TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kansallinen TEMPEST-ohje

Traficomin julkaisuja

18/2022

Sisällysluettelo

1 Johdanto

Tietojärjestelmät tuottavat ympärilleen tahattomasti sähkömagneettista säteilyä eli hajasäteilyä, joka voi edetä ilmarajapinnassa, tietoliikennekaapeleissa, sähköverkossa tai muissa tahattomissa tiedonsiirtokanavissa. Hajasäteily voi olla ei-vaarantavaa, jolloin se ei sisällä turvallisuusluokiteltua tietoa (esim. kellosignaali). Vaarantava hajasäteily sisältää turvallisuusluokiteltua tietoa, josta voidaan sopivilla laitteilla tietyissä olosuhteissa selvittää ja tallentaa käsiteltävien tietojen sisältö. Tämä vaarantava hajasäteily voi aiheuttaa käsiteltävien tietojen luottamuksellisuuden menetyksen, mikäli säteilyä tallennetaan ja analysoidaan elektronisin tiedustelumenetelmin. Tässä dokumentissa termillä *hajasäteily* viitataan nimenomaan käsiteltävän tiedon vaarantavaan hajasäteilyyn.

Kansallinen lainsäädäntömme (1101/2019, 11 §) edellyttää, että käsiteltäessä turvallisuusluokan I–III asiakirjoja sähköisesti on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. Riskien pienentämiseksi toteutettavat tietoturvallisuustoimenpiteet on suhteutettava tietojen hyväksikäytön riskiin ja turvallisuusluokan tasoon.

Euroopan Unionin ja Naton turvallisuusluokiteltuun tietoon kohdistuvat hajasäteilyltä suojautumisen vaatimukset on kuvattu kyseisten yhteisöjen turvallisuussäännöissä. Turvallisuussäännöissä kuvataan tarkat vaatimukset esimerkiksi toimitiloille ja elektronisille laitteille hajasäteilyn vaimentamiseksi sekä tarvittaessa sen poistamiseksi. EU:n ja Naton soveltamat hajasäteilyn hallintatoimet perustuvat Naton luomaan standardiin, joka on esitetty Naton julkaisuissa SDIP-27, -28 ja -29. EU:n neuvoston vastaavat dokumentit ovat IASP7 sekä IASG 7-01, -02 ja -03.

Tässä ohjeessa kuvataan Suomen kansalliset erityisvaatimukset ja toimenpiteet, joilla hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä voidaan pienentää riittävästi. Ohje pohjautuu EU:n ja Naton turvallisuusluokiteltuihin tietoihin sovellettaviin hajasäteilyltä suojautumisen periaatteisiin. Ohjetta sovelletaan kansallisten turvallisuusluokiteltujen tietojen suojaamiseen. Kansainvälisiin turvallisuusluokiteltuihin tietoihin sovelletaan lähtökohtaisesti kansallisia vaatimuksia, mikäli kyseisen valtion tai yhteisön kanssa tehdyssä turvallisuussopimuksessa on määritelty vastavuoroisen suojaamisen periaatteet. Kuitenkin esimerkiksi EU:n ja Naton turvallisuusluokiteltujen tietojen suojaamisessa sovelletaan kyseisen yhteisön tietoihin kohdistuvia erityisvaatimuksia.

Tämä ohje on laadittu täydentämään viranomaisten auditointityökalu Katakrissa (2020) kuvattuja toimitilaturvallisuuden (F-osa-alue) ja tietojärjestelmäturvallisuuden (I-osa-alue) suojauksia sekä tukemaan organisaation muuta riskienhallintaa (T-osa-alue).

2 Keskeinen lainsäädäntö

Laki julkisen hallinnon tiedonhallinnasta (906/2019) määrittelee velvoitteita viranomaisille tietoaineiston turvallisuuden varmistamiseksi. Turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvallisuustoimenpiteistä säädetään tarkemmin valtioneuvoston asetuksessa 1101/2019.

3 Keskeiset käsitteet ja määritelmät

Vaarantava hajasäteily

Vaarantavalla hajasäteilyllä tarkoitetaan elektronisten laitteiden tuottamia turvallisuusluokiteltua tietoa tahattomasti sisältäviä signaaleja, joista voidaan sopivilla laitteilla ja sopivissa olosuhteissa selvittää käsiteltävän tiedon sisältö. Vaarantava hajasäteily voi edetä säteilevänä ilmarajapinnassa tai johtuvana tietoliikennekaapeleissa, sähköverkossa tai muissa tahattomissa tiedonsiirtokanavissa. Tässä dokumentissa hajasäteilyllä viitataan nimenomaan vaarantavaan hajasäteilyyn, jolla on sekä johtuva että säteilevä komponentti.

TEMPEST

TEMPEST–termi (Telecommunications Electronics Material Protected from Emanating Spurious Transmissions) on kehitetty Natossa ja sitä käytetään yleisesti kansainvälisissä yhteyksissä. TEMPEST–termi tarkoittaa vaarantavaan hajasäteilyyn kohdistuvia tarkastuksia, tutkimuksia, kontrollointia, tiedustelu-uhkaa vastaan suoritettavia vastatoimia ja vaarantavaa hajasäteilyä vaimentavia (tukahduttavia) toimia.

Toimivaltainen TEMPEST-viranomainen

EU:n turvallisuussääntöjen mukaan jokaisella EU-valtiolla tulee olla määrätty toimivaltainen TEMPEST-viranomainen. Toimivaltaisen viranomaisen tulee vastata siitä, että EU:n turvallisuusluokiteltua tietoa käsittelevät tietojärjestelmät ovat TEMPEST–periaatteiden ja suuntaviivojen mukaisia. TEMPEST-viranomainen hyväksyy EU:n turvallisuusluokiteltuun tietoon liittyvät ratkaisut, joilla hallitaan vaarantavan hajasäteilyn aiheuttamia tietojen turvallisuuteen liittyviä riskejä. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus toimii Suomessa lain kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttämässä viranomaistehtävässä ja on tässä ohjeessa tarkoitettu toimivaltainen TEMPEST-viranomainen.

4 TEMPEST-riskien arviointi- ja hyväksyntäprosessi

TEMPEST-riskien arviointi- ja hyväksyntäprosessi sisältää toimintaympäristöanalyysin, riskien arvioinnin, riskien käsittelyn, jäännösriskien hyväksymisen sekä riskien seurannan ja katselmoinnin. Ohjeen rakenne on identtinen siinä kuvatun riskienhallintaprosessin etenemisen kanssa:

KUVA 1: Kansallisen TEMPEST-ohjeen rakenne

Ennen riskienhallintaprosessin soveltamista on tärkeä tunnistaa prosessiin liittyvät vastuutahot. Riskienhallintaprosessin vastuut voidaan jakaa esimerkiksi alla olevan taulukon mukaisesti. Jäännösriskin lakisääteisen hyväksyjätahon vastuumäärittely ei kuitenkaan ole muutettavissa.

TIETO	TIEDON KÄSITTELYPAIKKA	RISKIEN ARVIOIJATAHO	JÄÄNNÖSRISKIEN HYVÄKSYJÄTAHO
Kansallinen turvallisuus-luokiteltu tieto	Tietoon määräämisvallassa olevan viranomaisen (tiedonhallintayksikkö, "tiedon omistaja") kiinteistö/järjestelmä	Tietoon määräämisvallassa oleva viranomainen (tiedonhallintayksikkö, "tiedon omistaja")	Tietoon määräämisvallassa oleva viranomainen (tiedonhallintayksikkö, "tiedon omistaja")
Kansallinen turvallisuus-luokiteltu tieto	Tietoon määräämisvallassa olevan viranomaisen (tiedonhallintayksikkö, "tiedon omistaja") sidosryhmän kiinteistö/järjestelmä	Tietoon määräämisvallassa olevan viranomaisen (tiedonhallintayksikkö, "tiedon omistaja") sidosryhmä	Tietoon määräämisvallassa oleva viranomainen (tiedonhallintayksikkö, "tiedon omistaja")
Kansainvälinen erityissuojattava tietoaineisto	Tiedon käsittelijän kiinteistö/järjestelmä	Tiedon käsittelijä	Kansallinen TEMPEST-viranomainen

TAULUKKO 1: Jäännösriskien hyväksyntävastuut suojattaville tietoaineistolle

Kansallisen turvallisuusluokitellun tiedon osalta kukin viranomainen on itse vastuussa tietojenkäsittelynsä turvallisuudesta ja voi riskienarviointinsa (906/2019, 13 §) perusteella hyväksyä tietojärjestelmänsä määrittämänsä turvallisuusluokan tietojen käsittelyyn, kattaen myös hajasäteilyyn liittyvien riskien hallinnan. Kansallinen TEMPEST-viranomainen voi pyydettäessä antaa neuvontaa kansallisille viranomaisille.

4.1 TEMPEST-riskien arvioiminen (tunnistaminen ja analyysi)

TEMPEST-riskien arviointi on kokonaisprosessi, joka kattaa TEMPEST-riskien tunnistamisen, -riskianalyysin ja -riskien merkityksen arvioinnin. Arvioinnin perusteella TEMPEST-riskit voidaan asettaa tärkeysjärjestykseen. Merkittäviä kustannuksia aiheuttavien riskienhallintatoimenpiteiden tilalle voi olla mahdollista löytää kustannustehokkaampia ratkaisuja.

Arviointivastuu on turvallisuusluokiteltuun tietoon määräämisvallassa olevalla viranomaisella (tiedonhallintayksikkö, "tiedon omistaja"), joka valitsee arviointiin sopivimman toimintamallin. Arvioinnissa on tärkeää käyttää menetelmää, joka koetaan vaivattomaksi, johon voidaan luottaa ja joka tuottaa toistettavia tuloksia.

4.1.1 Turvallisuusluokiteltujen tietojen ja turvallisuusalueiden tunnistaminen

Tietoon määräämisvallassa olevan viranomaisen, tiloja hallinnoivan tai sen turvallisuudesta vastaavan organisaation avustuksella, on tunnistettava suojattavat tiedot ja käsittelytilat.

Turvallisuusluokiteltua tietoa käsittelevän organisaation tulee tunnistaa:

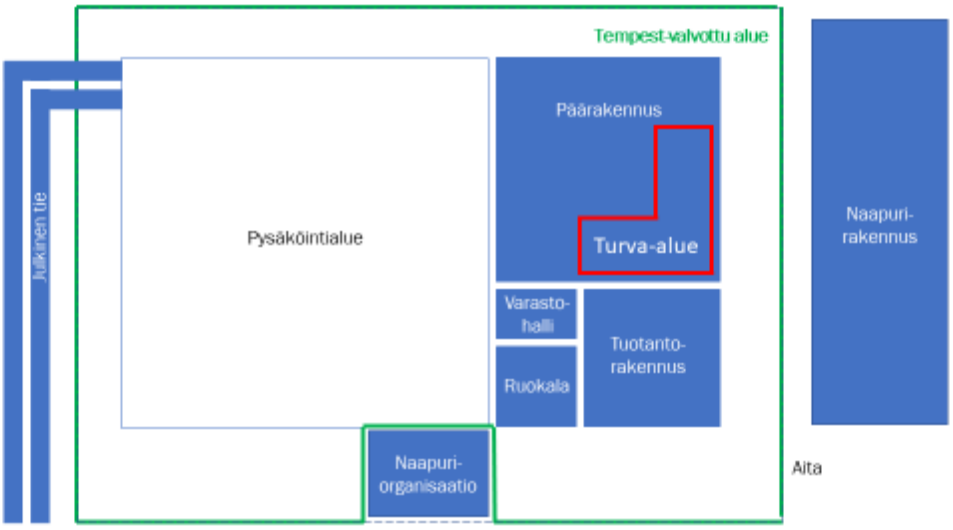
- turvallisuusluokitellut tiedot
- tietojärjestelmät, jotka sisältävät turvallisuusluokiteltua tietoa
- turvallisuusalueet, joissa turvallisuusluokiteltua tietoa sisältävät tietojärjestelmät sijaitsevat
- ja määritellä TEMPEST-valvottu alue.

Organisaation tulee ensin tunnistaa ja luokitella suojattavat tiedot (TL I – TL III). TEMPEST-riskien arviointia ei tarvitse soveltaa turvallisuusluokkaan KÄYTTÖ RAJOITETTU (TL IV) luokitellun tiedon suojaamiseksi. Tietojen luokittelun lisäksi tulee tunnistaa tietojärjestelmät sekä niiden osat, joissa turvallisuusluokiteltua

tietoa käsitellään. Tunnistaminen tulisi tehdä työryhmässä, johon kuuluu esimerkiksi tietohallinnosta, operatiivisesta toiminnasta ja turvallisuudesta vastaavia henkilöitä.

Lisäksi tulee tunnistaa turvallisuusalueet (1101/2019, 9§; Katakri 2020, F-04), joilla tietojärjestelmät ja tietoliikennejärjestelyt sijaitsevat. Tunnistamisen ja alueiden määrittämisen apuna voi käyttää Katakri 2020:n F-04-vaatimustaulukkoa. Tunnistamisen jälkeen tulee määritellä TEMPEST-valvottu alue. TEMPEST-valvottu alue tulee suunnitella tai määritellä niin, että alueen sisällä ei myöhemmin kuvatun elektronisen tiedustelu-uhan rakentaminen ole mahdollista tai jonka sisällä organisaatiolla on kyky tunnistaa ja oikeus poistaa TEMPEST-uhka.

TEMPEST-valvottu alue voidaan havainnollistaa riskien arvioinnin ja mahdollisen TEMPEST-mittauksen tueksi piirtämällä pohjapiirros, johon on merkitty tietojärjestelmät ja tietoliikennejärjestelyt sekä TEMPEST-valvottu alue. Esimerkki havainnollistuksesta on esitetty kuvassa 2.



KUVA 2: Tietojärjestelmät ja tietoliikennejärjestelyt sekä TEMPEST-valvottu alue

4.1.2 Elektronisten tiedustelu-uhkien tunnistaminen

Hajasäteilyä hyödyntävä elektroninen tiedustelu on pitkäkestoista, samassa tai läheisessä kiinteistössä tapahtuvaa peitetoimintaa. Edellä kuvattu toiminta voi tapahtua kiinteistön sijaan myös esimerkiksi lähiympäristöön pysäköidyssä ajoneuvossa. Tiedustelija voi hyödyntää sekä ilmarajapinnassa säteilevänä että tietoliikenne- tai sähköverkossa johtuvana etenevää hajasäteilyä. Tiedustelutoiminta ei tyypillisesti jätä jälkiä, jolloin sitä on usein erittäin vaikea tai jopa mahdotonta havaita tai tutkia jälkikäteen.

Elektroniset tiedustelu-uhat tulisi tunnistaa vähintään yleisellä tasolla. Uhan toteutumisen todennäköisyyteen vaikuttaa muun muassa se, miten houkutteleva käsiteltävä turvallisuusluokiteltava tieto on ja millainen on arvioidun uhan kyky elektroniseen tiedusteluun. Tiedon omistajan vastuulla, tiloja hallinnoivan tai sen turvallisuudesta vastaavan organisaation avustuksella, on elektronisten tiedustelu-uhkien tunnistaminen.

Uhkien tunnistamisvaiheen yhteydessä voidaan merkitä potentiaaliset tiedustelupisteet pohjapiirrokseen (vrt. kuva 2 edellä), johon on jo merkitty tietojärjestelmät sekä TEMPEST-valvottu alue. Potentiaalisten tiedustelupisteiden merkitseminen mahdollistaa järjestelmällisen lähestymistavan haavoittuvuuksien

arvioimiseen. Potentiaalisten tiedustelupisteiden tunnistamisessa ja valinnassa tulee huomioida nykyteknologian mahdollisuudet. Tiedusteluun tarvittavia laitteistoja voi nykyteknologian avustamana olla mahdollista kuljettaa esimerkiksi kiinteistön katolle. Tiedustelupisteiden tunnistamisessa ja valinnassa tulee huomioida luonnollisesti myös muut mahdolliset kiinteistöjen eri kerroksissa sekä niiden välillä sijaitsevat tilat, joihin pääsyä organisaatio ei pysty luotettavasti hallinnoimaan.

4.1.3 Olemassa olevien TEMPEST-riskienhallintakeinojen tunnistaminen

Tarpeettoman työn ja tarpeettomien kustannusten välttämiseksi on suositeltavaa ensin tunnistaa jo olemassa olevat hallintakeinot. Sellaisia ovat esimerkiksi tietojärjestelmiä ympäröivät rakenteet tai kiinteistön valvontajärjestelyt. Käytössä olevia hallintakeinoja voi tunnistaa muun muassa tutustumalla aiempaan TEMPEST-riskien arviointidokumentaatioon tai mittausraportteihin sekä tarkastamalla, mitkä hallintakeinot on jo otettu käyttöön ja vertaamalla keinoja muun muassa tässä ohjeessa käsiteltyihin menetelmiin.

4.1.4 TEMPEST-haavoittuvuuksien tunnistaminen

Säteilevänä etenevä hajasäteily läpäisee – riippuen materiaalista – rakenteet ja etenee ilmarajapinnassa, jolloin turvallisuusluokiteltu tieto on mahdollisesti tiedusteltavissa TEMPEST-valvotun alueen ulkopuolella. Ilmarajapinnassa etenevän hajasäteilyn yleisimpiä lähteitä ovat video- ja äänikortit, monitorit ja muut esityslaitteet, näppäimistöt, tulostimet sekä erityisesti näiden kaapeloinnit, jotka toimivat antenneina. Tahattomina tiedonsiirtokanavina voivat toimia esimerkiksi ilmanvaihtokanavat.

Tietojärjestelmien tahattomasti ympäristöönsä tuottama sähkömagneettinen säteily voi kytkeytyä (indusoitua) lähellä kulkevaan tietoliikenne- tai sähköverkon kaapeliin, jota pitkin johtuva hajasäteily etenee TEMPEST-valvotun alueen ulkopuolelle ja on näin tiedusteltavissa. Tietoliikennekaapeloinnin kautta tapahtuvaan johtumiseen liittyen yleisimpiä haavoittuvuuksia ovat kuparikaapelit, puhelinlinjat, faksit ja lähiverkon infrastruktuuri. Lisäksi hajasäteily voi välittyä tietojärjestelmän omaan, tai sen lähellä kulkevaan, sähköverkkoon.

Säteileviä haavoittuvuuksia voidaan tunnistaa joko tekemällä etäisyyksiin perustuva analyysi tai suorittamalla turvallisuusalueelle TEMPEST-mittaus. Turvallisuusalueet, tai niiden osat, luokitellaan ensisijaisesti etäisyyksiin perustuvan analyysin perusteella taulukon 2 mukaisesti TEMPEST-tilavyöhykkeiksi (0–3). Mikäli etäisyysvaatimus ei täyty, voidaan turvallisuusalueelle suorittaa TEMPEST-mittaus, jolla määritetään kohteen tuottama vaimennus valvotun alueen ulkopuolelle ja tätä kautta kohteen TEMPEST-tilavyöhyke taulukon 2 mukaisesti. TEMPEST-jäännösriskin hyväksyjä päättää, edellytetäänkö mittausten suorittamista haavoittuvuuksien tunnistamiseksi.

Johtuvat haavoittuvuudet liittyvät toteutettuihin asennusratkaisuihin ja tähän liittyvien ohjeiden noudattamiseen. Johtuvat haavoittuvuudet tunnistetaan suorittamalla kohteeseen asennus- ja tietojärjestelmäkokonaisuuden tarkastus.

TEMPEST-TILAVYÖHYKE	ETÄISYYSVAATIMUS	VAIMENNUSVAATIMUS
3	Etäisyys tietojärjestelmästä TEMPEST-valvotun alueen rajalle on vähintään 1000 m	Mitattu vaimennus kohteesta TEMPEST-valvotun alueen rajalle vähintään 34 dB verrattuna referenssimittaukseen
2	Etäisyys tietojärjestelmästä TEMPEST-valvotun alueen rajalle on vähintään 100 m, mutta alle 1000 m	Mitattu vaimennus kohteesta TEMPEST-valvotun alueen rajalle vähintään 14 dB, mutta alle 34 dB verrattuna referenssimittaukseen
1	Etäisyys tietojärjestelmästä TEMPEST-valvotun alueen rajalle on vähintään 20 m, mutta alle 100 m	Mitattu vaimennus kohteesta TEMPEST-valvotun alueen rajalle vähintään 0 dB, mutta alle 14 dB verrattuna referenssimittaukseen
0	Etäisyys tietojärjestelmästä TEMPEST-valvotun alueen rajalle on alle 20 metriä	Mitattu vaimennus kohteesta TEMPEST-valvotun alueen rajalle alle 0 dB verrattuna referenssimittaukseen

TAULUKKO 2: TEMPEST-tilavyöhykkeet sekä etäisyys- ja vaimennusvaatimukset

Edellä taulukossa 2 sarakkeessa *Etäisyysvaatimus* on kerrottu vaadittu etäisyys tietojärjestelmistä TEMPEST-valvotun alueen rajalle. Sarakkeessa *Vaimennusvaatimus* on kerrottu TEMPEST-mittauksella todennettava vaimennusarvo mitattavasta kohteesta TEMPEST-valvotun alueen rajalle verrattuna referenssimittaukseen.

4.1.5 TEMPEST-riskianalyysi

TEMPEST-riskianalyysillä tarkoitetaan prosessia, jolla pyritään määrittämään TEMPEST-riskitaso riskien seurausten vaikutukseen ja todennäköisyyteen perustuen. TEMPEST-riskien seurausten vaikutusten (vahingon) arvio perustuu erityisesti käsiteltävän tiedon turvallisuusluokkaan. Vaikutus määritellään turvallisuusluokitteluasetuksen (3§) mukaisen vahinkolausekkeen perusteella.

TEMPEST-riskien todennäköisyyden arvioinnissa tulee ottaa huomioon, kuinka todennäköisesti elektronista tiedustelua toteutetaan ja miten helposti tunnistettuja haavoittuvuuksia voidaan käyttää hyväksi huomioon ottaen:

- turvallisuusluokitellun tiedon merkitys arvioidulle tiedustelijalle
- tiedustelijan kyky suorittaa elektronista tiedustelua
- tiedustelijan riskinottohalu

TEMPEST-riskien seurausten ja todennäköisyyden arvioinnin jälkeen voidaan arvioida TEMPEST-riskien merkitys. Merkityksen arvioinnissa tehtävien päätösten tulisi perustua organisaation muuhun riskienhallintaan ja asetettuihin riskikriteereihin. Riskit voidaan merkityksen arvioinnin jälkeen esimerkiksi luetteloida riskien hallintakeinojen kustannustehokkaaksi kohdentamiseksi.

TURVALLISUUSLUOKKA	RISKIN SEURAUSTEN VAIKUTUS
TL I ERITTÄIN SALAINEN	Erityisen suuri vahinko
TL II SALAINEN	Merkittävä vahinko
TL III LUOTTAMUKSELLINEN	Vahinko

TAULUKKO 3: Vaikutusten arviointitaulukko

4.2 TEMPEST-riskien käsittely

Turvallisuusluokitteluasetuksen (1101/2019, 11§) mukaan TEMPEST-riskien pienentämiseksi toteutettavat turvallisuustoimenpiteet on suhteutettava tietojen hyväksikäytön riskiin ja turvallisuusluokan tasoon. TEMPEST-riskien käsittelyvaihtoehdot olisi valittava riskien arvioinnin tulosten sekä käsittelyvaihtoehtojen toteuttamisesta odotettavissa olevien kustannusten ja hyötyjen perusteella.

Sellaiset käsittelyvaihtoehdot olisi toteutettava, joilla TEMPEST-riskejä on mahdollista pienentää merkittävästi mahdollisimman alhaisin kustannuksin.

Yleisesti ottaen TEMPEST-riskien taso olisi pyrittävä saamaan mahdollisimman vähäiseksi huolimatta tarkoista etäisyys- tai vaimennusvaatimuksista. On kuitenkin tarkasteltava myös todennäköisyydeltään harvinaisia, mutta vakavia TEMPEST-riskejä. Tällaisissa tilanteissa saatetaan joutua toteuttamaan riskien hallintakeinoja (esimerkiksi suojatun tilan rakentaminen tai tietojen käsittely TEMPEST-suojatuilla laiteratkaisuilla), jotka eivät välttämättä ole perusteltuja pelkästään taloudellisin perustein. Tällainen tilanne voi syntyä esimerkiksi silloin, kun turvallisuusluokiteltua tietoa joudutaan käsittelemään maissa, joissa elektronisen tiedustelun uhkataso on korkeampi.

Jos tietty TEMPEST-riski arvioidaan liian suureksi tai käsittelyvaihtoehtojen kustannukset ovat hyötyjä suuremmat, voidaan riski päättää vältettäväksi esimerkiksi pidättäytymällä kokonaan käsittelemästä turvallisuusluokiteltua tietoa tietyissä osissa kiinteistöä tai tietyissä tietojärjestelmissä. Kustannustehokkain ratkaisu tällaisessa tilanteessa saattaa olla kohteena olevien tietojärjestelmien siirtäminen paikkaan, jossa riskiä ei ole tai se on hallittu (esimerkiksi suojattu tila).

4.2.1 Ilmarajapinnassa etenevään hajasäteilyyn liittyvät hallintatoimenpiteet

Ilmarajapinnassa säteilevänä etenevä hajasäteily on sähkömagneettista säteilyä, joka vaimenee etäisyyden funktiona. Etäisyyden lisäksi etenemiseen vaikuttavat erilaiset fyysiset esteet, kuten rakenteet ja rakennukset. Erilaisilla rakenteilla on erilaiset vaimennusominaisuudet, joita voidaan kuvata seuraavilla esimerkeillä:

- Lasi vaimentaa vähemmän kuin muurattu tiiliseinä, mikä taas puolestaan vaimentaa vähemmän kuin teräs. Näin ollen ikkunaton huone on aina suositeltavampi hajasäteilyn vaimentamisen kannalta kuin ikkunallinen.
- 20 senttimetrin materiaalipaksuus (esim. tiili tai betoni) vaimentaa enemmän kuin samasta aineesta koostuva 10 senttimetrin materiaalipaksuus. Kaksi seinää vaimentaa siis enemmän kuin yksi. Tiedon käsittelyalue kannattaa näin ollen sijoittaa mieluiten rakennuksen sisäosiin.

Toimintojen sijoittelu rakennuksen eri osiin kannattaa suunnitella sekä suhteessa rakennuksen rakenteisiin, että TEMPEST-valvottuun alueeseen. Turvallisuusluokitellun tiedon käsittely kannattaa sijoittaa tilaan, josta on mahdollisimman suuri etäisyys TEMPEST-valvotun alueen rajalle tai määriteltyyn TEMPEST-uhkapisteeseen. Lisäksi turvallisuusluokitellun tiedon käsittely kannattaa sijoittaa mahdollisimman kauas ikkunoista, mielellään ikkunattomaan tilaan useamman rakenteen taakse. Edellä mainittuja asioita arvioitaessa tulee ottaa huomioon, että turvallisuusalueella olevat kaapelit, ilmanvaihtoputket, vesijohdot, raudoitukset, jne. voivat toimia hajasäteilyä johtavina johtimina.

TEMPEST-riski voidaan hallita sijoittamalla tietojärjestelmät ja tietoliikennejärjestelyt soveltuvalle TEMPEST-tilavyöhykkeelle. TEMPEST-riskejä voi hallita myös käyttämällä erityisvalmisteisia TEMPEST-laitteita. Taulukossa 4 kuvatun TEMPEST-tilavyöhykkeen perusteella voidaan määritellä, voidaanko tilassa käyttää kaupallisia TEMPEST-suojaamattomia tietojärjestelmiä ja tietoliikennejärjestelyjä (COTS, commercial-off-the-shelf) vai tuleeko käyttää erityisiä TEMPEST-suojattuja laitteita (TEMPEST-laiteluokka C–A).

	LAITESUOJALUOKKA			
TIEDON TURVALLISUUS -LUOKKA	COTS	Laiteluokka C	Laiteluokka B	Laiteluokka A
TL I	tapauskohtainen arvio			
TL II	TEMPEST-tilavyöhyke 3	TEMPEST-tilavyöhyke 2	TEMPEST-tilavyöhyke 1	TEMPEST-tilavyöhyke 0
TL III	TEMPEST-tilavyöhyke 2	TEMPEST-tilavyöhyke 1	TEMPEST-tilavyöhyke 0	TEMPEST-tilavyöhyke 0

TAULUKKO 4: Kansalliset tiedon turvallisuusluokat ja TEMPEST-laitesuojaluokat

4.2.2 Johtuvana etenevään hajasäteilyyn liittyvät hallintatoimenpiteet

Johtuvana etenevä hajasäteily syntyy, kun tietojärjestelmän tahattomasti ympäristöönsä tuottama sähkömagneettinen säteily indusoituu järjestelmän lähellä kulkevaan tietoliikenne- tai sähköverkon kaapeliin. Haavoittuvuus voi syntyä joko tietojärjestelmien osien (laitteiden tai vastaavien) sisällä komponenttitasolla tai osien (laitteiden, kaapelointien tai vastaavien) välillä.

Johtuvaan hajasäteilyyn liittyviä riskejä hallitaan hyödyntämällä niin sanottua puna-musta-erottelua, jossa sellaiset sähkö- ja elektroniikkapiirit, komponentit ja järjestelmät, jotka käsittelevät turvallisuusluokiteltua tietoa salaamattomassa muodossa (PUNAINEN), erotetaan niistä, jotka käsittelevät salattua tai luokittelematonta tietoa (MUSTA). Tämän konseptin mukaisesti termejä PUNAINEN ja MUSTA käytetään selkeyttämään ja erottamaan eri piirejä, komponentteja, laitteita ja järjestelmiä. Terminologia tekee eron myös niiden fyysisten tilojen välillä, joihin tekniikka on sijoitettu.

Punaisia komponentteja ovat muun muassa:

- kaapelit, jotka kuljettavat turvallisuusluokiteltua tietoa salaamattomana
- laitteet ja järjestelmät, jotka käsittelevät turvallisuusluokiteltua tietoa salaamattomana mukaan lukien salausjärjestelmät
- laitteet ja järjestelmät, jotka toimivat siirtopisteenä punaisen ja mustan komponentin välillä
- tilat, jotka sisältävät edellä mainittuja komponentteja.

Mustia komponentteja ovat muun muassa:

- kaapelit, jotka kuljettavat luokittelematonta tietoa tai turvallisuusluokiteltua tietoa salattuna
- laitteet ja järjestelmät, jotka käsittelevät ainoastaan luokittelematonta tietoa tai turvallisuusluokiteltua tietoa salattuna mukaan lukien salausjärjestelmien salatut ulostulot

- sähkönjakelujärjestelmät sisältäen paikallisakustot ja teholähteet
- tilat, jotka sisältävät ainoastaan edellä mainittuja komponentteja.

Erottelu tapahtuu käytännössä sijoittamalla punaiset ja mustat komponentit tietyn etäisyyden päähän toisistaan. Etäisyysvaatimus riippuu muun muassa tiedon turvallisuusluokasta sekä turvallisuusalueen TEMPEST-tilavyöhykkeestä. Siirron ja tallenteiden osalta suositeltavin tapa on kuitenkin pitää sähköisessä muodossa olevat turvallisuusluokitellut tiedot salattuina käyttäen kyseessä olevalle turvallisuusluokalle riittävän luotettavaa salausta, jolloin edellä mainittuja menettelyjä ei tarvita.

4.2.3 Suojattu tila

Mikäli TEMPEST-riskiä ei voida riittävästi hallita muilla riskien käsittelykeinoilla, on tarvittaessa käytettävä suojattua tilaa. Suojattu tila on johtavasta materiaalista rakennettu suljettu tila, joka tuottaa sähkömagneettisen vaimennuksen ulko- ja sisätilojen välillä. Tällaista tilaa kutsutaan yleensä Faradayn häkiksi. Maanalaiset tai EMP-vahvennetut tilat voivat lähtökohtaisesti tarjota vastaavan suojan.

Toimittaessa suojatussa tilassa voidaan parhaassa tapauksessa muista TEMPEST-riskien käsittelykeinoista luopua.

4.3 TEMPEST-jäännösriskien hyväksyntä

TEMPEST-jäännösriskeillä tarkoitetaan tunnistetuille riskeille toteutettujen hallintakeinojen jälkeen jäljelle jääviä riskejä. TEMPEST-jäännösriskien hyväksymisestä päättää:

- Kansallisen suojattavan tiedon osalta tiedonhallintalain (906/2019) mukainen viranomaisen tiedonhallintayksikkö ("tiedon omistaja")
- Kansainvälisen erityissuojattavan tiedon osalta kansallinen TEMPEST-viranomainen tai sopimuksella Suojelupoliisi tai Pääesikunta, jos järjestely on tarpeen TEMPEST-tehtävien hoitamiseksi tarkoituksenmukaisesti, taloudellisesti ja joutuisasti (588/2004, 5 §)

Hyväksymispäätöksen tietyn TEMPEST-riskin säilyttämisestä olisi perustuttava riskin merkityksen arviointiin. TEMPEST-jäännösriskien hyväksyjä saattaa joutua hyväksymään myös riskejä, jotka eivät täytä tavanomaisia hyväksymiskriteerejä, kuten esimerkiksi etäisyysvaatimuksia. Jos tällainen hyväksyminen on perusteltua ja välttämätöntä, päätöksentekijän olisi selkeästi todettava kyseinen TEMPEST-riski ja perusteltava siihen liittyvä päätös ohittaa tavanomaiset riskien hyväksymiskriteerit.

Yleisenä jäännösriskinä voidaan hyväksyä ratkaisu, jossa suojaamaton tietojärjestelmä tai tietoliikennejärjestely (esimerkiksi päätelaite) vaihtaa sijaintiaan vähintään 60 päivän välein. Sijainti katsotaan vaihtuneeksi, jos tietojärjestelmän tai tietoliikennejärjestelyn sijainti muuttuu vähintään yhden kilometrin edellisestä sijainnista. Tällaista jäännösriskiä ei kuitenkaan voida hyväksyä EU:n tai Naton SECRET-luokan tiedolle.

5 TEMPEST-riskien seuranta ja katselmointi

TEMPEST-riskejä ja niiden osatekijöitä (turvallisuusluokiteltuja tietoja, tietojärjestelmiä, tietoliikennejärjestelyjä, TEMPEST-uhkia, -haavoittuvuuksia ja toteutumistodennäköisyyksiä) olisi seurattava ja katselmoitava, jotta kaikki

organisaation toimintaympäristön muutokset voidaan tunnistaa riittävän varhaisessa vaiheessa ja TEMPEST-riskeihin liittyvää yleiskuvaa voidaan ylläpitää. Organisaation olisi varmistettava, että se seuraa jatkuvasti muutoksia tietojärjestelmissä ja tietoliikennejärjestelyissä:

- uusia uhkia
- mahdollisuutta, että uhkat voivat hyödyntää uusia haavoittuvuuksia
- muutoksia kansallisessa TEMPEST-ohjeessa

TEMPEST-riskien arviointi tulisi tehdä tarvittavassa laajuudessa uudelleen edellä mainituissa seurantakohteissa tapahtuneiden muutosten johdosta tai muussa tapauksessa osana organisaation muuta riskienhallintaprosessia. Seuranta tulisi kohdistaa erityisesti tilanteisiin, joissa hajasäteilyltä erikoissuojattuja laitteita on huollettu. Osana TEMPEST-riskien arviointia kohteelle voidaan suorittaa haavoittuvuuksien uudelleenarviointi, mikäli turvallisuusalueella on tapahtunut sellaisia muutoksia, joilla voidaan olettaa olevan vaikutusta kohteen haavoittuvuuksiin. Suojatun tilan suorituskyky tulee varmentaa, mikäli tilaan on tehty sellaisia muutoksia, joilla voidaan olettaa olevan vaikutusta tilan suojaukseen. Kansallisen turvallisuusluokitellun tiedon omistaja päättää, edellyttääkö haavoittuvuuksien uudelleenarviointi tai suojatun tilan suorituskyvyn varmentaminen TEMPEST-mittausten suorittamista.

6 Ohjeen laadinta ja ylläpito

Tämän ohjeen ylläpidosta vastaa Traficomin Kyberturvallisuuskeskus. Mahdollisista puutteista pyydetään olemaan yhteydessä Kyberturvallisuuskeskukseen (ncsa@traficom.fi).

Tämän ohjeen valmisteluun ja laatimiseen on osallistunut henkilöitä seuraavista organisaatioista:

- Jukka Seppälä, Ulkoministeriö
- Ville Jääskeläinen, Suojelupoliisi
- Samu Koski, Puolustusvoimat
- Jarno Kilpinen, Puolustusvoimat
- Annina Aromäki, Puolustusvoimat
- Tommi Seppälä, Puolustusvoimat
- Aki Tauriainen, Liikenne- ja viestintävirasto
- Teemu Ruhanen, Liikenne- ja viestintävirasto
- Jari Rautiokoski, Liikenne- ja viestintävirasto

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus

PL 320, 00059 TRAFICOM
p. 029 534 5000

kyberturvallisuuskeskus.fi

ISBN 978–952–311–808–9
ISSN 2669–8757 (netti)

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus