. 2016. Kiintolevyjen elinkaaren hallinta – Ylikirjoitus ja uusiokäyttö. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-ylikirjoitus.pdf.

8. Kyberturvallisuuskeskus. 2013. Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kansallinen-TEMPEST.pdf.

[6] Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). URL: https://www.finlex.fi/fi/laki/ajantasa/2019/20191101.