Ohje periaatteista useiden tietojärjestelmien sijoittamisesta samaan fyysiseen tilaan

1 Tausta

Tietojärjestelmien arviointeihin ja hyväksyntöihin liittyvistä Liikenne- ja viestintävirasto Traficomin tehtävistä säädetään laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki), turvallisuusselvityslaissa (726/2014) ja laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista (1406/2011, arviointilaki).

Liikenne- ja viestintäviraston hyväksyntää (akkreditointia) on mahdollista hakea tietojärjestelmissä käsiteltävien kansainvälisten turvallisuusluokiteltujen tietojen suojaamiseen. Liikenne- ja viestintäviraston arviointia on mahdollista hakea tietojärjestelmissä käsiteltävien kansallisten turvallisuusluokiteltujen tietojen suojaamiseen. Hyväksyntä- ja arviointiprosesseja on kuvattu yksityiskohtaisemmin ohjeessa tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista[1].

Kansallisen turvallisuusluokitellun tiedon ja sitä käsittelevien tietojärjestelmien riskienhallinta kuuluu lähtökohtaisesti kyseisen tietojärjestelmän omistavan viranomaisen (tiedonhallintayksikön) vastuulle[2]. Sen sijaan kansainvälisen turvallisuusluokitellun tiedon ja sitä käsittelevien tietojärjestelmien riskienhallinnan vastuut jakautuvat tyypillisesti myös tietojärjestelmän hyväksyntäviranomaiselle (SAA, Security Accreditation Authority), tietojärjestelmän omistajalle/vastuuviranomaiselle (CISOA, CIS Operational Authority) tai/ja tietojärjestelmän hyväksyntälautakunnalle (SAB, Security Accreditation Board).

Tietojärjestelmien arviointi- ja hyväksyntäprosesseissa on havaittu, että toisinaan voi olla tarve sijoittaa samaan fyysiseen tilaan useita tietojärjestelmiä. Tällaisiin voi sisältyä kansallisia kansallisen tai/ja kansainvälisen turvallisuusluokitellun tiedon käsittelyyn tarkoitettuja tietojärjestelmiä sekä yhden tai useamman kansainvälisen yhteisön toimittamia tietojärjestelmiä. Tässä ohjeessa kuvataan yleisimmät periaatteet, joiden täyttyessä eri tietojärjestelmien sijoittaminen samaan fyysiseen tilaan on toteutettavissa kohtuullisilla jäännösriskitasoilla.

2 Yleisiä riskejä ja hallintakeinoja

Eri tietojärjestelmiin liittyy eroavia toiminnallisuuksia ja riskejä. Joissain tietojärjestelmissä voi olla toiminnallisia tarpeita laitteille, jotka kykenevät esimerkiksi äänen (mikrofoni) tai kuvan (kamera) taltioimiseen ja välittämiseen. Tällaiset toiminnallisuudet voivat mahdollistaa myös tiedon valtuuttamattoman kulkeutumisen samassa fyysisessä tilassa olevien eri tietojärjestelmien välillä.

Eri tietojärjestelmät voivat olla myös eri tavoin suojattuja ja niihin voi olla pääsy eri henkilöillä tai ryhmillä. Esimerkiksi Internet-kytkentäiset tietojärjestelmät ja niiden toiminnallisuudet voivat olla täysin ulkopuolisten tahojen haltuun otettavissa ilman merkittävää osaamista tai resursointia[3]. Toisaalta esimerkiksi eri kansainvälisten yhteisöjen tietoja käsittelevät tietojärjestelmät voivat olla sellaisia, että niihin on etähallintayhteys kyseisten yhteisöjen

[1] Liikenne- ja viestintävirasto. 2025. Liikenne- ja viestintäviraston ohje tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohje-tietojarjestelmien-arviointi-ja-hyvaksyntaprosesseista-2025.pdf.
[2] 906/2011 13 §.
[3] Esimerkiksi mikäli tietojärjestelmän päätelaitteelle on mahdollista lähettää tietojärjestelmän ulkopuolelta, kuten Internetistä, sähköposti liitteineen, on kyseinen päätelaite ja tietojärjestelmä lähtökohtaisesti ulkopuolisten tahojen haltuun otettavissa.

toimijoilla. Useat videoneuvottelujärjestelmät ovat aktivoitavissa etähallintayhteyden kautta, kuten myös esimerkiksi päätelaitteiden mikrofonit ja kamerat.

Sekä kansallisiin että kansainvälisiin turvallisuusluokiteltuihin tietoihin kohdistuu velvoite suojata niitä sivullisilta ja antaa niihin pääsy vain tiedonsaantitarpeen mukaisesti[4]. Edellä kuvatut tietojärjestelmien ominaisuudet ja toisaalta eri henkilöiden tai ryhmien pääsy eri järjestelmiin voivat johtaa siihen, että turvallisuusluokitellut tiedot ovat saatavilla myös tietoon valtuuttamattomille, toisin sanoen sivullisille.

Tyypillisenä riskienhallintakeinona käytetään toimintamallia, jossa eri turvallisuusluokan ja eri omistajien/originaattorien tietoja käsittelevät tietojärjestelmät sijoitetaan erillisiin fyysisiin tiloihin. Toteutusmallina voi olla esimerkiksi se, että EU:n ja Naton SECRET-luokan videoneuvottelulaitteistot sijoitetaan omiin fyysisiin tiloihin, ja kansalliset tietojärjestelmät turvallisuusluokittain eri fyysisiin tiloihin. Erityisesti turvallisuusluokasta III/CONFIDENTIAL lähtien suojaamisessa korostuu myös edistyneiden hyökkäystekniikoiden käyttöön liittyvien riskien hallinta. Riskienhallintakeinot voivat liittyä esimerkiksi fyysisen tilan salakuuntelulta ja -katselulta suojautumiseen (mukaan lukien TSCM-suojaukset[5]) sekä hajasäteilyltä suojautumiseen (TEMPEST-vastatoimet). Tilanteissa, joissa samassa fyysisessä tilassa on useita tietojärjestelmiä, tulee edellä mainitut riskit huomioida myös tietojärjestelmien toiminnallisuuksien osalta.

3 Periaatteet tietojärjestelmien samaan tilaan sijoittamisessa

Tässä luvussa kuvataan yleisimmät periaatteet, joiden täyttyessä eri tietojärjestelmien sijoittaminen samaan fyysiseen tilaan voi olla toteutettavissa kohtuullisilla jäännösriskitasoilla. Liikenne- ja viestintävirasto tukee viranomaisia periaatteiden tulkinnassa, erilaisiin toimintamalleihin liittyvien riskien arvioinneissa sekä mahdollisten korvaavien suojausten vaikuttavuuden arvioinneissa.

Periaate 1: Eri tietojärjestelmien samaan tilaan sijoittamisesta on olemassa kirjallinen riskienarviointi.

- Riskienarvioinnin tulee huomioida sekä toiminnalliset tarpeet, että eri tietojärjestelmissä käsiteltävien tietojen suojaaminen sivullisilta.
- Riskienarvioinnissa tulee olla tunnistettuna sekä eri tietojärjestelmien tekniset ominaisuudet (uhkat, esimerkiksi käytettävissä oleva mikrofoni tai kamera sekä tahot keillä on mahdollisuus kyseistä ominaisuutta hyödyntää, esimerkiksi tietojärjestelmän ylläpito), että niiden pahantahtoisen hyödyntämisen todennäköisyys (usein arvioituna hyödyntämisen vaikeustason tukemana).

Periaate 2: Samaan fyysiseen tilaan sijoitettavista tietojärjestelmistä ja niihin kuuluvista laitteistoista on olemassa ajantasaiset kuvaukset ja kirjanpito.

- Kirjanpidosta on selvitettävissä esimerkiksi kaikki tilaan asennetut tietojärjestelmät, tietojärjestelmiin kuuluvat laitteet ja tehdyt kytkennät, sekä tietojärjestelmissä käytettävät ohjelmistot. Esimerkiksi joihinkin kansainvälisten yhteisöjen toimittamiin tietojärjestelmiin voi sisältyä muun muassa räkkikaappi, salauslaite, kytkin, palomuuri, työasema, hiiri, näppäimistö, näyttö, VoIP-puhelin ja tulostin.

[4] 1101/2019 10 §; 2013/488/EU, II liite, kohdat 17, 23–28; C-M(2002)49-REV1, liite D, kohdat 4-5, 8.1, 10, 12, 23.
[5] TSCM, Technical surveillance counter-measures.

Periaate 3: Mikäli missään tilaan sijoitettavassa tietojärjestelmässä ei ole salakatseluun/-kuunteluun soveltuvaa toiminnallisuutta[6], kyseiset tietojärjestelmät voidaan ilmeisten salakatselu/-kuunteluriskien näkökulmasta sijoittaa samaan fyysiseen tilaan. Tämä periaate pätee myös eri turvallisuusluokkien tietojärjestelmiin[7].

- Riittävä näyttö siitä, että tietojärjestelmissä ei tällaisia toiminnallisuuksia ole, voi olla saatavissa esimerkiksi kyseisten tietojärjestelmien arviointi- tai hyväksyntäprosessin (akkreditoinnin) kautta.

- Joissain tilanteissa voidaan hyödyntää myös toimintamallia, jossa salakatseluun/-kuunteluun soveltuvat laitteistot sijoitetaan tilan ulkopuolelle, ja tilaan tuodaan tietojärjestelmästä vain näyttö, näppäimistö ja hiiri.

Periaate 4: Mikäli yhdessäkin tilaan sijoitettavassa tietojärjestelmässä on salakatseluun/-kuunteluun soveltuvaa toiminnallisuutta[6] ja riski arvioidaan oleelliseksi (vrt. periaate 1), tulee olla käytössä toteutusmalli, jolla estetään tiedon näkyvyys/kuuluvuus tietojärjestelmien välillä ja siten valtuuttamattoman tiedon siirtyminen tietojärjestelmien välillä.

- Toteutusmallin tulee pystyä estämään esimerkiksi Naton turvallisuusluokitellun tiedon välittyminen vain kansallisen turvallisuusluokitellun tiedon suojaamiseen tarkoitettuun tietojärjestelmään, Naton ja EU:n turvallisuusluokiteltujen tietojen välittyminen keskenään sekä tietojen valtuuttamaton välittyminen eri turvallisuusluokkien tietojärjestelmien välillä. Kansallisen viranomaisen riskienhallinnassa tulee erityisesti huomioida menettelyt, joilla estetään kansallisen turvallisuusluokitellun tiedon välittyminen tietojärjestelmiin, jonne tiedon luovuttamista (releasability) ei ole hyväksytty.

- Toteutusmalli voi perustua esimerkiksi siihen, että tilassa käsitellään kerrallaan vain yhden tiedon omistajan/originaattorin tietoja ja että käsittelyn ajan muiden omistajien/originaattorien salakatseluun/-kuunteluun soveltuvia toiminnallisuuksia[6] sisältävät tietojärjestelmät pidetään sammutettuina, sähkönsyöttö katkaistuna ja mahdolliset akut irrotettuina. Tilassa voidaan tässä toimintamallissa järjestää esimerkiksi EU SECRET -luokan videokokous, kun mahdolliset muut tilassa olevat salakatseluun/-kuunteluun kykenevät tietojärjestelmät on saatettu sähköttömiksi. Suojaamisessa tulee huomioida myös muut mahdolliset laitteistot[8], jotka voivat sähköisesti yhdistää eri tietojärjestelmiä. Toinen yleinen toimintamalli on ääni- ja näköeristettyjen, tilan sisälle rakennettujen käsittelypisteiden hyödyntäminen.

- Toimintamalli tulee jalkauttaa henkilöstölle. Henkilöstölle tulee olla toimintamallista selkeä ohje, ohjeen tulee olla henkilöstölle tiedotettu tai/ja koulutettu selkeästi ja henkilöt tulee velvoittaa toimimaan ohjeistetun toimintamallin mukaisesti.

- Lisäksi tulee huomioida, että tilassa ei ole nähtävissä/kuultavissa muuta sellaista tietoa (esimerkiksi tietoa tilan suojauksista tai mahdollisia asiakirjoja), jota ei voida käytettävässä videokokouksessa tuoda esille. Näkyvyyteen liittyviä riskejä voidaan usein pienentää myös laitteistojen sijoittelulla ja esimerkiksi sermien tai muiden näköesteiden käytöllä.

[6] Salakatseluun tai/ja -kuunteluun soveltuvia toiminnallisuuksia ovat esimerkiksi kamera tai/ja mikrofoni.
[7] Samaan tilaan voi olla mahdollista sijoittaa esimerkiksi CONFIDENTIAL- ja SECRET-luokkien tietojärjestelmät, mikäli voidaan saada riittävä varmuus siitä, että näissä tietojärjestelmissä ei ole salakatseluun-/kuunteluun soveltuvia toiminnallisuuksia (esimerkiksi kameraa tai mikrofonia).
[8] Esimerkiksi KVM-laitteistot (engl. "Keyboard, Video, Mouse") ja HDMI-jakajat.

Periaate 5: Tilaan, jossa on turvallisuusluokan III/CONFIDENTIAL tai korkeamman luokan tietojärjestelmiä, ei tuoda matkapuhelimia, älykelloja tai vastaavia muita laitteita, joissa on tekninen toiminnallisuus salakuunteluun/-katseluun[9].

Periaate 6: Tilaan, jossa on turvallisuusluokan III/CONFIDENTIAL tai korkeamman luokan tietojärjestelmiä, ei asenneta langattomaan tiedonsiirtoon kykeneviä laitteistoja.

Periaate 7: Hajasäteilysuojaus huomioidaan turvallisuusluokasta III/CONFIDENTIAL lähtien. Samaan tilaan sijoitettavien laitteistojen asennuksissa ja sijoittelussa tulee huomioida riittävät etäisyydet sekä muut hajasäteilysuojaamisen edellytykset[10]. Hajasäteilysuojauksessa on huomioitava riittävät etäisyydet/vaimennukset myös mahdollisiin lähialueen tukiasemiin ja muihin langattomiin laitteisiin. Hajasäteilysuojausta on käsitelty yksityiskohtaisemmin Liikenne- ja viestintäviraston ohjeessa[11].

Periaate 8: Samaan tilaan itsenäisesti (ilman valvontaa) pääsevillä ihmisillä tulee olla voimassa olevat turvallisuusselvitykset ja henkilöturvallisuusselvitykset (PSC, Personnel Security Clearance) kaikille kyseisen tilan tietojärjestelmissä käsiteltäville tiedoille. Vaihtoehtoisesti henkilö tulee päästää tilaan vain saatettuna ja varmistuen siitä, että henkilö ei voi tilassa käynnin aikana nähdä tai kuulla muita kuin hänelle valtuutettuja tietoja.

- Esimerkiksi tilanteissa, joissa samassa tilassa on EU:n ja Naton SECRET-luokan tietojärjestelmät, tulee henkilöillä olla vähintään SECRET-luokan PSC sekä EU:n että Naton turvallisuusluokitellulle tiedoille.

- Esimerkiksi tilanteissa, joissa henkilö on valtuutettu vain kansallisen turvallisuusluokan II tietojen käsittelyyn, henkilö tulee päästää tilaan vain saatettuna ja tilassa ei saa olla nähtävillä/kuultavilla EU:n tai Naton turvallisuusluokiteltua tietoa henkilön tilassa käynnin aikana. Vastaavasti mikäli henkilöllä on PSC vain Naton turvallisuusluokitellulle tiedolle, tulee pääsy EU:n turvallisuusluokiteltuun tietoon estää.

Periaate 9: Tilanteissa, joissa on toiminnallinen tarve siirtää tietoa eri tietojärjestelmien välillä, tulee olla käytössä toteutusmalli, jolla tiedonsiirtoon liittyvät riskit saadaan hallittua.

- Toimintamalliin voi sisältyä esimerkiksi tiedonsiirto tulostamista ja skannaamista hyödyntäen tai nimettyjä siirtomedioita käyttäen. Toimintamallissa tulee olla huomioituna erityisesti haittaohjelmariskejä sekä inhimillisten virheiden riskejä pienentävät toimet.

- Toimintamalli tulee jalkauttaa henkilöstölle. Henkilöstölle tulee olla toimintamallista selkeä ohje, ohjeen tulee olla henkilöstölle tiedotettu tai/ja koulutettu selkeästi ja henkilöt tulee velvoittaa toimimaan ohjeistetun toimintamallin mukaisesti.

Periaate 10: Tilanteissa, joissa yhteen samassa tilassa käytettävään tietojärjestelmään kohdistuu sen turvallisuuteen tai/ja toiminnallisuuteen oleellinen muutos, tulee muutokseen liittyvät riskit arvioida ja hyväksyä myös muiden samassa tilassa olevien tietojärjestelmien suojaamisen näkökulmasta.

- Esimerkiksi mikäli tietojärjestelmään on tarve lisätä videoneuvottelutoiminnallisuus, tulee siitä aiheutuvat riskit arvioida ja hyväksyä myös muiden samassa tilassa olevien tietojärjestelmien suojaamisen näkökulmasta. Toiminnallisuuden lisääminen saattaa aiheuttaa tarpeen lisäsuojauksille esimerkiksi laitteiston sijoittelussa, toimintamalleissa

[9] Laitteiden tunnistamisessa tulee huomioida, että esimerkiksi äänen tai/ja kuvan tallentamiseen liittyviä ominaisuuksia on käytössä sekä kuluttajille suunnatuissa että myös lukuisissa viranomaiskäyttöön tarkoitetuissa laitteissa, kuten esimerkiksi erilaisissa viranomaiskäyttöön tarkoitetuissa puhelimissa.
[10] Hajasäteilysuojaamisen edellytyksiin sisältyy esimerkiksi sähkönsyötön puna-musta -erottelu.
[11] Liikenne- ja viestintävirasto. 2022. Kansallinen TEMPEST-ohje. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Kansallinen_TEMPEST-ohje_20220705.pdf.

tiedon välittymisen estämisessä (ks. periaate 3) tai salakuuntelulta ja -katselulta suojautumisen (mukaan lukien TSCM-suojaukset) arvioinneissa ja toteutuksissa.

- Yhteen tietojärjestelmään kohdistuva tai siihen vaikuttava poikkeama on tyypillisesti oleellinen tietojärjestelmän turvallisuuteen vaikuttava muutos, ja se tulee käsitellä edellä kuvattujen periaatteiden mukaisesti myös muiden samassa fyysisessä tilassa olevien tietojärjestelmien suojaamisen näkökulmasta. Esimerkiksi yhteen tietojärjestelmään kohdistunut tietomurto voi vaikuttaa myös muiden samassa fyysisessä tilassa olevien tietojärjestelmien riskeihin.
- Muutosten ja poikkeamien hallinnassa tulee huomioida myös eri tietojärjestelmiin liittyvät eroavat vastuut[12]. Muutosten ja poikkeamien käsittelyyn tulee osallistaa kaikki toimijat, joiden tietoihin tai joiden tietojärjestelmään muutoksella tai poikkeamalla voi olla vaikutusta.
- Tilanteissa, joissa samassa tilassa on vähintään yksi hyväksynnän (akkreditoinnin) piirissä oleva tietojärjestelmä, tulee muutoksista ja poikkeamista olla viipymättä yhteydessä myös hyväksynnän (akkreditoinnin), vaatimustenmukaisuuslausunnon (SoC, Statement of Compliance) tai puoltolausunnon (endorsement) myöntäneisiin viranomaisiin. Epäselvissä tilanteissa suositellaan olemaan välittömästi yhteydessä Liikenne- ja viestintävirastoon, joka tukee tilanteen selvittelyssä.

4 Ohjeen voimassaolo ja jatkokehitys

Ohje on voimassa toistaiseksi ja sitä päivitetään tarvittaessa. Kehitysehdotukset ja lisätietokyselyt pyydetään lähettämään osoitteeseen ncsa (at) traficom (piste) fi.

[12] Esimerkiksi kansallisen turvallisuusluokitellun tiedon ja sitä käsittelevien tietojärjestelmien riskienhallinta kuuluu lähtökohtaisesti kyseisen tietojärjestelmän omistavan viranomaisen (tiedonhallintayksikön) vastuulle. Sen sijaan kansainvälisen turvallisuusluokitellun tiedon ja sitä käsittelevien tietojärjestelmien riskienhallinnan vastuut jakautuvat tyypillisesti myös tietojärjestelmän omistajalle/hyväksyntäviranomaiselle (SAA, Security Accreditation Authority), tietojärjestelmän vastuuviranomaiselle (CISOA) tai/ja tietojärjestelmän hyväksyntälautakunnalle (SAB).