LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

TEMPEST-hyökkäykset ja suojautumiskeinot

Velemir, Jokso Juhana

2018 Laurea

Kiitokset

Tie tämän opinnäytetyön valmistumiseen on ollut pitkä ja haastava. Työn aiheen ollessa sensitiivinen pelkästään työn kunnolla käynnistyminen vei kuukausia. Lopulta "oikeat ovet" aukesivat ja työ saatin käyntiin asiantuntijan suostuessa antamaan tietyin yhdessä sovituin reunaehdoin relevanttia asiantuntijan ohjausta työn substanssiin liittyen. Haluan kiittää kaikkia niitä, jotka tukivat tämän työn valmistumista. Erityisesti toimeksiantajan puolelta haluan kiittää Senaatti-kiinteistön turvallisuuspäällikköä Tuomas Lehmusmetsää näin mielenkiintoisen tilaisuuden tarjoamisesta, tuesta, sekä kärsivällisyydestä. Iso kiitos kuuluu yhtälailla opinnäytetyön ohjaajalle Valtioneuvoston tietoturvapäällikkö Petri Puhakaiselle ohjauksesta, työn vauhdittamisesta, sekä erityisesti kiitokset "oven avaamisesta" Viestintäviraston suuntaan substanssisosaamisen varmistamiseksi ja salassapitovelvoitteiden noudattamiseksi. Tästä erityiset kiitokset Viestintäviraston johtavalle tarkastajalle Aki Tauriaiselle, ilman apuasi tämän työn valmistuminen ei olisi ollut mahdollista, kiitos relevantin lähdemateriaalin pariin ohjauksesta, työn substanssipuolen tarkastamisesta, haastatteluista ja ajastasi oman työsi ohella. Kiitos lisäksi Laurean informaatikko Hannu Jokirannalle avustasi lähdemateriaalin löytämiseksi. Kiitos Christer. Thank you Jimmy. Lopuksi kiitos vaimolleni Anulle ja lapsille kärsivällisyydestänne, tämä työ vei paljon aikaa teiltä. Tämä oli antoisa ja hyvin mielenkiintoinen mahdollisuus, joka toivottavasti palvelee toimeksiantajan tarkoitusta, sekä parantaa omalta osaltaan suomalaisen yhteiskunnan tietoisuutta hajasäteilyyn liittyvistä riskeistä.

TEMPEST-hyökkäykset ja suojautumiskeinot

Velemir, Jokso Juhana
Turvallisuusjohtaminen, (YAMK)
Opinnäytetyö
Helmikuu, 2018

Laurea-ammattikorkeakoulu
Leppävaara
Turvallisuusjohtaminen (YAMK)

Tiivistelmä

Velemir, Jokso Juhana

TEMPEST-hyökkäykset ja suojautumiskeinot

Vuosi 2018 Sivumäärä 55

Tiivistelmän jäsennys:

Tämä opinnäytetyö käsittelee sähkömagneettista hajasäteilyä hyödyksi käyttäviä hyökkäyksiä ei-valtiollisten toimijoiden taholta, sekä suojautumiskeinoja tällaisia hyökkäyksiä vastaan. Opinnäytetyö on tehty Senaattikiinteistön turvallisuusorganisaation tilauksesta, yhteistyössä sekä Senaattikiinteistön turvallisuusorganisaation, että Viestintäviraston NCSA yksikön kanssa. Työn tarkoituksena on tuottaa Senaattikiinteistölle syvällisempää ymmärrystä hyökkäyksistä, joissa käytetään hyväksi sähkömagneettista hajasäteilyä, sekä ohjeistusta suojautumiskeinojen muodossa. Edellä mainittujen tavoitteiden lisäksi, opinnäytetyön toivotaan lisäävän tietoisuutta hajasäteilyyn liittyvistä riskeistä suomalaisen yhteiskunnan ja elinkeinoelämän keskuudessa.Tässä opinnäytetyössä on käytetty lähteinä paljon englanninkielistä lähdemateriaalia, sekä kotimaisista lähteistä etenkin Viestintäviraston julkaisuja. Opinnäytetyön aihe on sensitiivinen ja tämä aiheutti merkittäviä haasteita opinnäytetyön valmistumiseen liittyen. Haasteina olivat mm. lähdemateriaalian sensitiivisyys ts. lähdemateriaali on tietyin osin turvaluokiteltua, suomenkielisen lähdemateriaalin rajallisuus, sekä sensitiivisyyden vuoksi asiantuntijaorganisaatioiden haluttomuus osallistua opinnäytetyön tekemiseen. Vuonna 2013 Viestintävirasto on julkaissut sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet. Opinnäytetyön tuloksena syntyi selvitys sähkömagneettisen hajasäteilyn aiheuttamien turvallisuusriskien Senaattikiinteistön turvallisuusorganisaation käyttöön.

Asiasanat: TEMPEST , Hajasäteily , Signaalitiedustelu

Laurea University of Applied Sciences
Degree Programme in Security management
Master's Thesis

Abstract

Velemir, Jokso Juhana

TEMPEST-attacks and protective countermeasures

Year 2018 Pages 55

This thesis examines attacks using electromagnetic radiation vulnerabilites by non-govermental actors and protective countermeasures against this kind of attacks. This Thesis has been done by assigment by Senaattikiinteistöt security organisation, in cooperation with NCSA unit of Finnish communications regulatority authority. The purpose of this thesis is to produce deeper understanding about the attacks using electromagnetic radiation vulnerabilities together with guidance in form of protective countermeasures. In addition to above mentioned objectives it is hoped that this thesis will increase the awareness of risks involved in electromagnetic radiation among Finnish society and especially business industry. Much of source material is English, from Finnish sources especially publications made by the Finnish communications regularotory authority are used. The subject of this thesis is sensitive and this fact caused significant challenges in regards of the completion of this thesis. Challenges were inter alia sensitivy of source material in other words certain parts of source material is security classified, limited amount of Finnish source material and in addition the reluctance of expert organisations willingness to participate in this Thesis. The outcome of this thesis is a study including protective countermeasures of electromagnetic radiation for use of Senaattikiinteistö.

Keywords: TEMPEST, Electromagnetic radiation, Signal intelligence

Sisällys

1 Johdanto

Tämä opinnäytetyö käsittelee sähkömagneettista hajasäteilyä hyödyksi käyttäviä hyökkäyksiä ei-valtiollisten toimijoiden taholta, sekä suojautumiskeinoja tällaisia hyökkäyksiä vastaan. Opinnäytetyö on tehty Senaattikiinteistön turvallisuusorganisaation tilauksesta, yhteistyössä sekä Senaattikiinteistön turvallisuusorganisaation, että Viestintäviraston NCSA (National Cyber Security Centre) yksikön kanssa. Senaattikiinteistö, sekä Viestintävirasto on esitelty tämän työn kohdissa 2 ja 3. Työn tarkoituksena on tuottaa Senaattikiinteistölle syvällisempää ymmärrystä hyökkäyksistä, joissa käytetään hyväksi sähkömagneettista hajasäteilyä, sekä ohjeistusta suojautumiskeinojen muodossa. Edellä mainittujen tavoitteiden lisäksi, opinnäytetyön toivotaan lisäävän tietoisuutta hajasäteilyyn liittyvistä riskeistä suomalaisen yhteiskunnan ja elinkeinoelämän keskuudessa. Teknologian kehittyessä nopeasti, signaalitiedustelu menettää jossain määrin merkitystään, mutta tästä huolimatta signaalitiedusteluun liittyvät suojaustoimet on huomioitava jatkossakin. Ensinnäkin Suomea velvoittavat kansainväliset sopimukset ja toiseksi hyökkääjä valitsee pääsääntöisesti itselleen helpoimman hyökkäystavan päästäkseen tavoitteeseensa. Euroopan Unionin, sekä Naton turvallisuussäännöissä on määritelty tarkat vaatimukset jäsenvaltioille hajasäteilyn vaimentamiseksi tai jopa poistamiseksi. EU:ssa ja Natossa näistä estotoimista käytetään termiä TEMPEST. Naton julkaisuissa SDIP-27, - 28 ja –29 on määritelty hajasäteilyyn liittyvät hallintatoimet (standardi), NATO ja EU soveltavat näitä ohjeita. Näin ollen, myös Suomi on EU:n jäsenvaltiona velvoitettu noudattamaan edellä mainittuja sopimuksia vaihtaessaan esimerkiksi tietoja NATOn kanssa.
Viestintävirasto on julkaissut v. 2013 ”sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet” huomioiden Suomen kansalliset erityisvaatimukset ja toimenpiteet, joilla hajasäteilyyn liittyviä riskejä voidaan laskea hyväksyttävälle tasolle.
Edellä mainittujen kansainvälisten velvoittavien sopimusten, sekä kansallisten ohjeiden lähtökohdista Senaattikiinteistön turvallisuusorganisaatiolla oli tarve kartoittaa riskejä ja suojautumistoimia liittyen sähkömagneettisen hajasäteilyn aiheuttamiin uhkiin.

1.1 Opinnäytetyön tausta, työn rajaus ja tavoitteet

Senaattikiinteistön turvallisuusorganisaatio määritteli opinnäytetyön tavoitteeksi selvittää 1) pystyykö nk. ”keskivertokansalainen” hankkimaan ja käyttämään sellaista laitteistoa, joilla hän voi suorittaa (laitonta) tiedustelua sähkömagneettista hajasäteilyä hyväksikäyttäen, sekä 2) suojautumiskeinoja hajasäteilyn aiheuttamien riskien ehkäisyksi. Valtiolliset toimijat rajattiin tietoisesti opinnäytetyöstä kokonaan pois ja tarkoitus oli keskittyä nk. ”keskivertokansalaiseen”. Keskivertokansalaisella tarkoitetaan tässä opinnäytetyössä henkilöä, jolla ei ole koulutusta tai syvällistä erikoisosaamista hajasäteilyyn ja siihen liittyviin ilmiöihin, esim. viestintään liittyvää osaamista. Tässä opinnäytetyössä keskivertokansalaisella tarkoitetaan lisäksi henkilöä, jolla ei ole käytössään huomattavia taloudellisia resursseja hankkia ammattikäyt-

töön tarkoitettuja laitteita sähkömagneettisen hajasäteilyn aiheuttamien haavoittuvaisuuksien hyväksikäyttöön.
Opinnäytetyön aihepiirin sensitiivisyys aiheutti merkittäviä haasteita opinnäytetyön tavoitteiden saavuttamiseksi. Lähtökohtaisesti asiantuntijaorganisaatioita löytyy Suomesta, mutta aiheen sensitiivisyyden vuoksi ja väärinkäsitysten välttämiseksi pyyntö opinnäytetyön tukemiseksi esitettiin ainoastaan Viestintävirastolle. Tavoitteena oli saada Viestintävirastolta asiantuntijan opastusta ja valvontaa työn tekemiseen liittyen. Ensimmäinen lähtökohta asiantuntijan ohjauksen saaminen työlle oli se, että työn lopputulos ei saa olla sellainen, että sitä voisi käyttää hyväksi rikoksien suunnittelussa tai tekemisessä. Toisin sanoen, asiantuntija ohjaisi opinnäytetyön tekoa siten, että opinnäytetyön julkinen versio ei sisältäisi turvaluokiteltua tietoa, eikä työ kokonaisuutenakaan mahdollistaisi työn sisältämän tiedon käyttöä laittomiin tarkoituksiin. Toinen tarve asiantuntijatahon löytämiseksi oli varmistaa, että työ sisältää mahdollisimman kattavasti ammatillista lähdemateriaalia. Kolmas tarve asiantuntijatahon löytämiseksi oli varmistaa työn sisältämän tiedon oikeellisuus, sekä oikeiden ammattitermien käyttö. Lisäksi opinnäytetyössä käytettävä kielen päättäminen ei ollut aivan yksinkertaista, sillä suurin osa lähdemateriaalista on englannin kielistä. Viestintäviraston asiantuntijatahon perusteltu näkemys siitä, että työn tulee ensisijaisesti palvella suomalaista yhteiskuntaa, vaikutti ratkaisevasti siihen, että kieleksi valikoitui Suomen kieli.

Opinnäytetyön tekeminen alkoi lähdemateriaalin etsinnällä niillä termeillä mitä opinnäytetyön aloittamisen aikaan oli tiedossa. Termillä "TEMPEST" ei löytynyt merkittävästi lähdemateriaalia, mutta opinnäytetyön aiheeseen liittyvän ymmärryksen syventyessä myös hakutermit tarkentuivat ja lisääntyivät, mikä helpotti lähdemateriaalin löytämistä.

1.2 Tutkimusmenetelmät, raportin rakenne, sekä opinnäytetyössä käytetyt lähteet

Tämä opinnäytetyön on toiminnallinen, eli työelämälähtöinen kehityshanke. Työssä käytetty tutkimusmenetelmä on kvalitatiivinen, eli tavoitteena on tutkittavan asian kokonaisvaltainen ymmärtäminen. Tutkimusongelma on kysymys, johon tutkimuksella pyritään vastaamaan. Tavoite tämän ongelman ratkaisemiseksi määrittelee, minkälaista aineistoa haetaan ja millä menetelmillä aineistoa kerätään. Tutkimusongelma jakautuu pääongelmaan, sekä mahdolliseen tarkentavaan alaongelmaan ja se tulee määrittää ennen aineiston keruuta (Hirsjärvi ym. 2009, 125-126).

Tämän opinnäytetyön tutkimusongelmana on suojautumisohjeiden luominen turvallisuusalan asiantuntijoille kiinteistöalan toimintaympäristöön. Tutkimusstrategiana on selvittää mitä sähkömagneettinen hajasäteily on ilmiönä, sekä minkälaisella laitteistolla ja osaamisella hajasäteilystä voidaan selvittää käsiteltävien tietojen sisältö. Tutkimuksen keskiössä on Viestintäviraston TEMPEST -asiantuntijan haastattelu ja ohjaus lähdemateriaalin löytämiseksi.

Opinnäytetyötä varten haastateltiin Viestintäviraston asiantuntijana kansallinen TEMPEST -vastuuhenkilö Aki Tauriainen. Kaikki haastattelut tapahtuivat kasvotusten aiheen sensitiivisyyden vuoksi. Haastattelut olivat erittäin tärkeässä asemassa tätä opinnäytetyötä ajatellen. Haastattelujen yhteydessä korostui ohjaus relevantin lähdemateriaalin pariin, mikä nopeutti opinnäytetyön valmistumista. Johtuen opinnäytetyön aiheen sensitiivisyydestä, sekä siitä, että opinnäytetyön tekijällä ei ole kyseisestä aihepiiristä aikaisempaa syvällistä ymmärrystä, haastatteluiden yhteydessä saatu ohjaus relevantin lähdemateriaalin pariin aiheutti myös sen, että opinnäytetyön tekijä tutustui ensin lähdemateriaaliin ja tämän jälkeen palasi asiantuntijan luokse tarkentavien kysymysten kanssa. Kirjallisten lähteiden osalta tähän työhön valikoitui määrällisten seikkojen sijaan laadulliset kriteerit täyttäviä teoksia. Viestintäviraston ohje sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteiden ollessa keskiössä, tärkeä lähdekirja on myös Valtiovarainministeriön julkaisema "Toimitilojen tietoturvaohje" vuodelta 2013. Edellä mainittujen teosten keskittyessä hajasäteilyyn ja siihen liittyviin uhkiin, myös sellaisia kirjallisia lähteitä käytettiin mitkä tarkastelevat hajasäteilyyn liittyviä ilmiöitä, kuten radioaaltojen etenemistä käsitteleviä teoksia. Lisäksi mainittakoon Laurea Leppävaaran tiedonhankintaan erikoistuneen informaatikko Hannu Jokirannan avustuksella löytynyt William E. Cobb:in Yhdysvaltain ilmavoimien teknologian instituutille tekemä teos ”Exploitation of unintentional information leakage from integrated circuits, jossa kuvataan hyvin seikkaperäisesti hajasäteilyyn liittyviä haavoittuvuuksia. Lopuksi vielä mainittakoon internetissä tehty tiedustelu eri radiolaitevalmistajien kotisivuille hajasäteilysignaalin sieppaamiseksi ja lukemiseksi tarvittavien laitteiden ja ohjelmistojen hintojen ja saatavuuden selvittämiseksi.

2 Senaatti-kiinteistöt

Senaattikiinteistöt on valtionhallinnon työympäristökumppani ja toimitila-asiantuntija. Senaattikiinteistön tavoitteena on auttaa asiakkaita tehostamaan toimintaansa ja säästämään toimitilakustannuksissa. Senaatin monialaiset ammattilaiset huolehtivat valtion kiinteistövarallisuudesta ja sen tehokkaasta käytöstä. Senaatin vastuulla on myös valtion käytöstä poistuneiden kiinteistöjen myynti ja kehittäminen. Vastuullisuus on keskeinen osa Senaatin kaikkea toimintaa. Senaattikiinteistö tarjoaa asiakkailleen toimitilojen ja työympäristöjen lisäksi monipuolisen valikoiman toimitiloihin liittyviä palveluita keskitetysti yhdestä paikasta. Joustavat palvelut ottavat huomioon myös toimintaan liittyvät erityisvaatimukset ja muuttuvat tarpeet. Kaikkiin palvelukokonaisuuksiin sisältyy palvelujohtaminen ja laadunvalvonta. Senaattikiinteistö tarjoaa myös tarvittaessa toimitilapalveluiden asiantuntijapalveluita esimerkiksi kilpailutuksen tueksi. Valtionhallinnon erityispiirteiden tuntemus on yksi Senaattikiinteistön mainitsema erityisosaamisala, mikä sisältää hajaasäteilyhyökkäyksiin liittyvät suojaustoimenpiteet. Senaattikiinteistöt tilasi tämän tutkimustyön saadakseen syvällisempää ja ajantasaista tietoa

hajasäteilyhyökkäyksiin ja niihin liittyviin suojaustoimenpiteisiin asiantuntijaorganisaationsa käyttöön. Tämän tutkimuksen tavoitteena on vastata Senaattikiinteistön toimeksiannossa määriteltyihin tutkimuskysymyksiin, joiden avulla Senaattikiinteistöt voisivat entistä paremmin toteuttaa toimeksiantoja, joissa tulee huomioida suojautumistoimet hajasäteilyhyökkäyksiä vastaan. https://www.senaatti.fi/tietoa-senaatista/

3 Viestintävirasto

Viestintävirasto ohjaa ja valvoo teletoimintaa. Se varmistaa, että sähköiset tietoverkot ja palvelut ovat turvallisia käyttää, toimivat luotettavasti ja ovat jokaisen kuluttajan ja yrityksen saatavilla. Viestintävirasto huolehtii, että posti- ja sähköisten viestintäpalvelujen lainsäädäntöä ja tv-mainonnan säädöstenmukaisuutta noudatetaan. Viestintäviraston keskeisiä työvälineitä ovat Viestintäviraston määräykset, lausuntopyynnöt, tiedoksiannot ja kyselyt ja yhteistyö kansallisissa ja kansainvälisissä työryhmissä.Viestintäverkkojen ja -palvelujen toimintavarmuus ja turvallisuus kehittyvät. Viestintävirasto lisää viestinnän ja yhteiskunnan luotettavuutta huolehtimalla siitä, että viestintäverkot, tietoturva ja tietosuoja ovat kunnossa. Viestintäviraston tehtävänä on vahvistaa kansallista tietoturvaa ja terävöittää teknistä ohjausta ja valvontaa. Euroopan unionin turvallisuussääntöjen mukaan jokaisella EU- valtiolla tulee olla määrätty toimivaltainen viranomainen, joka vastaa siitä, että viestintä- ja tietojärjestelmät ovat TEMPEST- periaatteiden ja suuntaviivojen mukaisia. TEMPEST viranomainen hyväksyy ratkaisut, joilla suojaudutaan hajasäteilyn aiheuttamilta tietojen turvallisuuteen liittyviltä riskeiltä. Viestintävirasto, joka toimii Suomessa lain kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttämässä viranomaistehtävässä, on tässä työssä tarkoitettu toimivaltainen TEMPEST- viranomainen. Viestintävirasto edistää verkkojen ja palveluiden toimintavarmuutta ja turvallisuutta etupäässä seuraavin keinoin.

3.1 Viestintävirasto vahvistaa kansallista tietoturvaa

Viestintävirasto tuottaa monipuolisia tietoturvapalveluita kansalaisten ja yritysten käyttöön. Virasto varmistaa, että alan toimijat ottavat huomioon kansalliset ja kansainväliset tietoturvavelvoitteet tieto- ja viestintäjärjestelmissä.
Viestintäviraston Kyberturvallisuuskeskuksen tietoturvauhkien valvontapalveluita tarjotaan myös valtiokonsernille ns. GOVCERT-toimintana. Siten myös julkishallinnon havainnointikykyä kehitetään tietoturvaloukkausten varalta.Viestintävirasto vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Suomeen perustettaneen kansainvälisen mallin mukainen viranomaistoiminto tietoturvauhkien ja -loukkausten havainnointiin ja ratkaisemiseen sekä tietoturvan tilannekuvan ylläpitoon. Viestintävirasto pyrkii toimillaan varmistamaan, että tietoliikenneyhteydet toimivat hyvin myös poikkeustilan-

teissa. Mikäli yhteyksiin kuitenkin tulee häiriötä tai vikoja, Viestintävirasto pyrkii antamaan ajantasaista tietoa tietoliikenneyhteyksien häiriö- ja vikatilanteista. Viestintävirasto myös varmistaa, että laitteiden valmistajilla on käytössä tarpeeksi häiriöttömiä taajuuksia. Myös kuluttaja voi luottaa siihen, että hänen käyttämänsä langaton laite toimii häiriöttömästi.

Korkeatasoinen tietoturva ja luottamuksellinen viestintä on Viestintäviraston toiminnan keskiössä. Kuluttajilla ja yrityksillä on käytössä toimivat ja tietoturvalliset viestintäyhteydet.Viestintäpalveluiden käyttäjät pysyvät ajan tasalla tietoturvariskeistä ja niiden torjumisesta.Viestintävirasto ylläpitää sähköisten viestintäverkkojen toimivuuden ja tietoturvan tilannekuvaa ja tiedottaa mahdollisista tietoturvauhkista. Tavoitteena on myös lisätä kansalaisten ja yritysten tietoturvaosaamista muun muassa ohjeistuksen avulla. Viestintävirasto varmistaa myös viestintäverkkojen ja -palveluiden yhteen toimivuuden.

Kansallisesti ja kansainvälisesti merkittävä tehtävä virastossa on radiotaajuuksien keskitetty hallinnointi, jotta voidaan taata taajuuksien tehokas ja mahdollisimman häiriötön käyttö. Viestintävirasto toimii liikenne- ja viestintäministeriön hallinnonalalla. https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat.html

4 Hajasäteilyn määritelmiä

Tässä työssä sähkömagneettisella hajasäteilyllä tarkoitetaan elektronisten laitteiden tahatonta radiotaajuuksilla tapahtuvaa säteilyä, tätä tahatonta hajasäteilyä voidaan kuvata elektronisen laitteen toiminnan ”sivutuotteeksi” esim. englanninkielisessä kirjallisuudessa käytetään yleisesti termiä ”side-channel leakage”. Muita tämän kaltaisia ”sivutuotteita” ovat vaihtelut laitteen (esim. tietokoneen) sähkönkulutuksessa, vaihtelut tietokoneen sisäisissä operaatioissa, sekä hajasäteilyä mikä voi ilmetä jopa akustisena- tai lämpösäteilynä. Tiivistettynä, elektronisen laitteen ympärilleen tahattomasti lähettämä hajasäteily on laitteelle ja sen käyttäjälle turvallisuusriski, koska tietyissä olosuhteissa, tietyllä laitteistolla hajasäteilyä hyväksikäyttämällä hyökkääjä voi selvittää laitteella käsiteltävien tietojen sisällön. Tässä työssä tarkastellaan suojautumistoimenpiteitä, joilla voidaan vähentää tai kokonaan estää tahattoman vaarantavan hajasäteilyn pääsy ympäristöön ja mahdollisen hyökkääjän haltuun.

Viestintävirasto kuvaa hajasäteilyä seuraavasti: "Viestintä- ja IT-laitteet säteilevät ympärilleen sähkömagneettista säteilyä, josta voidaan sopivilla laitteilla tietyissä olosuhteissa selvittää ja tallentaa käsiteltävien tietojen sisältö. Esimerkiksi tietokoneen näytöllä olevaa kuvaa voidaan katsella ja tallentaa kaappaamalla näyttölaitteesta lähtevää hajasäteilyä. Tämä aiheuttaa riskin käsiteltävien tietojen luottamuksellisuuden säilymiselle". (Viestintävirasto, 2013)

William E. Cobb kuvaa työssään "Exploitation of unintentional information leakage from integrated circuits" mikrosirun hajasäteilyä seuraavasti: kaikki fyysiset järjestelmät, joita tarkastellaan ulkoisesti, tuottavat tarkoitettua ja tahatonta sähkömagneettista säteilyä, myös tahattomat lähetykset ovat mitattavia, fyysisesti tarkasteltavia ilmiöitä, jotka syntyvät tarkoitetun toiminnan sivutuotteena. Cobb kuvaa hajasäteilyä omassa työssään seuraavasti: ” On yleisesti tiedossa, että elektroniset laitteet säteilevät sähkömagneettista hajasäteilyä ympärilleen, mikä voi häiritä muita lähistöllä olevia laitteita. Tästä syystä lentokonematkustajia pyydetään sulkemaan kaikki kannettavat elektroniset laitteet ja kaikki Yhdysvalloissa myytävät elektroniset laitteet ovat velvoitettuja sertifioituihin testauksiin, joissa niiden tulee täyttää niille asetetut vaatimukset. Digitaaliset laitteet, jotka sisältävät mittareita, oskillaattoreita tai muita korkean taajuuden pulsseja ovat erityisesti säädeltyjä, koska ne ovat tunnettuja tahattoman säteilyn tuottajia ja näin ollen tuottavat säteilyä radiotaajuuksilla. Viime vuosikymmenen aikana tietoisuus tahattomien lähetyksien suhteen on lisääntynyt, sen lisäksi, että säteily voi häiritä muita laitteita, säteilyn kautta laite voi ”vuotaa” tahattomasti tietoja laitteen käytöstä säteilyn mukana (Cobb, 2011).

Vaihtelut tietokoneen sisäisten operaatioiden ajoissa. Aika mikä mikroprosessorilta tai muulta elektroniselta laitteelta kuluu sille annetun tehtävän suorittamiseen, riippuu yleisesti käsiteltävästä datasta. Vaihtelut prosessointiajoissa ovat yksilölliset ja riippuvat kulloisestakin toimenpiteestä, vaihtelut voivat aiheutua esim. riippuvuuksista muihin ohjelmistoihin ja niiden toimintoihin, välimuistin ominaisuuksiin, tehtäväjonoihin, ulkoisten laitteiden ominaisuuksiin (esim. ulkoinen lisämuisti) jne. Yksinkertaistaen, tarkastelun kohteena oleva laite (esim. tietokone) käyttäytyy eri tavalla riippuen minkälaista tietoa, sillä käsitellään. Laite suoriutuu ”pienistä” tehtävistä nopeammin ja helpommin kuin suurempien tiedostojen käsittelystä. Nämä erot ovat havaittavissa ja siten mitattavissa tietyllä laitteistolla, tietyissä olosuhteissa. Kocher havaitsi, että edellä mainitun kaltaiset tahattomat vaihtelut (laitteen) suoritusajoissa voidaan merkittävissä määrin korreloida laitteella käsiteltävään tietoon. Useissa tapauksissa tahattoman hajasäteilyn kautta tarkasteltavana olevan laitteen prosessiaikojen vaihtelujen korreloinnin kautta on riittävästi selvittääkseen salatun laitteen (salaus)avaimen (Cobb, 2011).

Jokaisella tietokoneella on identifioitavissa oleva ns. ”elektroninen sormenjälki” ts. vaikka tietyn tietokonevalmistajan tuotantolinjalta otettaisiin peräkkäiset tietokoneet niin ne eivät ole täysin identtiset, vaikka olisivat samasta tuotantoerästä. Samoin jokaisella tietokoneen näppäimistön painikkeella on oma identifioitavissa oleva ”elektroninen sormenjälki”. Tietyllä laitteistolla, tietyissä olosuhteissa on päästy yli yhdeksänkymmenen prosentin todennäköisyyteen tarkasteltavana (tai hyökkäyksen kohteena) olevan näppäimistön painetusta näppäimestä. (Cobb, 2011). Näin korkealla todennäköisyydellä yksittäisen näppäimen identifiointi, hyök-

kääjällä on erinomaiset mahdollisuudet saada selville esim. näppäimistöllä kirjoitetun viestin sisältö. Hajasäteilyn ymmärtämistä ilmiönä voi myös kuvata vertaamalla ilmiötä lämpösäteilyyn. Jokainen elävä ihminen säteilee ympärilleen lämpöä. Ihmissilmällä tätä lämpösäteilyä ei voida havaita, mutta oikeissa olosuhteissa tietyllä laitteistolla tämä lämpösäteily on havaittavissa. Esimerkkinä metsään kadonneen etsintä yöaikaan. Etsinnöissä mukana olevan lämpökameran avulla pimeästä metsästä voidaan havaita lämpöä säteilevä ihminen, edellyttäen että lämpökameran ja lämmönlähteen (ihmisen) välissä ei ole esteitä mitkä estäisivät lämpösäteilyn havaitsemisen, sekä etäisyyden täytyy olla sellainen, että laite havaitsee lämpösäteilyn (lämpösäteilyn lähde on laitteen toiminta-/kantoalueella.

Koska hajasäteilyä hyväksikäyttävässä hyökkäyksessä on kyseessä on ns. "signaalin nappaaminen ilmasta", hyökkäyksestä ei jää mitään jälkiä verrattuna esim. fyysiseen murtautumiseen toimistotilaan tai tietokoneen hakkerointiin, joista molemmista mahdollisesti jää jälkiä ja tietovarkauden uhri tulee tietoiseksi mahdollisesta rikoksesta. Hajasäteilyä hyväksikäyttävässä hyökkäyksessä hyökkäyksen kohde ei todennäköisesti saa koskaan tietää joutuneensa tietovarkauden uhriksi, mikä on puolestaan merkittävä etu hyökkääjälle. Esimerkiksi voidaan kuvitella tilanne, jossa kilpailija saa haltuunsa miljoonakauppoihin valmistautuvan yrityksen tai valtiollisen toimijan suunnitteleman tarjouksen ja voi laittomin keinoin haltuunsa saamiensa tietojen perusteella jättää paremman tarjouksen ja voittaa tarjouskilvan. Kilpailija voi vain ihmetellä, kuinka toinen yritys vei kaupan ns. "nenän edestä" vain marginaalisesti paremmalla tarjouksella. Tarjouksen hävinneessä yrityksessä mahdollisesti ajateltaisiin seuraavasti: "aivan kuin kilpailija olisi jotenkin tiennyt jättämämme tarjouksen ehdot".

4.1 Hajasäteilyn historiaa

Vuosien ajan hajasäteilyä on käsitteenä ympäröinyt tietynlainen mystiikka ja salaisuuksien verho. Hajasäteilyyn liittyy vieläkin erilaisia teorioita, jopa väitteitä siitä, että hajasäteily on huijausta. Hollantilainen tiedemies professori Wim van Eck julkaisi vuonna 1985 tutkielman aiheesta, jossa hänen arvionsa mukaan (signaalin) maksimi vastaanottoetäisyys oli n. yksi (1) kilometri. Hänen julkaisustaan johtuen näitä signaaleja alettiin kutsua ”Van Eckin säteilyksi”. Tähän termiin voi törmätä ammattikirjallisuudessa edelleenkin. Van Eckin julkaisun jälkeen tiedustelupalvelut luokittelivat metodologian salaiseksi, mutta se oli liian myöhäistä. Vuonna 1992 New Yorkin kaupungissa poliisi raportoi havaitsemastaan antennista erään kerrostalon parvekkeella, sillä antenni oli suunnattu lähellä sijaitsevan pankin suuntaan. Kyseisen pankin toimipisteessä oli useita pankkiautomaatteja, sekä pankin luottokortien käsittelytilat. Havainnot suunnatusta antennista pankin suuntaan viittasivat siihen, että pankki oli van Eckin hyökkäyksen kohteena, mutta siinä vaiheessa kun poliisi käynnisti tutkimuksensa, antenni ja sen operaattori olivat kadonneet. (Denning 1999) On todennäköistä, että jo ennen Wim van

Eckin julkaisua, hajasäteilyyn liittyvää tiedonhankintaosaamista on ollut olemassa teknisesti kehittyneiden valtioiden tiedustelupalveluilla.

4.2 Keskeisiä käsitteitä

Termi "Tempest" on kehitetty Natossa ja sitä käytetäänkin yleisesti kansainvälisissä yhteyksissä, kuten Natossa ja Euroopan Unionissa. Termi "Tempest" tulee sanoista Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. Terminä "Tempest" käsittää hajasäteilyyn kohdistuvia riskejä vähentäviä toimenpiteitä, kuten tutkimuksia, tarkastuksia, kontrollointia, sekä vaimentavia toimia.

Jokaisella Euroopan Unionin jäsenvaltiolla tulee olla turvallisuussääntöjen mukainen, erikseen määrätty toimivaltainen viranomainen, joka vastaa siitä, että viestintä- ja tietojärjestelmät ovat TEMPEST- periaatteiden mukaisia. TEMPEST- viranomainen hyväksyy ne ratkaisut, joilla suojaudutaan hajasäteilyn aiheuttamilta tietojen turvallisuuteen liittyviltä riskeiltä. Suomessa toimivaltainen TEMPEST- viranomainen on Viestintävirasto, joka toimii Suomessa lain kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) edellyttämässä viranomaistehtävässä.

Valtiovarainministeriön toimitilojen tietoturvaohjeessa hajasäteilyä käsitellään seuraavasti. Sähkömagneettisen hajasäteilyn uhka on kansainvälisten vaatimusten mukaisesti otettava huomioon jo korotetun tason tiedonkäsittely – ympäristöissä. Kansallinen ohjeistus antaa erityisesti korotetun tason suojausvaatimusten toteuttamiselle enemmän tulkintavaraa. Uhkaa torjutaan riskiarvioon ja mahdollisesti vaimennusmittauksiin perustuen kansainvälisen TEMPEST- standardin mukaisin toimenpitein. Standardi ei ole julkinen. Standardin kansallisesta tulkinnasta ja suojautumisen ohjauksesta vastaa toimivaltaisena viranomaisena Viestintäviraston NCSA-FI yksikkö. Hajasäteilyn vastatoimet voidaan jakaa karkeasti kahteen menetelmään: laitteiden suojaaminen metallikoteloinnilla tai työskentelytilan suojaaminen rakenteellisilla ratkaisuilla. Tavoitteena on, ettei salassa pidettävää tietoa pääse vuotamaan tilasta ulos sähkömagneettisen säteilyn välityksellä vaimennusvaatimukset ylittävällä tasolla.

4.3 Maxwellin yhtälö

Radioaallot, mikroaallot, infrapuna-valo, sekä silmällä näkyvä valo ovat kaikki Maxwellin teorian mukaisia ilmiöitä, joita kutsutaan sähkömagneettiseksi säteilyksi. James Clerk Maxwell (1831-1879) oli skotlantilainen fyysikko, joka tuli parhaiten tunnetuksi hänen sähkömagneettisesta teoriastaan. Vuonna 1873 James Maxwell kehitti Maxwellin yhtälön, jonka syntyyn vaikutti Michael Faradayn havainnot sähköön ja magnetismiin liittyen. "Maxwellin yhtälöt luovat pohjan kaikelle nykyaikaiselle sähkötekniikalle (sähkömoottorit, sähkön siirto, valokaapelit, tietokoneet, televisio, tutkat, kännykä, jne."(Valtanen 2007, 69). Maxwellin yhtälöt kuvaavat

neljää sähkö- ja magnetismiopin perusominaisuutta: 1) Gaussin laki (kuinka sähkövaraus tuottaa sähkökentän), 2) Gaussin laki magneettikentille (kuinka sähkömagneettisia monopoleja ei ole olemassa), 3) Faradayn induktiolaki (kuinka muuttuva magneettikenttä tuottaa sähkökentän), 4) Amperen laki ja Maxwellin lisäys (kuinka sähkövirta ja muuttuva sähkökenttä tuottavat magneettikentän). Maxwellin yhtälöillä kuvataan tiiviissä muodossa sähkö-ja magneettikenttien käyttäytymistä. "Maxwellin yhtälöt muodostavat radiotekniikan ja koko sähkötekniikan perustan" (Räisänen & Lehto 2001, 21).

4.4 Hertsi (Hz)

Heinrich Hertz, (1857- 1894) oli saksalainen fyysikko, joka vahvisti James Clerk Maxwellin teorian sähkömagnetismista oikeaksi, sekä valon ja lämmön olevan sähkömagneettista säteilyä. Herz sai aikaan sähkömagneettisia aaltoja laboratoriossaan ja onnistui mittaamaan niiden pituuden ja kiihtyvyyden. Näitä aaltoja kutsuttiin aluksi ”Herzianeiksi”, mutta myöhemmin niitä alettiin kutsua radioaalloiksi.https://www.britannica.com/biography/

Hertsi (Hz) on kansainvälisen yksikköjärjestelmän mukainen taajuuden yksikkö. Yksikkö on nimetty saksalainen Heinrich Rudolf Hertzin mukaan tunnustukseksi hänen työstään sähkömagnetismin alalla. Yksi hertsi tarkoittaa taajuutta, jossa värähdysjaksot toistuvat sekunnin välein. Ääni on etenevä pitkittäinen aalto, joka aiheutuu paineen värähtelystä. Jokainen nuotti vastaa tiettyä taajuutta, mikä taas voidaan mitata hertseinä.
Sähkömagneettinen säteily. Sähkömagneettista säteilyä kuvataan usein sen taajuuden mukaan, sen mukaan kuinka monta värähtelyä ilmenee sekunnissa pystysuorassa sähkökentässä ja magneettikentässä, ilmaistuna hertseinä. Radiotaajuuksien säteily yleensä mitataan kilohertseinä (kHz), megahertseinä (MHz) tai gigahertseinä (GHz).
https://en.wikipedia.org/wiki/Hertz

5 Radioaaltojen ominaisuuksista:

Radioaallot käyttäytyvät eri tavalla kuin sähkö johtimissa. Radioaallot ovat tilassa liikkuvia sähkömagneettisia aaltoja, joiden energia esiintyy sekä sähköisinä (E) että magneettisina (H) kenttinä. Nämä kentät esiintyvät yhdessä, koska muutos sähkökentässä aiheuttaa muutoksen magneettisessa kentässä ja vastaavasti muutos magneettisessa kentässä aiheuttaa muutoksen sähkökentässä. Radioaaltojen edetessä kohti vastaanottajaa, ne saapuvat eri teitä ja eri voimakkuuksilla vastaanottajan antennille. Antennissa aallot summautuvat ja vastaanotin näkee yhden signaalin. Koska summautumisen lopputulokseen vaikuttaa eri komponenttien keskinäiset vaihe-erot, vastaanotetun signaalin ero lähetettyyn signaaliin nähden riippuu siitä, ku-

moavatko summautuneet komponentit toisensa vai tapahtuuko vahvistus. Sähkömagneettinen signaali muodostuu usein monesta taajuuskomponentista, parhaiten tämä tulee esiin ihmisen puheessa, joka sisältää taajuuksia alkaen muutaman sadasta värähtelystä sekunnissa (Hz). Tietoliikennetekniikassa tietoa ei siirretä digitaalisesti on/off tekniikalla lukuun ottamatta tietokoneiden sisäisiä väyliä ja oheisliitäntöjä tai optisia kuituja, vaan tieto moduloidaan ottaen huomioon siirtotien ominaisuudet. Tämä johtuu siitä, että digitaalinen signaali sisältää aivan liian suuren joukon taajuuskomponentteja, jotta se siirtyisi luotettavasti pitkiä matkoja ja lisäksi taajuuskomponenttien suuri lukumäärä laajentaa teoriassa tarvittavaa kaistanleveyttä äärettömäksi, yksi digitaalinen radioyhteys häiritsisi näin ollen kaikkea muuta radioliikennettä. Arkielämässä tällainen tapaus tulee esille, kun television lähetyksissä näkyy ”lumisadetta”. (Granlund, 2001)

5.1 Radioaallon eteneminen

Radioaallon etenemiseen vaikuttavat troposfäärin, ionosfäärin ja maaston ominaisuudet. Troposfääri on ilmakehän alin kerros, jossa sääilmiöt tapahtuvat. Napa-alueilla troposfääri yltää n. kymmenen (10) kilometrin korkeuteen ja päiväntasaajalla n. kahdenkymmenen (20) km korkeuteen. Troposfäärissä radioaallon tila muuttuu, se vaimenee, kaartuu ja heijastuu ja sen vaihe voi muuttua monitie-etenemisen takia. Ionosfääri muodostuu auringon ultravioletisäteilyn ionisoimista vapaista elektroneista ja ioneista ja se ulottuu noin kuudenkymmenen (60) kilometrin korkeudesta aina tuhannen (1000) kilometriin korkeuteen. Rajataajuuden kymmenen (10) MHz alapuolella olevat taajuudet eivät läpäise ionosfääriä vaan ne heijastuvat takaisin ja tätä ominaisuutta käyttämällä voidaan pientaajuinen radioliikenne saada kiertämään maapallon. Radioaallon taajuus vaikuttaa sen etenemiseen ja suurimmat taajuudet käyttäytyvät valon tavoin. Jos tarkastelemme radioaallon etenemistä lähettäjältä vastaanottajalle, tärkeimpänä väylänä on niiden välinen suorin yhteys. Radioaalto saavuttaa vastaanottajan, jos hän on lähettimen kuuluvuusalueella. Tällainen kuuluvuusalue ei ole yksiselitteinen eikä se muodosta säännöllisiä rengasta lähettimen ympärille vaan sen muotoon vaikuttavia tekijöitä ovat esimerkiksi maasto, esteet ja radioaallon pituus. Laskennallisella kuuluvuusalueella voi syntyä ns. katvealueita, joita radiosignaali ei tavoita ja tästä johtuen esimerkiksi GSM puhelimen kuuluvuus saattaa vaihdella jopa yhden neliömetrin kokoisella alueella. Kuuluvuusalue voidaan jakaa kolmeen (3) vyöhykkeeseen: 1) Alue, jonka sisällä lähettimen signaali kuuluu ja sen sisältämä informaatio on luettavissa, 2) Alue, jonka sisällä lähettimen signaali erottuu taustan kohinasta, mutta tietoliikenne ei onnistu huonon yhteyden takia, 3) Alue, jonka sisällä lähettimen signaali saattaa häiritä muuta radioliikennettä, mutta sitä ei voida erottaa taustakohinasta. (Grandlund, 2001). Maanpinnan ja rakennuksien aiheuttamat heijastukset voivat olla sekä haitallisia että hyödyllisiä, sillä monitie-etenemisen takia radioaalto voi häipyä, mutta heijastuksien ansiosta radio voi kuulua myös paikoissa, joihin aalto ei

suoraan pääsisi. (Lehto 2006, 82). Myös sää vaikuttaa radioaaltojen etenemiseen jossain määrin.

5.2 Kohina

Pyrittäessä kunnolliseen vastaanottoon radioyhteydessä on tärkeää, että signaali erottuu riittävän hyvin taustakohinasta. Ismo Lindell kuvaa kirjassaan "Radioaaltojen eteneminen" kohinaa seuraavanlaisesti: "Luonnossa esiintyvä häiriökenttä, sekä vastaanottimessa syntyvä kohina aiheuttavat yhdessä kohinasignaalin, joka kilpailee vastaanotettavan signaalin kanssa". Vastaanotettava signaali on siis kyettävä erottamaan kohinasignaalista, jotta vastaanotettava lähetys (signaali) olisi ymmärrettävä. Kohina voidaan jaotella sen aiheuttajan perusteella: 1) vastaanottimesta aiheutuva kohina, 2) ilmakehästä ja maasta syntyvä lämpökohina, 3) salamapurkausten aiheuttamat häiriöt, 4) avaruuskohina, 5) sähkölaitteiden aiheuttama kohina (man-made noise)" (Lindell, 1985). Tässä työssä ei ole tarkoituksenmukaista kuvata syvällisemmin eri kohinan aiheuttajien taajuuksia tai syntymekanismeja. Yllä mainitut kohinan lähteet on kuitenkin hyvä tiedostaa yleisellä tasolla tarkasteltaessa signaalin erottelua on kyseessä sitten vaimennusmittaus tai hajasäteilyhaavoittuvuutta hyväksikäyttävä hyökkäys, sillä nuo kohinan lähteet ovat yleensä ei -toivottuja häiriön lähteitä (Lindell, 1996).

5.3 Radioaaltojen vaimeneminen

Kaj Granlund kuvaa kirjassaan "Langaton tiedonsiirto" vaimenemista seuraavasti: "Vaimeneminen (eng. "attenuation" tai "path loss") on ilmiö, jossa on kyse signaalin sisältämän tehon vähenemisestä. Johtimessa signaali vaimenee, koska osa signaalin tehosta muuttuu signaalin resistanssista johtuen lämmöksi. Vaimeneminen tapahtuu siten, että signaalin amplitudi (aallon korkeus) pienenee matkan kasvaessa hävitäkseen sitten kokonaan. Vaimeneminen ei tapahdu tasaisesti niin, että kaikki taajuudet vaimenisivat samassa suhteessa vaan, vaan vaimeneminen vaihtelee riippuen taajuudesta ja käytetystä siirtotiestä. Koska kaikki taajuuskomponentit eivät vaimene samalla tavalla, tapahtuu vaimenemisen mukana myös signaalin muodon vääristymistä. Kokonaisvaimennus lasketaan siirrettävän ja vastaanotetun signaalin suhteena käyttäen yksikköä desibeli (dB). Vaimennus on suoraan verrannollinen radioaallon taajuuteen" (Granlund,2001). Myös erilaiset fyysiset esteet aiheuttavat vaimennusta (esim. kasvillisuus, rakennukset, sadepisarat, yms.).

5.4 Häipyminen (fading)

Häipyminen jaetaan kahteen ryhmään, hidas häipyminen (eng. slow fading) ja nopea häipyminen (eng. fast fading or Raleigh fading). Hitaalla häipymisellä tarkoitetaan vastaanotetun signaalin keskiarvon muutosta, mikä johtuu esim. näköesteistä, maaston muutoksista yms. No-

pealla häipymisellä puolestaan kuvataan satunnaisesti välille 0-2 π jakautuneiden osasignaalien summautumisesta vastaanottajalla, joka noudattaa ns. Raleigh jakaumaa. Nopeassa häipymisessä signaali siis interferoi (summautuu) itsensä kanssa. Nopea häipyminen johtuu sekä lähettimen liikkeestä, että monitie-etenemisestä. (Granlund 2001)

5.5 Monitie- eteneminen

Monitie-eteneminen (eng. multipath fading) on ilmiö, joka muistuttaa optisissa kuiduissa tapahtuvaa pulssin leviämistä eli dispersiota. Kuiduissa tämä ilmiö johtuu siitä, että signaali etenee heijastuen kuidun rakenteissa ja valonsäteiden erilaiset heijastuskulmat muuttavat niiden kulkemaa kokonaismatkaa. Radioliikenteessä ongelma on kertaluokkaa vaikeampi. Jos tarkastelemme optista kuitua, eri taajuuksien kulkemat matkat eivät merkittävästi poikkea toisistaan, mutta radiosignaali saattaa heijastua ympäristössä olevista esineistä ja kulkea jopa kaksinkertaisen matkan verrattuna lyhimpään reittiin. Heijastuva signaali tulee siis perille ”väärään aikaan” ja lisäksi se on menettänyt osan energiastaan heijastuksen yhteydessä. Signaalin heijastumiseen vaikuttaa aallonpituus, sekä aine jonka signaali kohtaa (esim. seinä). Tämä riippuvuus on helpoimmin nähtävissä eri väreinä luonnossa. Vihreä pinta heijastaa vihreätä valoa, mutta absorboi (imee) punaista valoa ja voimme vaikuttaa esineen heijastusominaisuuksiin peittämällä esine eri värejä heijastavilla aineilla (maaleilla). (Granlund 2001)

Eräs yksinkertainen tapa havainnollistaa radioaaltojen ilmenemistä ja sen aiheuttamaa häiriötä muille elektronisille laitteille on asettaa matkapuhelin tavallisen näyttöpäätteen tai television vieressä muutaman sentin etäisyydellä. Kun puhelimella soittaa, se aiheuttaa havaittavaa värähtelyä näyttöpäätteellä. (Granlund 2001)

5.6 Hajasäteilyn etenemiseen ja hyötysignaalin kaappaamismahdollisuuksiin vaikuttavat tekijät

Hajasäteily tapahtuu radioaaltotaajuuksilla, tästä johtuen (kuten radioaallot yleensäkin) hajasäteily etenee luonnollisesti parhaiten silloin, kun säteilylähteen ja vastaanottimen välillä ei ole minkäänlaisia fyysisiä esteitä. Etäisyys säteilylähteestä (esim. tietokone) vastaanottimeen (antenni) vaikuttaa havaittavaan säteilyn voimakkuuteen. Tämän vuoksi suojattava kohde kannattaa sijoittaa mahdollisimman kauas paikasta, mistä säteilyn kuuntelemista tai kaappaamista voidaan yrittää. Seuraavat esimerkit kuvaavat erilaisten rakenneratkaisujen vaikutusta hajasäteilyn etenemiseen: Lasi vaimentaa vähemmän kuin muurattu tiiliseinä, mikä taas puolestaan vaimentaa vähemmän kuin teräs jne. Näin ollen ikkunaton huone on aina suositeltavampi kuin ikkunallinen. Kahdenkymmenen (20) senttimetrin materiaalipaksuus (esim. tiili tai betoni) vaimentaa enemmän kuin samasta aineesta koostuva kymmenen (10)

senttimetrin materiaalipaksuus. Kaksi seinää vaimentaa siis enemmän kuin yksi. Hajasäteilyltä suojattava huone kannattaa näin ollen sijoittaa mieluiten rakennuksen sisäosiin. Mahdollisuuteen kaapata yksittäisen laitteen säteilyä vaikuttaa myös se, onko samassa paikassa useampia samalla taajuudella säteileviä samanlaisia säteilylähteitä (esimerkiksi tietokoneen näyttöjä). (Viestintävirasto 2013).

Edellä mainittuja asioita arvioitaessa tulee ottaa huomioon se, että suojattavassa tilassa olevat kaapelit, ilmanvaihtoputket, vesijohdot, raudoitukset jne. Voivat toimia säteilyä johtavina johtimina, eli antenneina. Erilaisten rakenneratkaisujen avulla voidaan saavuttaa vain suuntaa- antavia ratkaisuja. Lopullisen varmuuden hajasäteilyn vaimennusarvoista voi kuitenkin saada vain asianmukaisella mittauksella (Viestintävirasto 2013).

5.7 Sähköisen tiedon käsittely-ympäristöjen erotteleminen hajasäteilyriskin pienentämiseksi (PUNA/MUSTA – periaate)

Sähköiset tietojenkäsittely-ympäristöt (kaapeloinnit, elektroniikkakomponentit, salauslaitteet jne.) tulee erottaa toisistaan, mikäli niissä käsitellään salassa pidettäviä tietoja siten, että toisessa järjestelmässä tieto on salaamattomana ja toisessa salattuna. Erotteleminen voi tapahtua käytännössä esimerkiksi sijoittamalla ko. järjestelmien salauslaitteet, tietokoneet tai tietoja siirtävät kaapelit määrätyn välimatkan päähän toisistaan. Nämä suojaetäisyydet on mainittu EU:n ohjeessa IASG 07-01, osa III (Viestintävirasto 2013).

PUNA/MUSTA – periaate vaatii sen, että 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 piiristöjä, komponentteja, laitteita ja järjestelmiä. Terminologia tekee eron myös niiden fyysisten alueiden välillä, joihin em. Tekniikka on sijoitettu. Siirron ja tallenteiden osalta suositeltavin tapa on kuitenkin pitää sähköisessä muodossa olevat salassa pidettävät tiedot salattuina, jolloin em. menettelyjä ei tarvita (Viestintävirasto 2013).

5.8 Hajasäteilyn vaimennusvaatimukset eri suojaustasojen tiedoille

Hajasäteilyn vaimennustarve riippuu käsiteltävien tietojen suojaustasosta. Korkeampi suojaustaso edellyttää tehokkaampaa hajasäteilyn vaimentamista kuin matala. Hajasäteilyä voidaan vaimentaa (vähentää) tilaratkaisuilla tai käyttämällä erityisiä hajasäteilyltä suojattuja laitteita. Euroopan Unioni on laatinut luokittelumallit vaatimuksineen tiloille ja laitteille. Näi-

tä malleja sovelletaan myös kansallisten tietojen suojaamisessa. Malleissa vaimennusvaikutusvaatimukset on jaettu neljään tilavyöhykkeeseen (0-3) ja neljään laitesuojaluokkaan (A-C ja COTS eli kaupallinen TEMPEST – suojaamaton laite). Tilavyöhykkeiden vaimennusvaatimukset on kuvattu tämän ohjeen luvussa 5.2. laitesuojaluokat on kuvattu luvussa 5.3.

Hajasäteilyltä suojautuminen voidaan tehdä tilaratkaisulla, suojatuilla laitteilla tai molempien yhdistelmällä. Tilojen luokittelu ja hajasäteilyltä suojatun tilan valinta on suositeltavinta tehdä luvussa 5.2 kuvatun mittauksen tulosten perusteella tai VAHTI 2/2013, liitteessä 1 kuvatun pisteytysmallin mukaisesti. Tilojen luokittelu suojaetäisyyden perusteella on mahdollista silloin, kun mittausta ei jostain syystä pystytä suorittamaan tai sitä ei katsota riskianalyysin perusteella välttämättömäksi.

5.9 Toimitilojen jaottelu vyöhykkeisiin hajasäteilyn vähentämisen näkökulmasta

Tilojen luokittelu hajasäteilyn vaimentumisen mittausten perusteella:
Tilat voidaan luokitella neljään vyöhykkeeseen, jotka määräytyvät tilan rakenteiden mitatusta kyvystä vaimentaa hajasäteilyä. Vaimennuskyky määräytyy tilojen rakenteiden mukaisesti, kuten luvussa 4 on kuvattu. Lisäksi rakennuksen, jonka sisällä luokiteltava tila sijaitsee, ympärillä olevan valvotun/aidatun alueen myötä etäisyyden kasvattaminen suojattavan kohteen ja potentiaalisen hyökkääjän välillä lisää hajasäteilyn vaimennusta. Eri tiloista tehtyjen mittaustulosten perusteella voidaan valita työtilat, joista pääsee ympäristöön mahdollisimman vähän hajasäteilyä.

TEMPEST – vyöhykemittaukset, joiden perusteella tilojen luokittelu tehdään, on kuvattu EU:n ohjeessa IASG 07- 02. Taulukossa 1. on kuvattu tilavyöhykkeiden vaimennusvaatimuksia kaupallisilla laitteilla.

Taulukko 1: Kansalliset TEMPEST – tilavyöhykkeiden vaimennusvaatimukset toimittaessa COTS (suojaamattomat kaupalliset) -laitteilla.

Kansallinen turvallisuusvyöhyke	Kansallinen TEMPEST-tilavyöhyke	Vaimennusvaatimus
KELTAINEN	2	Lisävaimennus 14 dB< vaimennus< 34 DB (vertailu referenssimittaukseen)
SININEN	3	Lisävaimennus >34 dB (vertailu referenssimittaukseen)
PUNAINEN	n/a	Vaatii erityistarkastelun

(Viestintävirasto 2013)

Tilojen luokittelu etäisyyden perusteella:

Tilat voidaan myös luokitella ilman vyöhykemittauksia perustuen suojattavan tilan etäisyyteen mahdollisesta riskialttiiksi arvioidusta hajasäteilyn kaappauspisteestä (useimmiten rakennuksen tai valvotun/aidatun alueen ulkokehältä).Taulukossa 2 on kuvattu etäisyyden perusteella määritetyt tilavyöhykkeet toimittaessa suojaamattomilla kaupallisilla laitteilla kun taas taulukossa 3 on kuvattu hajasäteilyltä suojattujen laitteiden (valinta) ja tilavyöhykeluokat.

Taulukko 2: Etäisyyden perusteella määritetyt tilavyöhykkeet toimittaessa COTS- laitteilla.

Kansallinen turvallisuusvyöhyke	TEMPEST-tilavyöhyke	Etäisyysvaatimus
KELTAINEN	2	Etäisyys tarkastettavan alueen ulkokehälle on yli 100 m mutta alle 1000m
SININEN	3	Etäisyys tarkastettavan alueen ulkokehälle on yli 1000m
PUNAINEN	n/a	n/a

(Viestintävirasto 2013)

Taulukko 3: Hajasäteilyltä suojattujen laitteiden valinta ja tilavyöhykeluokat.

Turvallisuusvyöhyke (VAHTI 2/2013)	Tilavyöhyke tai laitesuojaluokka

Suojaustaso (sähköinen)		COTS	Laiteluokka C	Laiteluokka B	Laiteluokka A
ST IV		X	X	X	X
ST III		Vyöhyke 2	Vyöhyke 1	Vyöhyke 0	Vyöhyke 0
ST II		Vyöhyke 3	Vyöhyke 2	Vyöhyke 1	Vyöhyke 0
ST I		n/a	n/a	n/a	n/a

ST I- aineiston käsittely sähköisesti vaatii aina erityistarkastelun, myös kokonaisturvallisuuden osalta. *Hyväksytty käsittely perustuu vaimennusmittaukseen, etäisyyteen tai riskienarviointimenettelyyn.

TEMPEST-laitesuojaluokat:

- COTS=kaupallinen, ei-suojattu laite
- C=vähiten suojattu

- B= keskimääräisesti suojattu
- A=vahvimmin suojattu

(Vahti, 2/2013)

5.10 Hajasäteilyriskin pienentämisvaatimuksia ohjaavat tekijät

Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) 16 pykälän 5 momentin mukaan laadittaessa suojaustasoon I-III kuuluvaa asiakirjaa sähköisessä muodossa ja sitä muokattaessa on pidettävä huolta, että hajasäteilystä aiheutuvia haittoja voidaan riittävästi vähentää.Viestintäviraston ohjetta "Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet" tulee lukea rinnan VAHTI 2/203 – ohjeen kanssa, jossa on esitetty vaatimuksia tai ohjausta hajasäteilyltä suojautumiseksi.(Viestintävirasto 2013)

Lisäksi viestintäviraston ohjeessa on huomioitu soveltaen seuraavat EU:n laatimat hajasäteilyn hallitsemiseen liittyvät määräykset ja ohjeet:
EU:n TEMPEST – toimintojen tietoturvapolitiikka (IASP-07) / EU RESTRICTED
EU:n teknisen tietoturvallisuuden turvallisuusohjeisto TEMPEST- laitteiden valintaan ja asentamiseen (IASG 07-01) / EU RESTRICTED
EU:n teknisen tietoturvallisuuden turvallisuusohjeisto TEMPEST- vyöhykejaottelusta (IASG 07-02)/ EU RESTRICTED
Teknisen tietoturvallisuuden ohjeisto EU:n TEMPEST- vaatimuksista ja niiden arviointimenettelyistä (IASG 07-03) /EU CONFIDENTIAL
Teknisen tietoturvallisuuden ohjeisto EU:n EU CONFIDENTIAL
Teknisen tietoturvallisuuden ohjeisto EU:n TEMPEST – yritysten hyväksymisestä (IASG 07-04) / EU LIMITE

6 Laitonta toimintaa

Tarkasteltaessa Suomen Rikoslakia ja sieltä mahdollisesti löytyviä soveltuvia rikoksia voidaan todeta, että hajasäteilyhaavoittuvuutta hyväksikäyttävä hyökkäys ei aivan yksiselitteisesti sovi mihinkään nykylainsäädännön pykälään vaan Rikoslakia on sovellettava tapauskohtaisesti. Osaltaan tähän vaikuttaa se, että kyseessä on ns. "passiivinen toimi", eli hyökkääjä ei lähetä itse aktiivisesti mitään, vaan hänen työkalunsa on vastaanotin. Toisaalta hyökkääjän tavoitteena on saada teknisen laitteen avulla haluamaansa tietoa luvattomasti haltuunsa, mikä puolestaan on täysin yksiselitteisesti rikos. Lyhyesti voidaan todeta, että hajasäteilyhyökkäyksellä toteutettu tiedonhankinta on laitonta toimintaa. Rikoslakia sovelletaan tapauskohtaisesti

riippuen laittomasti haltuun saadusta materiaalista (muistio vai viesti), tiedon omistajasta (yksityishenkilö vai yritys), kyseeseen voi tulla Rikoslain 24. luvun 5 § mukainen salakuuntelu tai 6 § salakatselu tai näiden törkeä muoto, Rikoslain 38. luvun 3 § mukainen viestintäsalaisuuden loukkaus tai Rikoslain luvun 30. 4 § mukainen yritysvakoilu.

6.1 Hyökkääjän näkökulma

Hyökkääjän näkökulman ymmärtäminen on tärkeää suunniteltaessa suojautumistoimenpiteitä. Hyökkääjän näkökulmasta hänen täytyy a) selvittää hänen kohteensa fyysinen sijainti b) päästä kuuluvuusalueelle tarvittavan laitteiston kanssa salaa (olettaen, että hyökkääjällä on virtalähde, tarvittavat laitteet ja osaaminen ko. laitteiden käyttöön), c) havaittava ja identifioitava kohteen tietokoneesta lähtevä tahaton hajasäteily, sekä d) osattava muuttaa hajasäteilysignaalin sisältämä tieto ymmärrettävään ts. luettavaan muotoon. Hyökkäyksen eteneminen on kuvattu alla kuviossa 1.

Kuvio 1. Hyökkäyksen eteneminen

Ennen kuin hyökkääjä voi aloittaa hajasäteilyyn kohdistuvan hyökkäyksen, hyökkääjän täytyy suorittaa muuta tiedustelua. Hyökkääjän täytyy selvittää kohteena olevan laitteen sijainti ja prosessointiajat. Hyökkääjän motivaatio ja käytössä olevat resurssit määrittelevät hyökkäyksen kohteen valikoitumisen. Myös Yhdysvaltain ilmavoimien hajasäteilysuojautumisohjeissa kehotetaan asettumaan hetkeksi hyökkääjän paikalle: "Aseta itsesi hyökkääjän paikalle. Sinulla on ohjattavanasi henkilö, jolla on korkean tason teknistä osaamista, koulutettu testaukseen ja analyysin tekemiseen, sekä kolmesta viiteen vuotta kokemusta. Varustat tämän henkilön tarvittavalla laitteistolla, useilla vastaanottimilla, demodulaattoreilla, oskilloskoopilla, monitorilla, nauhoittimilla ja lisälaitteilla. Kuinka paljon olet valmis riskeeraamaan tämän henkilön kanssa? On erittäin epätodennäköistä, että ohjaat tämän henkilön käynnistämään TEMPEST-hyökkäyksen esimerkiksi sotilastukikohtaan. Mikäli tieto on hyökkääjälle elintärkeää ja tämä on ainoa käytettävissä oleva keino tiedon saamiseksi, saatat harkita sitä, mutta riskit ovat hyvin korkeat sillä hyökkääjän on päästävä hyvin lähelle kohdetta, johtuen useista suojautumistoimenpiteistä. Käytä suojautumisessa hyväksesi olosuhteita, jotka pitävät hyökkääjät poissa tai mitkä lisäävät joko fyysistä etäisyyttä tai vyöhykeluokittelua". (Us Air Force Manual 33- 214, Volume 2, 2001).

Hyökkääjän motivaatio voi vaihdella, mutta motivaatiosta riippumatta hyökkääjän tavoite on saada haltuunsa (laittomasti) kohteen hallitsemaa tietoa. Esimerkiksi kohteena voi olla korkean teknologian parissa työskentelevä insinööri, merkittävää poliittista valtaa käyttävä valtiomies, merkittävään ulkomaankauppaan valmistautuvan yhtiön toimitusjohtaja tjms. On sitten kyseessä kilpailija, joka haluaa laittomin keinoin saada tietoonsa kilpailijan uuden tuotteen piirustukset tai toimeksiannon saanut rikollisryhmä, hyökkääjän ensimmäinen selvitettävä seikka, on selvittää missä kiinnostuksen kohteena oleva laite sijaitsee fyysisesti. Otetaan esimerkiksi korkean teknologian parissa työskentelevä insinööri, joka on tekemässä merkittävää läpimurtoa omalla alallaan. Hyökkääjä pyrkii selvittämään missä sijaitsee se laite, mikä sisältää hänen tavoittelemaansa tietoa, hyökkääjä voi joutua kohdistamaan ensitöikseen tiedustelua selvittääkseen kyseisen insinöörin työpaikan sijainnin, sekä työajat.

Tämän jälkeen hyökkääjän on (pystyäkseen kohdistamaan hajasäteilyä hyväksikäyttävää laitonta tiedustelua kohteeseensa) päästävä nk. kuuluvuusalueelle, eli sille alueelle, minkä kiinnostukseen kohteena olevan laitteen hajasäteily todennäköisesti kattaa. Hyökkääjän kannalta on merkittävä ero sillä, minkälainen hyökkäyksen kohteena olevan laitteen ympäristö (kuuluvuusalue) on. Vertailukohteiksi voidaan esimerkiksi ottaa kiinnostuksen kohteena olevan yrityksen "X" monikerroksinen pääkonttori, missä on kulunvalvonta, sekä rakennusta ympäröivä aita, missä kohteena oleva insinööri työskentelee projektinsa parissa maanantaista torstaihin klo 08.00 – 16.00 välisenä aikana, mutta perjantaisin hän pitää etäpäivän ja työskentelee omakotitalostaan käsin esikaupunkialueella. Hyökkääjän näkökulmasta monikerroksinen, vartioitu ja aidattu pääkonttori on haasteellinen monestakin syystä. Hyökkääjän on ensiksi arvioitava, kykeneekö hän selvittämään kiinnostuksen kohteena olevan laitteen fyysisen sijainnin ja saako hän kuljetettua hyökkäykseen tarvitsemansa laitteiston nk. "kuuluvuusalueelle" salassa. Seuraavaksi hyökkääjä pyrkii löytämään mahdollisen tilan tältä kuuluvuusalueelta, jonne hänellä on pääsy ja jossa hän voi käyttää laitteistoaan salassa. Tällainen tila voi olla esim. kadun toisella puolella oleva hotellihuone, jonne hyökkääjä kuljettaa tarvitsemansa laitteet matkalaukuissa.

Hyökkääjä pyrkii saamaan käyttöönsä tilan sellaisella sijainnilla, että kohteen ja hänen välillään on esteetön näköyhteys, samalla korkeudella. Tämä edellyttää, että hyökkääjä on selvittänyt kohteena olevan insinöörin työskentelyhuoneen summittaisen sijainnin. Huoneen tarkalla sijainnilla ei ole merkitystä mikäli tietokoneen signaali on sähkömagneettisesti havaittavissa hyökkääjän toimesta. Insinöörin työhuoneen summittaisen (tai jopa tarkan) sijainnin selvittämiseen on erilaisia keinoja ja riippuen sijainnista ja yhtiön turvallisuustoimenpiteistä se on hyökkääjälle joko helppoa, vaikeaa tai mahdotonta (riippuen myös hyökkääjän osaamisesta, resursseista ja käytettävissä olevasta ajasta). Yksi tapa jolla hyökkääjä voi pyrkiä selvittämään monikerroksisesta rakennuksesta hänen kohteenaan olevan insinöörin työhuoneen summittaisen sijainnin on tarkkailla insinöörin työskentelyaikoja. Hyökkääjän on jälleen huo-

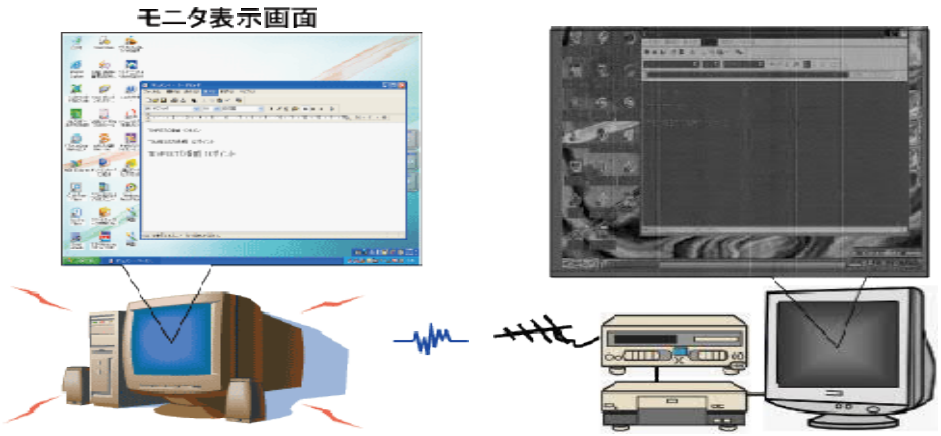
mattavasti vaikeampaa identifioida juuri hänen kohteenaan olevan insinöörin koneen hajasäteily yhtiön pääkonttorin mahdollisesti satojen muiden tietokoneiden hajasäteilyn joukosta, jos kohteena oleva insinööri käynnistää ja sammuttaa tietokoneensa samassa rytmissä muiden yrityksen työntekijöiden kanssa, esim. käynnistys maanantain ja torstain välillä aikaikkunassa 08.00 – 08.30 ja sammuttaa tietokoneensa satojen muiden kanssa myös maanantain ja torstain välillä aikaikkunassa 16.00-16.30. Hyökkääjän mahdollisuudet identifioida kohteena olevan insinöörin käyttämä tietokone paranevat huomattavasti, mikäli hyökkääjä havaitsee esimerkiksi, että tiettynä päivänä insinöörin käyttämä ajoneuvo onkin myöhään iltaan yrityksen pihalla kun klo 17.00 mennessä suurin osa yrityksen työntekijöistä ovat lähteneet ja sammuttaneet tietokoneensa. Tällöin hyökkääjän on huomattavasti helpompi seuloa ja identifioida hänen kohteenaan olevan tietokoneen todennäköinen signaali. Verrattuna tilanteeseen missä hyökkääjä yrittää identifioida hänen kohteensa tietokoneen signaalia satojen muiden signaalien joukosta 08.00-16.00 välisenä aikana vrt. tilanne, missä hyökkääjä havaitsee, että pääsääntöisen 08.00-16.00 virastoajan jälkeen yrityksen pihalla on enää muutama ajoneuvo, ml. kohteen käyttämä auto ja tähän yhdistettynä valot päällä niissä huoneissa missä työntekijät vielä tekevät työtään.

Tällaiset olosuhteet helpottavat huomattavasti hyökkääjään työmäärää ja hänellä on paremmat mahdollisuudet identifioida jatkossa kohteensa tietokoneen signaali kun hänellä on esim. viiden (5) tietokoneen signaalit seulottavana kun samaan aikaan kohteen ajoneuvo on vielä yrityksen pihalla (kohde todennäköisesti rakennuksessa). Näin hyökkääjä voi yhdistämällä havaintojaan lopulta saada selville kohteensa työhuoneen sijainnin. Esim. tarkkailemalla kohteen työpaikan pysäköintipaikkaa varhain aamulla, kunnes kohde saapuu töihin autollaan ja kävelee rakennukseen sisälle ja tämän jälkeen tarkkailemalla missä huoneessa mahdollisesti syttyy valo ja mikä tietokoneen signaali ilmestyy hänen laitteistolleen samaan aikaan. Hyökkääjän jatkaessa tätä edellä mainitun kaltaista toimintaansa hän voi todennäköisesti saada identifioitua kohteen käyttämän tietokoneen signaalin, jonka jälkeen hän voi kohdistaa laitonta tiedustelua kyseiseen tietokoneeseen hajasäteilyä hyväksikäyttämällä. Hyökkääjän työ helpottuu huomattavasti, mikäli kohteena oleva henkilö esimerkin omaisesti tekee perjantaisin töitä ns. ”etänä” kotoaan käsin samalla tietokoneella. Tällöin hyökkääjän on huomattavasti helpompaa identifioida kohteena olevan tietokoneen signaali. Hyökkääjän tarvitsee jälleen päästä kuuluvuusalueelle, kohteen omakotitalon lähelle laitteittensa kanssa. Esimerkkitapauksessa hyökkääjä menee alueelle esim. vuokraamaansa naapuritaloon tai matkailuautoon aikaisin perjantaina, laittaa laitteensa valmiiksi ja havainnoi onko kuuluvuusalueella vielä ko. kellon aikaan yhtään tietokoneen signaalia. Samaan aikaan hyökkääjä voi pyrkiä tekemään silmämääräisiä havaintoja, esim. kohteen omakotitalon makuuhuoneessa syttyy aamulla valot jne. Hieman tämän jälkeen hyökkääjän laitteet havaitsevat kuuluvuusalueelle ”ilmestyvän” tietokoneen signaalin, eli joku on käynnistänyt kuuluvuusalueella tietokoneensa. Mikäli hyökkääjä(t) havaitsevat samaan aikaan silmämääräisesti, että kohde on esim. takapihallaan kan-

nettava tietokone sylissään, hyökkääjä voi olla melko varma, että hänen laitteensa havaitsema signaali on hänen kohteensa tietokoneen signaali, varsinkin jos hyökkääjän laitteet eivät havaitse samaan aikaan muita signaaleja. Tämän jälkeen hyökkääjän on huomattavasti helpompi identifioida seuraavana maanantaina yrityksen pääkonttorilla satojen tietokoneiden joukosta hänen kohteensa tietokoneen signaali. Hyötysignaalin eristäminen on yleensä hyökkääjän näkökulmasta vaikein osa hänen tavoittelemansa tiedon haltuun saamiseksi.

6.2 Hyökkääjän tarvitsema laitteisto

Hyökkääjä tarvitsee käyttöönsä 1) tietokoneen, 2) oskilloskoopin, 3) antennit 10 MHz -3GHz taajuusalueelle hajasäteilysignaalien vastaanottamiseksi, 4) taajuusspektrin (taajuusanalysaattori), oskilloskoopin havainnollistamien signaalien muuntamiseksi numeeriseen muotoon, sekä 5) tietokoneohjelman oskilloskoopin muuntaman numeerisen tiedon muuntamiseksi selkokieliseen muotoon esim. tekstiksi, kuvaksi tjms. Alla on esimerkinomainen kuva (kuvio 2.) selkiyttämään hajasäteilyhyökkäyksen ymmärtämistä. Vasemmalla on hyökkäyksen kohteeksi joutunut tietokone ja oikealla on hyökkääjän laitteisto.



Kuvio 2. Hajasäteilyhyökkäys yksinkertaistettuna

Lähde: https://climateviewer.wordpress.com/2014/01/18/nsa-tempest-attack-can-remotely-view-computer-cellphone-screen-using-radio-waves/

Internetistä löytyy runsaasti materiaalia missä kuvataan hajasäteilyhyökkäys, esimerkiksi youtubesta löytyy videoita missä kuvataan hajasäteilyhyökkäys "laboratoriomaisissa" olosuhteissa. Seuraavista linkeistä on tämän työn tekohetkellä löydettävissä videoita aiheesta: https://www.youtube.com/watch?v=AFWgIAgMtiA, sekä https://www.youtube.com/watch?v=HjhS_JQ80k.

6.3 Antenni

Antenni on radiolaitteiston osa, jota käytetään lähettämään ja vastaanottamaan sähkömagneettisia aaltoja (radioaaltoja). Antenni on sähkömagneettisten aaltojen lähettämiseen ja vastaanottamiseen suunniteltu laite, joka siirtää sähköisen suurtaajuustehon sähkömagneettiseksi kentäksi välineeseen tai vastaavasti siirtää tulevan sähkömagneettisen kentän laitteiston vastaanottimeen. Erilaisia antenneja on yllättävän monissa sovelluksissa mm. radio- ja televisiotekniikka, erilaiset tutka- ja satelliittijärjestelmät, matkapuhelinteknologiat yms. Hajasäteilyyn liittyviä suojaustoimia suunniteltaessa on erittäin tärkeätä ymmärtää, että antenneja syntyy myös tahattomasti. Esimerkiksi päätelaitteen välittömässä läheisyydessä oleva kupariputki voi toimia antennin tavoin ja johdattaa päätelaitteeltaä lähtevää hajasäteilyä tilan ulkopuolelle putkea pitkin. Esimerkiksi auton moottorin virtakaapeli voi toimia antennina ja aiheuttaa esimerkiksi häiriöitä mittalaitteisiin tai jopa itse moottorin ohjaukseen.
Antennit voidaan jakaa kahteen pääryhmään: suunta-antenneihin ja ympärisäteileviin antenneihin. Suunta-antenneja käytetään silloin, kun tiedetään lähetys- tai vastaanottosuunta. Suunta-antenneja ovat esimerkiksi paraboliset peiliantennit, joita käytetään satelliittiviestinnässä. Ympärisäteileviä antenneja ovat esimerkiksi mastoantennit, joita käytetään esim. matkapuhelinviestinnässä. Lähetysantennin tehtävänä on säteillä lähettimen muodostama signaali sähkömagneettisena aaltona ulos antennilla ja vastaanottoantennin tehtävänä on siepata mahdollisimman suuri teho vastaanotettavasta radioaallosta. Antennien tärkeimpiä sähköisiä ominaisuuksia, joiden perusteella voidaan arvioida antennin sopivuus tiettyyn käyttötarkoitukseen, ovat säteilykuvio, suuntaavuus, keilan leveys, polarisaatio, ristipolarisaatio, hyötysuhde, sivukeilataso, vahvistus (yksikkönä desibeli, dB), impedanssi, eli vaihtovirtavastus, häviöt, sekä kaistanleveys eli taajuudet, joilla antenni toimii (usein yksikkönä MHz), sekä resonanssitaajuus eli taajuus, jolla antenni resonoi eli toimii parhaiten. On myös huomioitava, että antenni on ns. resiprookkinen laite, eli että antennin ominaisuudet eivät riipu siitä, käytetäänkö sitä lähetys- vai vastaanottoantennina.(Granlund 2001) Radioaaltojen taajuusalueita ja käyttöesimerkkejä on kuvattu alla taulukossa 4.
Radioaaltojen taajuusalueita

Lyhenne	Nimi	Taajuus	Aallon pituus	Käyttöesimerkki
VLF	Hyvin pitkät aallot	3-30 kHz	10-100 km	Radionavigointi
LF	Pitkät aallot	30-300 kHz	1-10 km	Pitkän matkan radioyhteys
MF	Keskipitkät aallot	300-3000 kHz	100-1000 m	Yleisradio
HF	Lyhyet aallot	30-300 MHz	10-100m	Yleisradio ja radioamatöörit
VHF	Hyvin lyhyet aallot	30-300Mhz	1-10m	Televisio ja ularadio
UHF	Ultralyhyt aalto (ula)	300-3000MHz	100-1000 mm	Radiolinkit, televisio ja tutka
SHF	Mikroaallot	3-30 GHz	10-100 mm	Mikroaaltouuni

EHF	Erikoislyhyet aallot	30-300 GHz	1-10mm	Tutka ja radiolinkit

Taulukko 4. Radioaaltojen taajuusalueet. Lähde: http://jkorpela.fi/smag.html

TEMPEST -suojaamattomien tietokoneiden tuottaman hajasäteilyn signaalien vastaanottamiseen tarvitaan antenni, mikä on tehty taajuuksille 100 Hz – 1000 MHz. Kuten aikaisemmin on todettu, tila missä käsitellään III - II luokan turvaluokiteltua tietoa tulee olla TEMPEST- suojattu. Ainoa varma tapa varmistua tilan riittävästä TEMPEST- suojauksesta on ammattilaisen suorittama vaimennusmittaus. Testimittauksella tarkoitetaan nimensä mukaisesti tilan ympäristössä suoritettavia mittauksia, joiden tarkoituksena on selvittää pääseekö suojatusta tilasta hajasäteilyä ns. ”vuotamaan” ulos. Mittaus on ainoa tapa saada varmuus suojatun tilan hajasäteilyn eristys- ja vaimennuskyvystä. Toisin sanoen, sekä tilan suojauksesta vastaava kuin hyökkääjäkin tarvitsevat käyttöönsä samoille taajuuksille tarkoitetun antennin. Antennit jotka ovat tehty taajuuksille 100 Hz – 1000MHz ovat kooltaan sellaisia, että ne mahtuvat eriteltyinä osiin esim. keskikokoiseen matkalaukkuun, jolla hyökkääjä voi kuljettaa antennin käyttämäänsä rakennukseen tai huoneeseen tjms. jossa hyökkääjä voi koota antennin käyttökuntoon. Sisätiloissa esim. kaiuttomissa kammioissa TEMPEST-mittauksiin tarkoitetut antennit ja ulkokäyttöön tarkoitetut antennit poikkeavat ulkonäöltään toisistaan.

Kuvio 3. Kuvassa on esimerkinomaisesti matkalaukkuun mahtuva antenni. https://www.theemcshop.com/antenna-sets-kits-compliance-emc-rf-energy-detection-radiation/932-ah-systems-ak-2g-antenna-kit-for-fcc-mil-std-vde-and-tempest-testing-up-to-2-ghz.html

Erilaisia antenneja on vapaasti saatavilla yleisiltä markkinoilta, mutta haasteena keskivertokansalaiselle on löytää käyttöön soveltuva ns."oikeille" taajuuksille soveltuva antenni. Viestintään tai radiolaitteistoihin perehtymätön henkilö voi löytää suuntaa antavan tiedon, millä taajuuksilla tietokoneet (erityisesti monitorit) yleensä tuottavat hajasäteilyä. Tämän tiedon avulla hyökkääjän ollessa nk. ”keskivertokansalainen” on hänen helppo hankkia itselleen oikeanlainen antenni hyökkäystä varten. Hyökkäykseen soveltuvat antennit ovat ns. kaikkien saatavilla vapailta markkinoilta, hintojen ollessa halvimmillaan alle sata (100) euroa.

6.4 Oskilloskooppi

Oskilloskooppi on mittalaite, joka muuttaa sähköisen signaalin näkyvään muotoon. Tyypillisesti sillä mitataan toistuvaa ilmiötä kuten värähtelyaaltoa. Oskilloskooppi piirtää mitattavan signaalin oskilloskoopin näytölle. Ensimmäiset oskilloskoopit olivat analogisia, mutta markkinoilla on myös digitaalisia, sekä pc oskilloskooppeja. Jotkin uudet digitaaliset oskilloskoopit (mallista riippuen) ilmoittavat mitattavan signaalin taajuuden numeerisessa muodossa (herzeinä). Kuten aikaisemmin on todettu, jokaisella tietokoneen näppäimistön näppäimen painalluksella on ns. oma signaalinsa (hajasäteilyä), oskilloskoopin avulla tämä signaali voidaan muuttaa numeeriseen muotoon (herzeiksi). Signaalien numeeriset muodot syötetään tietokoneohjelmaan, joka puolestaan muuntaa numeeriset muodot esimerkiksi tekstiksi, kuviksi tjms. mitä kohteena olevalla tietokoneella sitten tehdäänkään. Oskilloskoopin ollessa melko yleinen laite varsinkin aloilla missä mitataan sähkövirtaa autokorjaamoista alkaen, erilaisia oskilloskooppeja on vapaasti saatavilla markkinoilta. Hinnat ovat halvimmillaan muutamasta sadasta eurosta tuhansien eurojen hintaisiin ammattikäyttöön tarkoitettuihin laitteisiin. Oskilloskooppeja on analogisia, digitaalisia, sekä pc- oskilloskooppeja ja näillä kaikilla on omat ominaisuutensa. Analoginen oskilloskooppi on ominaisuuksiltaan vaatimattomin, kun taas digitaalisessa oskilloskoopissa on jo muistiominaisuus. Lisäksi digitaalinen oskilloskooppi on mahdollista liittää mittaustietojärjestelmään ja analogisessa oskilloskoopissa ei tällaista ominaisuutta ole. PC-oskilloskoopissa on eniten ominaisuuksia ja se on suunniteltu toimimaan tietokoneella yhteensopivan ohjelman kanssa. Oskilloskoopissa on näyttö, jossa on horisontaalinen viiva, joka kuvaa X – akselia ja vertikaalinen viiva, joka kuvaa Y-akselia. X-akseli kuvaa signaaliin kulunutta aikaa (yleensä sekunteina) ja Y-akseli kuvaa jännitteen tai muun suureen aaltomuotoa. Oskilloskoopin käyttöön löytyy erilaisia seikkaperäisiä käyttöohjeita, jotka ovat helposti saatavilla esim. internetistä. Oskilloskoopin käyttö vaatii siihen perehtymättömältä harjoitusta ja perehtymistä käyttöohjeisiin, kun taas esim. sähkömiehen koulutuksen saaneella on jo huomattavasti paremmat lähtökohdat laitteen käyttöön. Kuten aikaisemmin on mainittu oskilloskooppeja on erilaisia, alla on kuva digitaalisesta oskilloskoopista. Kuviossa 4. on esimerkinomaisesti kuvattu oskilloskooppi sen tunnistamisen helpottamiseksi.

Kuvio 4. http://www.radio-electronics.com/info/t_and_m/oscilloscope/oscilloscope_types.php

6.5 Tietokoneohjelma "analyysisofta"

Tietokoneohjelma mikä muuttaa radiosignaalit luettavaan muotoon on oleellinen osa tarvittavaa välineistöä. Tarkoitukseen soveltuvia tietokoneohjelmia voi ostaa eri valmistajilta.

6.6 Signaalispektri (Signal spectrum analyser)

Signaalispektrejä on vapaasti saatavilla, oikean taajuusskaalan valinta on helppoa, mutta käyttö vaatii jo osaamista ja ymmärrystä tulkittavasta tiedosta.Laitteiston yhdistäminen ja käyttäminen hajasäteilyn vaatii osaamista ja harjoittelua. Laitteiston sopivuus esim. oikeanlaisen antennin valinta, oskilloskoopin käyttö sekä signaali analysoija ja tietokoneohjelman käyttö vaatii perehtyneisyyttä, motivaatiota, sekä harjoittelua. Yllämainittujen laitteiden lisäksi on olemassa muitakin laitteita, mitä voidaan käyttää hyökkäyksen tekemiseen, mutta niitä ei esitellä tässä työssä. Laitteiden tuloksekas käyttö ei onnistu asiaan perehtymättömältä. Laitteiden käyttäminen vaatii hyökkääjältä koulutusta, kokemusta, motivaatiota, sekä taloudellisia resursseja.

7 Suojautumistoimepiteet

7.1 Hajasäteilyyn liittyvät suojausvaatimukset

Sähkömagneettisen hajasäteilyn uhka on kansainvälisten vaatimusten mukaisesti otettava huomioon jo korotetun tason tiedonkäsittely-ympäristöissä. Kansallinen ohjeistus antaa erityisesti korotetun tason suojausvaatimusten toteuttamiselle enemmän tulkintavaraa.
Uhkaa torjutaan riskiarvioon ja mahdollisesti vaimennusmittauksiin perustuen kansainvälisen TEMPEST-standardin mukaisin toimenpitein. Standardi ei ole julkinen. Standardin kansallisesta tulkinnasta ja suojautumisen ohjauksesta vastaa toimivaltaisena viranomaisena Viestintäviraston NCSA-FI -yksikkö. Hajasäteilyn vastatoimet voidaan jakaa karkeasti kahteen menetelmään: laitteiden suojaaminen metallikoteloinnilla tai työskentelytilan suojaaminen rakenteellisilla ratkaisuilla. Tavoitteena on, ettei salassa pidettävää tietoa pääse vuotamaan tilasta ulos sähkömagneettisen säteilyn välityksellä vaimennusvaatimukset ylittävällä tasolla.

7.2 Hajasäteilyltä suojautuminen käytännössä

Tässä työssä keskitytään vain rakenteellisiin ja laitteiden suojaominaisuuksien kautta saataviin suojaustoimiin. Tässä työssä ei käsitellä radioaaltojen häirintää, eikä "jammausta". Hajasäteilyltä suojautumisen riskienarviointi voidaan toteuttaa VAHTI 2/2013 liitteessä 1 kuvatulla pisteytysmenetelmällä, jolloin hajasäteily on yksi arvioitavista kohteista toimintaympäristön riskienarvioinnissa. Hyvällä suunnittelulla ja huolellisen riskienarvionnin perusteella tehdyillä päätöksillä saadaan tiedot hyvin käytettäviksi ja suojattua kustannustehokkaasti.

7.3 Suojattujen tietojen tunnistaminen

Mikäli organisaatiossa käsitellään pelkästään julkista tai korkeintaan suojaustason IV asioita, ei hajasäteilyä tarvitse ottaa huomioon. Hajasäteilyriski tulee huomioida tätä ylempien suojaustasojen (ST III – ST II), sekä Euroopan Unionin ja Naton CONFIDENTIAL tai sitä korkeampien turvallisuusluokiteltujen tietojen sähköisessä käsittelyssä. Tunnistamisprosessiin kuuluu myös määritellä, kuinka moni ja millaisissa tehtävissä työskentelevä henkilö joutuu ko. tietoja käsittelemään. Hajasäteilyltä suojattavien tietojen käsittelypisteet kannattaa kustannustehokkuutta ajatellen yleensä kehittää.

7.4 Riskien arviointi

Riskien arvioinnin tuloksen perusteella voidaan määritellä millä tavalla hajasäteilysuojaus täytyy ja kannattaa tehdä. Tietoihin kohdistuvia riskejä tunnistettaessa kannattaa pohtia ainakin seuraavia asioista:

Herättävätkö käsiteltävät tiedot sisältönsä perusteella kiinnostusta ulkopuolisissa hajasäteilyn kaappaamiseen kykenevissä tahoissa?
Esimerkiksi sotilaalliseen maanpuolustukseen liittyvät tiedot saattavat kiinnostaa enemmän kuin henkilötiedot.
Mahdollistaako ympäristö hajasäteilyyn kohdistuvan tiedustelun?
Onko samassa kiinteistössä muita ja erityisesti tuntemattomia toimijoita?
Millaiset rakenteet toimitiloissa on? Läpäisevätkö ne helposti sähkömagneettista säteilyä? Onko tiloissa ikkunoita? Ovatko seinät tiiltä, betonia vai kevyttä levyrakennetta? Löytyykö toimitilasta paikkaa, joka olisi keskellä rakennusta ja muutenkin vahvarakenteinen? Onko rakennuksen ympäristö valvottu/aidattu? Tunnistetaan ympäristöstä riskialtteimmat paikat, mistä käsin voitaisiin kohdistaa omiin toimitiloihin suuntautuvaa hajasäteilyn kuuntelua ja kaappaamista. Tällaisia paikkoja ovat erityisesti samassa kiinteistössä tuntemattoman tahon hallinnassa olevat tilat. Tällaisia paikkoja voivat myös olla toimitilojen välittömässä läheisyydessä olevat rakennukset tai muut näkösuojassa olevat paikat, joiden haltijoista ei ole tietoa. (Viestintävirasto 2013)

8 KATAKRI

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on tarkoitettu työvälineeksi niille viranomaisille tai viranomaisten lukuun toimiville turvallisuustarkastajille (auditoijille), joille on annettu valtuus todentaa auditoinnin kohteen turvallisuuden taso erityisesti KATAKRIin peilaten. KATAKRI ja sen suositusosio on suunnattu myös perustyökaluksi yritysten omaehtoiselle turvallisuustyölle. On huomattava, että elinkeinoelämän suositukset eivät ole viranomaisvaatimuksia.Suositusten toteuttaminen on kuitenkin varma ja oikean suuntainen tie yrityksille silloin, kun halutaan varautua etukäteen tilanteeseen, jolloin viranomaisvaatimukset joudutaan täyttämään. KATAKRIn johdannossa kuvataan KATAKRIN päätavoitteet.

Ensimmäisenä päätavoitteena on yhtenäistää viranomaistoimintoja tilanteisiin, joissa viranomainen toteuttaa esim. yrityksessä kohteen turvallisuustason auditoinnin. KATAKRIN toisena päätavoitteena on auttaa yrityksiä ja muita yhteisöjä, sekä viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössään. Kriteeristö sisältää tästä syystä erilliset, viranomaisvaatimusten ulkopuoliset lähtötason suositukset, joista toivotaan voitavan poimia kulloinkin käyttökelpoisia turvallisuuskäytänteitä ja edetä tätä kautta tarvittaessa viranomaisvaatimusten tasolle.

Turvallisuusauditointikriteeristö jakautuu neljään pääosioon: hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Auditointitapahtumassa tulee huomioida näiden kaikkien neljän osion vaatimukset, eli niitä ei ole rakennettu itsenäisiksi kokonaisuuksikseen. Jokaiselle osiolle on laadittu kolmiportainen vaatimusluokittelu, joka vastaa paraikaa laajamittaisesi käyttöön otettavia turvallisuustasokäsitteitä - perustaso, korotettu taso ja korkea taso. Näitä täydentävät edellä mainitut lähtötason suositukset. Kriteeristö on rakennettu ehdottomien vaatimusten näkökulmasta, eikä se sisällä joissakin kriteeristöissä käytettävää pisteytysmenettelyä. Tällä on pyritty siihen ettei, auditoinnin lopputulokseen jäisi mahdollisesti tunnistamattomia, mutta kriittisiä riskejä.

Riskianalyysin perusteella tehdään suunnitelma (suunnittelu ja toteutus) tietojen suojaamiseksi hajasäteilyltä. Jokaisen suojautumistoimenpiteen hinta tulee arvioida erikseen ja yhdessä. Analysoi suunnitelmaan sisältyvien suojaustoimien tulokset ja määrittele ovatko ne hyväksyttävissä (ts. järkeviä, käytännöllisiä ja kustannustehokkaita). Yhdysvaltain puolustusministeriön vuonna 1994 tilaaman raportin tuloksena todettiin, että satoja miljoonia dollareita on käytetty haavoittuvuuden suojaamiseksi, jonka hyväksikäytön todennäköisyys on hyvin matala. Valiokunta suositteli, että kotimaassa (Yhdysvalloissa. kirj.huom.) TEMPEST- vastatoimia(suojaustoimet) ei oteta käyttöön poikkeuksina erityista suojaa vaativa tieto ja silloinkin

vain osaston tai toimiston ylimmän johdon valtuuttamana. (Air force manual 33-214, Volume 2, 2001, emission security countermeasures reviews). Toisin sanoen voidaan todeta, että jo vuonna 1994 TEMPEST suojaustoimien tarpeellisuutta arvioitiin hyöty-hinta arvioinnin perusteella ja valtuutuksen piti tulla korkeimmalta johdolta asti.

Tilanne on jossain määrin samankaltainen tänäkin päivänä, tiettyä kehitystä on kuitenkin tapahtunut mm. on määritelty selkeästi ne tietoturvaluokituksen tasot, jolloin TEMPEST- suojaus on otettava huomioon. Lisäksi TEMPEST suojattuja tuotteita on markkinoilla kalliiden tilaratkaisujen mahdollisiksi vaihtoehdoiksi. Kalleimmillaan esimerksiksi serverihuoneen suojaaminen (Faradayn häkin rakennuttaminen) vaatinee niin suuren budjetoinnin, että sen voi valtuuttaa vain yhtiön tai viraston korkein johto. Suomessa on onneksi saatavilla viranomaisilta asiantuntijatason neuvoja ja ohjausta, joiden avulla suojaustoimien budjetointi on helpompi saada hyväksytettyä yhtiön, viraston korkeimmalla johdolla. Suunnitelman tavoitteena on löytää ratkaisu, jonka tuloksena tietoihin hajasäteilyn kautta kohdistuva riski poistetaan kokonaan tai se jää mahdollisimman pieneksi. Tähän tavoitteeseen päästään seuraavalla tavalla: sijoitetaan tilat, joissa suojattavaa tietoa käsitellään, mahdollisimman kauas sellaisista tunnistetuista paikoista, joista käsin tehtävän tiedustelun uhka on korostunut. Valitaan tietojen käsittelytiloiksi huoneet, joissa ei ole ikkunoita ja joiden rakenteet vaimentavat mahdollisimman tehokkaasti hajasäteilyä (mahdollisimman paksut ja raskaat rakennemateriaalit tai pintojen metallipinnoitteet). Huoneiden ja riskialttiiksi arvioitujen paikkojen välillä on mahdollisimman monta seinää tai vastaavaa rakennetta. Tehdään käytettäväksi suunnitelluille tiloille TEMPEST-mittaukset, joilla voidaan varmentaa riittävä hajasäteilyn vaimennustaso (vaatimus riippuu tiloissa käsiteltävien tietojen suojaustasosta). Mikäli rakennuksen rakenteiden luontaista vaimennusta hyödyntämällä ei saada vaadittua suojavaikutusta, rakennetaan radiotaajuiselta säteilyltä suojattu huone eli (Faradayn häkki) tai otetaan käyttöön hajasäteilysuojatut laitteet (Viestintävirasto 2013).

Liikkuvien johtamispaikkojen suojausratkaisut, yksittäinen kannettava työasema ml., on toteutettava taulukon 3 mukaisesti. Poikkeuksena tästä on ST III-aineiston käsittely sähköisesti, jossa otetaan huomioon 60 päivän sääntö:
Johtamispaikan sijainnin on vaihduttava vähintään kuudenkymmenen (60) päivän välein. Sijainti katsotaan vaihtuneeksi silloin, kun lähettimen sijainti muuttuu vähintään yhden kilometrin verran edellisestä sijainnista riippumatta ympäristöstä.
Kuudenkymmenen (60) päivän sääntöä ei voi noudattaa käsiteltäessä ST II – aineistoa sähköisesti (Viestintävirasto, 2013).

Tarvittaessa valitut ja toteutetut suojausratkaisut tarkastaa ja hyväksyy toimivaltainen TEMPEST-viranomainen. Tarkastaminen perustuu, joko tiedon omistajan laatimaan perusteltuun riskienarviointin, tai tehtyihin mittausraportteihin. Jos tiloissa käsitellään EU:n tai Naton tur-

vallisuusluokiteltuja tietoja, tilat ja suojausratkaisut hyväksyy, toimivaltainen TEMPEST- viranomainen (Viestintävirasto 2013).

Tehdyt suojausratkaisut tulee dokumentoida. Dokumentaatiossa tulee olla vähintään seuraavat asiakirjat: Tilojen suunnitteludokumentit, joissa on perustelut valituille suojausratkaisuille. Mahdolliset tilojen tarkastusdokumentit, joissa on perustelut valituille suojausratkaisuille. Mahdolliset tilojen tarkastusdokumentit ja – lausunnot (mittauspöytäkirjat ml.), sekä päätös hyväksytystä jäännösriskistä. Dokumentaatiota tulee ylläpitää jatkuvasti.

Suojausratkaisuja tulee ylläpitää jatkuvasti ja huolehtia, ettei niiden suojauskyky laske. Erityisesti tämä on huomioitava hajasäteilyltä suojattuja laitteita huollettaessa. Tilojen tarkastaminen mittaamalla tulisi tehdä aina, kun tilaan tehdään sellainen rakenteellinen muutos, jolla on vaikutusta tilan suojaukseen. Määräaikaistarkastukset tulisi tehdä vähintään kolmen vuoden välein (Viestintävirasto 2013).

Lähde: Viestintäviraston sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien aiheuttamien tietoturvariskien ehkäisyn periaatteet 15.11.2013 Dnro: 1305/653/2013

8.1 Suojautumistoimenpiteitä

Suojautumistoimenpiteinä kohteen (tietokoneen tjms. laitteen) fyysinen sijainti tulee olla sellainen, että ko. laitteen sijainnin selvittäminen ulkopuoliselle tehdään hyvin vaikeaksi. Laitteiden joilla käsitellään tietoja, joiden turvaluokitus vaatii TEMPEST – suojautumistoimia, tulee sijoittaa rakennuksissa siten, että niiden lähelle pääsy on rajattua ja kontrolloitua, niiden sijainnin määritys rakennuksen ulkopuolelta on vaikeaa tai mahdotonta.

Tämä tarkoittaa käytännössä sitä, että edellä mainitun kaltaisia turvaluokiteltuja tietoja käsitellään laitteella, joka on huoneessa mikä puolestaan on sijoitettu rakennuksen keskelle tai jopa maapinnan alapuolelle. Tällaisella sijoittelulla varmistetaan, että laitteen ympärillä on mahdollisimman paljon rakenteellista eristystä vaimentamassa laitteesta lähtevää hajasäteilyä, sekä huoneen ulkopuolelta ei voida havainnoida mitä ko. huoneessa tehdään (ikkunaton). Vrt. Tilanne missä hyökkääjällä on esteetön näköyhteys ikkunan kautta kohteen työhuoneeseen, jolloin hän tietää milloin kohteen tietokone on päällä ja milloin ei verrattuna tilanteeseen, jossa hyökkääjällä ei ole tätä tietoa.

Edellä mainitut ohjeet mitätöityvät mikäli turvaluokiteltuja tietoja käsitellään turvallisuusohjeiden vastaisesti esimerkiksi ottamalla sama tietokone mukaan kotiin etätyöskentelyn mahdollistamiseksi.Etätyön osalta voidaan todeta, että jokaisen työntekijän tulee lähtökohtaisesti toimia oman työntantajansa etätyölle asetettujen ohjeiden mukaisesti, TEMPEST– suojaustoi-

met huomioiden, mikäli käsiteltävän tiedon turvaluokitus niin vaatii. Mikäli etätyönä on aikomus käsitellä turvaluokiteltua tietoa, mikä edellyttää TEMPEST- suojaustoimia on kyseiset vaatimukset täytyttävä (kyseeseen tulee ainoastaan TEMPEST-suojatun laitteiston käyttö) ja mikäli tämä vaatimus ei täyty (esim. käytössä TEMPEST- suojaamaton kannettava tietokone) niin tällöin TEMPEST- suojausta vaativia tietoja ei tule käsitellä etänä.

8.2 Kaapelointimateriaalit

Kaapeloinneissa on käytettävä mahdollisimman paljon valokuituja. Valokuitukaapelit eivät reagoi millään tavoin sähkömagneettiseen säteilyyn ja kestävät melko hyvin palokuormaa. Valokuidun salakuuntelu on vaikeaa ja edellyttää fyysistä käsiksi pääsyä kaapeliin. Tästä syystä valokuidun kautta välitetyn dataliikenteen salausvaatimus voidaan tapauskohtaisesti omassa hallinnassa olevan tilakokonaisuuden sisällä korvata fyysisen pääsynhallinnan ja – valvonnan menetelmillä. Valokuitukaapelien käyttöä puoltaa myös niiden siirtonopeus, suuri kaistaleveys, kestävyys, sekä pieni koko ja paino. (Vahti 2013)

8.3 Faradayn häkki

Michael Faraday (1791 – 1867) oli englantilainen tiedemies, joka vaikutti suuresti sähkömagnetismin ja sähkökemian syntymiseen. Faradayn häkki on sähköä johtavasta materiaalista valmistettu häkki tai muu yhteinen kuori, jota, staattinen sähkökenttä, audio- tai radiotaajuinen sähkömagneettinen säteily eivät läpäise. Toisin sanoen Faradayn häkin sisäpuolella oleva sähkömagneettisen kentän lähde ei vaikuta häkin ulkopuolella, ja sähkömagneettinen kenttä ei pääse häkin ulkopuolelta sen sisäpuolelle.
Faradayn häkki on nimetty fyysikko Michael Faradayn mukaan. Hän rakensi vuonna 1836 ensimmäisen Faradayn häkin. Monissa sähkölaitteissa, varsinkin radiolaitteissa, on osia, jotka eivät saa lähettää tai vastaanottaa sähkömagneettista säteilyä. Siksi sellaiset osat tyypillisesti suojataan metallikotelolla tai metallin säästämiseksi metalliverkkokotelolla. Tällaisia metallikoteloita voi olla laitteen sisällä useita. Myös koko laite voi olla metallikotelossa juuri häiriöeristyksen takia. Ydinräjähdysten EMP (electromagnetic pulse) sähkömagneettinen pulssi, rikkoo elektronisia laitteita. Yhteiskunnalle välttämättömät laitteet ja etenkin sotilaskäyttöön tarkoitetut laitteet rakennetaan EMP-suojattuun tilaan, joka on yhtenäisellä metallilla esim. metalliverkolla kauttaaltaan vuorattu huone, Faradayn häkki.
Lääketieteessä käytetään paljon tutkimuslaitteita, joiden suuren sähkömagneettisen herkkyyden takia ne on rakennettava huoneeseen, joka on rakennettu Faradayn häkiksi.
Jokaisen tuntema mikroaaltouuni on arkinen esimerkki Faradayn häkistä, mikroaaltouunin ovessa oleva verkko yhdistettynä laitteen metallikuoreen estää mikroaaltojen pääsyn uunin ulkopuolelle. Faradayn häkki on tärkeä suojautumiskeino hajasäteilyn tahatonta säteilyä ”pa-

kenemista" vastaan. Faradayn häkki voidaan rakentaa itse suojattavan laitteen ympärille esim. kannettavan tietokoneen kuoret, tai serverien asentaminen erikoisvalmistetun metallivuoratun kaapin sisään. EU:lla, sekä NATO:lla on molemmilla lista akkreditoiduista yrityksistä, joiden tuotteet täyttävät edellä mainittujen organisaatioiden vaatimukset hajasäteilyvuotojen osalta. Nämä tuotteet ovat erikoiskoteloituja tietokoneita, serverikaappeja yms. Joissakin tapauksissa laitteiden sijaan kokonainen huone, esim. neuvotteluhuone tjms. on eristetty metallilla ja näin huoneesta on tehty Faradayn häkki, jottei huoneen sisällä käsiteltävistä laitteista pääse hajasäteilyä huoneen ulkopuolelle. Kokoustilojen lisäksi serverihuoneita ja kokonaisia rakennuksia voidaan suojata (esim. kupariverkolla vuoraamalla) rakentamalla niistä Faradayn häkkejä. Kokonaisen huoneen tai rakennuksen TEMPEST-suojaaminen edellyttää perusteellista tarveharkintaa, koska se on ratkaisuna niin kallis. Tietyillä organsiaatioilla tälläisia tarpeita kuitenkin on.

8.4 Laitehygienia

Termillä "laitehygienia" tarkoitetaan tässä työssä sitä, että TEMPEST-suojattuihin laitteisiin ei tule kiinnittää minkäänlaisia lisälaitteita, jotka eivät ole TEMPEST- suojattuja. TEMPEST- suojattu tietokone on suojattu luokituksensa mukaisesti, mikäli se on ehjä, eikä siihen ole kiinnitetty TEMPEST-suojaamattomia lisälaitteita. Mikäli TEMPEST- suojattuun tietokoneeseen liitetään esimerkiksi tavallinen johdollinen hiiri, hiiren johto käyttäytyy johtimena antennin tavoin ja voi johtaa laitteesta hajasäteilyä, mitä ei pääsisi laitteesta ulos ilman hiiren liittämistä. Sama koskee käytännössä kaikkia TEMPEST-suojaamattomia lisälaitteita. Suojaamattomat lisämuistilaitteet, kuten USB tikut, suojaamattomat kiintolevyt tai erilaiset turvallisuustuotteet, kuten metallinen vaijerilukko, toimii aivan kuten antenni. Esimerkkinä hiiren johto toimii antennina, aivan kuten nykyisissä matkapuhelimissa ei ole antennia radion kuuntelua varten vaan ohjekirjassa todetaan esimerkiksi, että "kuulokkeesi toimivat antennina". Tempest-suojatut laitteet menettävät suojausominaisuutensa, mikäli niihin liitetään TEMPEST-suojaamattomia lisälaitteita. ml. johdot. Johtojen osalta ratkaisu on käyttää kuparisydämisten johtojen sijaan optista kuitua.

Eri valmistajilta löytyy myös vaimennusratkaisuja tietokoneen liittimien suhteen. Esim. monitorijohtojen liittimeen ja tietokoneen liitinosan väliin laitettava filtteri, joka vaimentaa mahdollista hajasäteilyä liittimen kohdalta. Laitehygienian varmistamiseksi on tärkeätä, että TEMEPST-suojatuissa tiloissa ja niiden ulkopuolella on asianmukaiset, selkeät kieltomerkit lisälaitteiden liittämiseksi huoneessa oleviin laitteisiin. Käytännöllinen ratkaisu on asentaa TEMPEST-suojatun tilan ulkopuolelle lukittavat metallilokerot, jotta TEMPEST- suojattuun tilaan menevät henkilöt voivat jättää hallussaan mahdollisesti olevat laitteet kuten matkapuhelimet, USB muistitikut jne. kyseiseen lokerikkoon TEMPEST- suojatun tilan ulkopuolelle.

9 IT laitetilaa uhkaavat riskit

Valtiovarainministeriön Toimitilojen tietoturvaohjeen liitteessä 4, käsitellään IT laitetilojen turvallisuusohjeita. IT laitetilojen riskikartoituksessa kehotetaan etsimään järjestelmällisesti vaaratekijöitä, arvioitava näistä mahdollisesti aiheutuvat menetykset (immateriaaliset, taloudelliset) ja lopuksi asetettava riskit tärkeysjärjestykseen. Kutakin riskiä varten on laadittava vahingontorjuntasuunnitelma ja katastrofiluonteisten vahinkojen varalle toipumissuunnitelma. VAHTI kirjan liitteen 4, mukaan tärkeimmät IT-laitetilaa uhkaavat riskit ovat: tietoturvaloukkaus, tietovarkaus, palo ja räjähdys, vesivahinko, tulva, sähkökatko, jännitehäiriö, laiterikko, lämpötilan nousu, laitevarkaus, inhimillinen erehdys, vahingonteko, vaarallisten aineiden kuljetusväylät, varastot, satamat, teollisuuslaitokset, virus tai muu haittaohjelma, sovellusohjelmiston omat viat tai puutteet, EMP:n ja HPM:n aiheuttamat vahingot, kemiallisten aineiden aiheuttamat vahingot, säteilyonnettomuus. (VAHTI 2/2013)

9.1 Suojautuminen varkautta ja tunkeutumista vastaan

Asiattomien pääsy IT-laitetiloihin on estettävä. Erikseen määritetyn IT-henkilöstön lisäksi ainoastaan laitteiden huoltohenkilöstö ja siivoojat saa päästää laitetiloihin ja hekin vasta sen jälkeen kun he ovat todistetusti todistaneet henkilöllisyytensä ja käyntinsä tarpeellisuuden. Käynnit suoritetaan valvottuina, ottaen huomioon kohteen tärkeys. Kulunvalvonta IT-laitetiloihin on järjestettävä siten, ettei kukaan pääse saapumaan tai poistumaan tulematta rekisteröidyksi (sähköinen loki). Laitetilojen osalta on pyrittävä käyttämään erillistä kulunvalvontajärjestelmää, jota toimitiloissa toimiva organisaatio hallinnoi. Erityistä suojausta vaativissa kohteissa voidaan liikkumista rajoittaa siten, että sisään- tai uloskäyntiovista ei saa yhdellä avauksella päästä kulkemaan kuin yksi henkilö kerrallaan. IT-laitetilaan johtavien ovien ja niiden lukitusjärjestelyjen tulee täyttää pääasiakirjan liitteessä 1 esitetyt vaatimukset. https://www.vahtiohje.fi/web/guest/666

9.2 Suojautuminen sähkömagneettista säteilyä vastaan

IT-laitetiloja suunniteltaessa on selvitettävä, onko lähietäisyydellä jo olemassa tai suunnitteilla niin voimakkaita radiolähettimiä, tutkia tai muita laitteita, että niiden aiheuttama kenttävoimakkuus ylittää tietokonelaitteistojen valmistajan määrittelemän suurimman sallitun kenttävoimakkuuden. Jollei valmistaja tällaista arvoa ilmoita, ohjearvona voidaan pitää kenttävoimakkuutta 1 V/m.
Sähkömagneettisen säteilyn tietoliikennelaitteita tuhoava vaikutus perustuu energiapulsseihin, jotka indusoituvat antenneihin tai antenneina toimiviin johtimiin vaurion syntymisen herkkyys riippuu laitteiston herkkyydestä, sähkömagneettisen kentän voimakkuudesta ja antennien sekä antenneina toimivien johtimien ominaisuuksista. Tällaisen suurienergisen säh-

kömagneettisen pulssin voi synnyttää joko korkealla tapahtuva ydinräjähdys (EMP) tai radiotaajuinen ase (konventionaalinen EMP-ase tai suurtehomikroaaltoase, HMP). Sähkömagneettisilta aseilta suojautumisen tarve ratkaistaan uhka-arvion perusteella, omien laitteiden osalta sähkömagneettinen hajasäteily tulee huomioida suojaustasolta III alkaen ja tarvittaessa on ryhdyttävä ns. TEMPEST- vastatoimiin toimivaltaisen viranomaisen* ohjauksen mukaisesti. Toimivaltaisella viranomaisella tarkoitetaan Viestintäviraston NCSA- yksikköä. https://www.vahtiohje.fi/web/guest/666

9.3 TEMPEST valtuutetut yritykset

Euroopan Unionilla on lista TEMPEST valtuutetuista yrityksistä, joiden tuotteet täyttävät niille asetetut vaatimukset. Lista löytyy internetistä osoitteesta: www.consilium.europa.eu/figeneral-secretariat/corporate-policies/classified-information/information-assurance/tempest/. Lisäksi lista yrityksistä on tämän työn liitteenä (Liite 1). Natolla on myös oma vastaava lista Naton hyväksymistä yrityksistä TEMPEST-suojattujen tuotteiden osalta. Osa näistä yrityksistä ovat molempien (EU & Nato) listoilla. Tässä työssä mainitaan ainoastaan Euroopan Unionin hyväksymät yritykset. Tämä valtuutus on usein esitetty englanniksi seuraavasti:"Accredited TEMPEST Company". EU:n dokumentissa IASG 7-04 "Information Assurance Security Guidelines on Accredtiation of EU TEMPEST Companies", määritellään termiä "TEMPEST company" seuraavasti: TEMPEST- yrityksen pääsy valtuutettujen yritysten listalle edellyttää yritykseltä seikkaperäistä yritysturvallisuuden hallintaa. TEMPEST- yrityksen määritelmään sisältyy mm. seuraavia asioita: TEMPEST- yhtiöllä on itsellään kaikki tarpeelliset kyvyt liittyen TEMPEST- laitteiston kehitystyöhön, testaukseen, tuotantoon, sekä huoltoon. TEMPEST- yhtiö, mikä on erikoistunut TEMPEST- testaukseen ja tarjoaa tätä osaamista muille yhtiöille. TEMPEST- yhtiö, joka tuottaa TEMPEST- tuotteita sertifioituun prototyyppiin perustuen, sekä myy tuotteita.

EU:n dokumentissa "Information Assurance Security Guidelines on Accredtiation of EU TEMPEST Companies" kuvataan mm. seuraavia vähimmäisvaatimuksia, joiden tulee täyttyä ennen kuin yritykselle voidaan myöntää TEMPEST- valtuutus. Turvallisuusseikkoja, joiden tulee olla kunnossa:fyysinen turvallisuus, yrityksen henkilöstön asianmukaiset turvallisuuselvitykset, IT järjestelmien turvallisuusvaltuutukset, yritysturvallisuus, testauslaitteiden (mittauslaitteiston) hyväksytty kalibrointi, ISO 9001:2008 todistus, ISO 17025:2005 todistus.

EU:n dokumenteissa on kuvattu useita eri seikkoja, joiden perusteella kiinnostunut ostaja voi näiden kriteerien perusteella päättää itse minkä yrityksen tuotteet ja/ tai palvelut hän kokee luotettavimmiksi. Esittelyosta jo käy selväksi, että dokumentin tarkoitus on tukea jäsenval-

tioden asiakkaita löytämään nopeasti valtuutettuja TEMPEST-yhtiöitä ja näin selkeyttää ja parantaa hankintaprosessia. Asiakkaan hankkiessaan TEMPEST-tuotteita kansallisilta tai kansainvälisiltä markkinoilta häneltä voi usein puuttua asiaan liittyvä tietoa ja tai testauslaitokset varmistaakseen, että tarjotut (tai lopulta toimitetut) TEMPEST-tuotteet täyttävät todellisuudessa EU:n TEMPEST- standardin vaatimukset ja joutuu yksinkertaisesti vain luottamaan yhtiön itsensä ilmoittamaan tietoon (EU standardista). Välttääkseen edellä mainitun kaltaisen tilanteen ja saadakseen varmuuden laitteiden laatukriteereistä, asiakakkaalla on mahdollisuus ottaa yhteyttä Viestintäviraston kansalliseen TEMPEST-viranomaiseen (NTA:han). Kansallinen TEMPEST-viranominen voi antaa asiakkaalle virallisen sertifikaatin tai muun virallisen vakuutuksen, mikä osoittaa, että kyseessä olevan yhtiön tarjoamat TEMPEST-laitteet todella täyttävät EU:n TEMPEST- standardin mukaiset vaatimukset. Tästä syystä EU:n TEMPEST- valtuutetuista yhtiöistä on tehty lista, joka on julkinen. Kuitenkin voidaan tiivistettynä todeta, että EU:n (tai Nato:n) valtuuttamalle listalle päässeet yritykset ovat käyneet läpi hyvin seikkaperäiset turvallisuuselvitykset ja läpäisseet ne. Kaikkien alla mainittujen yritysten kotisivut ovat luettavissa englanniksi ja sisältävät tietoa hajasäteilystä, TEMPEST-suojauksesta, sekä esittelyjä yritysten valmistamista TEMPEST- suojatuista laitteista ja asiantuntijapalveluista. TEMPEST- suojattujen laitteiden lisäksi saatavilla on tuotteita, jonka avulla asiakas voi suojata esim. oman tablettinsa ostamalla yritykseltä TEMPEST- suojatun kotelon laitteelleen. TEMPEST- suojatut laitteet on luokiteltu kahteen (2) luokkaan niiden TEMPEST- suojauksen vaimennusominaisuuksien mukaan. Level A on kuvattu täyden suojauksen tuotteeksi ja level B keskitason suojauksen tuotteeksi. Karkeasti tuotteiden hinnoista voidaan todeta, että TEMPEST- suojattu tietokone maksaa noin kolme (3) kertaa enemmän kuin vastaava suojaamaton "normaali" tietokone. TEMPEST- suojattu laitekaappi (jääkaapin kokoinen) maksaa puolestaan noin kaksikymmentä tuhatta (20 000) euroa. Yritysten myymiä tuotteita ovat: pöytätietokoneet (keskusyksiköt), kannettavat tietokoneet, virtalähdefiltterit, monitorit, tulostimet, skannerit, USB hubit (USB jakajat), tietokonekaapit (eri kokoisia), sekä ulkoiset DVD asemat.

10 Tilaratkaisut

Yksittäisen tietokoneen suojaaminen on luonnollisesti kustannustehokkaampaa kuin kokonaisen tilan tai huoneen suojaaminen, mutta joskus organisaation tarpeet ovat sellaiset, että kokonaisia huoneita täytyy suojata rakenteellisesti. Yhdysvaltain ilmavoimien hajasäteilyturvallisuuden suojaustoimien käsikirjassa (Air force manual 33-214, Volume 2, 2001, emission security countermeasures reviews) termi "tarkastettava tila" kuvaa erinomaisesti oleellisen. Käsikirjan mukaan kontrolloitaessa vaarantavaa hajasäteilyä, hajasäteilyä tuottavat laitteet (joilla turvaluokiteltua tietoa käsitellään) on sijoitettava tilaan mikä on tarkastettavissa. Tarkastettavan tilan määritelmä on se kolmiulotteinen tila, mikä ympäröi järjestelmiä, joilla käsitellään turvaluokiteltua tai sensitiivistä tietoa, joihin TEMPEST hyväksikäyttöä ei voida pitää käytännöllisenä tai missä on lakiperusteinen peruste tunnistaa ja poistaa mahdollinen TEM-

PEST uhka. Alla olevassa kuvassa on TEMPEST- suojattu huone mikä on sijoitettu rakennuksen sisälle. Huone on rakenteeltaan ja materiaaleiltaan Faradayn häkki ts. tila mikä ei päästä hajasäteilyä ulos eikä sisään. Tila on irti rakennuksen varsinaisista pinnoista (lattia, seinät ja katto), jottei esim. seinien sisällä mahdollisesti olevat metallirakenteet (esim. kupariputket) johda tilasta hajasäteilyä rakennuksen ulkopuolelle. Samasta syystä (kuvan vasemmassa yläkulmassa) huoneen ilmastointiputken ”galvanisaatio on katkaistu” eli metalliseen ilmastointiputkeen on asennettu pätkä muoviputkea. Mikäli TEMPEST- suojatusta huoneesta lähtisi katkeamaton metallipintainen johdin, tässä tapauksessa ilmastointiputki esim. rakennuksen katolle niin tämä mahdollisesti voisi toimia antennin tavoin, johdattaen hajasäteilyä huoneesta putkea pitkin rakennuksen katolle ja rakennuksen ulkopuolelle, jolloin hajasäteily olisi mahdollisen hyökkääjän saatavilla. Mikäli huoneeseen menisi tietokaapeleita, niiden läpiviennit tulee rakentaa erityisellä tarkkuudella ja kaapeloinnissa tulee käyttää optista kuitua ns. perinteisen kuparisydämisen kaapelin sijaan. Oven ja karmien asennuksessa, sekä käytössä tulee noudattaa erityistä huolellisuutta. Tilaan tulee kohdistaa tasaisin väliajoin suojatun tilan vaimennusmittaus, tämä on ainoa keino saavuttaa varmuus siitä, ettei huoneen ympäristössä tai rakenteissa ole tapahtunut sellaisia muutoksia joiden vuoksi huone ”vuotaisi” hajasäteilyä. Toisin sanoen varmistua siitä, että huoneen vaimennus täyttää kansainväliset vaatimukset tai kansalliset vaatimukset 1-3 zoning. Huoneen sijoittelussa tulee huomioida toimitilojen tietoturvaohjeessa mainittu vyöhykkeistäminen, sekä luonnollinen vaimennus. Toisin sanoen TEMPEST- suojattu huone tulee sijainniltaan olla sellainen, että sinne pääsy vaatii kulkuoikeuden kyseiselle vyöhykkeelle. Luontaisella vaimennuksella tarkoitetaan sijainnin valintaa siten, että TEMPEST- suojatun huoneen ympärillä on mahdollisimman paljon omassa hallinnassa olevaa rakennusmateriaalia seiniä, kattoja, eli TEMPEST- suojatun huoneen tulisi olla rakennuksen keskellä tai mahdollisuuksien mukaan jopa sijoitettu maanpinnan alapuolelle. Näin huoneen ympärillä on sen oman suojauksen lisäksi mahdollisimman paljon ns. ”luonnollista vaimennusta” seiniä yms. rakenteita. Edellytyksenä on, että TEMPEST-suojatun huoneen ympäröivät tilat (huoneet, kerrokset jne.) ovat omassa hallinnassa ts. esim. seinän takana oleva tila ei ole tuntemattoman tahon hallinnassa (ei tietoa mitä tai kuka on seinän takana) aikaisemmin kuvattu "tarkastettava tila". Kuviossa 5. on kuvattu erään valmistajan näkemys erilaisista TEMPEST suojausratkaisuista.

Kuvio 5. TEMPEST-suojattu tila https://emp-tronic.com/shielding/profishield/

10.1 Kaapelointimateriaalit

Valtiovarainministeriön toimitilojen tietoturvaohjeen luvussa ”suojattavat kohteet ja niitä uhkaavat tekijät” käsitellään mm. IT -laitteistoa uhkaavia tekijöitä ja suojautumistoimenpiteitä. Laitteistoturvallisuuteen liittyy oleellisesti myös kaapelointiturvallisuus. VAHTI ohjeen mukaan kaapeloinnissa on käytettävä mahdollisimman paljon valokuituja. Valokuitukaapelit eivät reagoi mitenkään sähkömagneettiseen säteilyyn ja kestävät melko hyvin palokuormaa. Valokuidun salakuuntelu on vaikeaa ja edellyttää fyysistä käsiksi pääsyä kaapeliin. Tästä syystä valokuidun kautta välitetyn dataliikenteen salausvaatimus voidaan tapauskohtaisesti omassa hallinnassa olevan tilakokonaisuuden sisällä korvata fyysisen pääsynhallinnan ja –valvonnan menetelmillä. Valokuitukaapelien käyttöä puoltaa myös niiden siirtonopeus, suuri kaistaleveys, kestävyys ja pieni koko ja paino.

10.2 Mittaus

TEMPEST-mittaus on ainoa varma keino varmistua siitä, että suojattavan tilan tai kohteen vaimennustaso on riittävä. Kuten Valtiovarainministeriön toimitilojen tietoturvaohjeessa mainitaan, kohteissa, joissa käsitellään suojaustason 3 (ST III) turvaluokiteltua materiaalia tulee huomioida hajasäteilyn uhka. Uhkaa torjutaan riskiarvioon ja mahdollisesti vaimennusmittauksiin perustuen kansainvälisen TEMPEST-standardin mukaisin toimenpitein. Standardi ei ole julkinen. Viranomaisen suorittaman TEMPEST- mittauksen voi saada perustellulla pyynnöllä. Esim. Senaattikiinteistö rakennuttaa asiakkaalleen TEMPEST- suojatun tilan, johon liittyen Senaattikiinteistö esittää perustellun (riskianalyysiin perustuvan) pyynnön Viestintävirastolle, joka sitten organisoi ko. kohteeseen TEMPEST- mittauksen. Mittaukset on tehtävä säännöllisin väliajoin tai kun on tehty muutoksia rakennuksessa tai ympäristössä. Jäljempänä olevissa tau-

lukoissa on kuvattu eri rakennusmateriaalien vaimennusominaisuuksia eri taajuuksilla. Taulukossa 5 on kuvattu eri seinämateriaalien vaimennusominaisuuksia mm. lastulevyn, betonin, tiilin, sekä ikkunan vaimennusominaisuuksia. Taulukossa 6 on puolestaan kuvattu teräsbetonin vaimennusominaisuuksia.

Eri seinämateriaalien vaimennusominaisuuksia eri taajuuksilla:

Seinämateriaali	Taajuus	Vaimennus
Lastulevy	2GHz	4 dB
Lastulevy	60 GHz	5 dB
Betoni	2 GHz	1 dB
Tiili 120 mm	2 GHz	4 dB
Tiili 360 mm	2 GHz	10 dB
Ikkuna	2 GHz	0,5 dB

Taulukko 5.
https://www.finlex.fi/data/normit/41654/Toimitilojen_tietoturvaohje_VAHTI_2_2013_netti.pdf

Teräsbetoniseinän vaimennus eri taajuuksilla on kuvattu seuraavassa taulukossa:

Taajuus GHz	25cm	16cm
1	10dB	8dB
2	14dB	11dB
4	32dB	17dB
6	35dB	31dB
8	58dB	32dB
10	68dB	32dB
12	80dB	32dB

Taulukko 6. (Vahti 2/2013, 68)

Vaatimustaulukon osa-alueet hajasäteilyyn liittyen:

Vaatimus	Perustaso Turvallisuus-vyöhyke VIHREÄ	Korotettu taso Turvallisuus-vyöhyke KELTAINEN	Korkea taso Turvallisuus-vyöhyke SININEN	EU/NATO erityisvaatimukset	Pist.
Hajasäteilyn estäminen	Ei vaatimuksia	Arvioidaan tarve huonetilan tai laitteiden suo-	Tilassa ei käytetä mitään sellaisia elektronisia	NATO: vastatoimet riskianalyysiin pohjau-	

		jaamiseksi TEMPEST-vastatoimin	laitteita, joiden käyttö on kielletty. Lukittavat lokerot matkapuhelimille vyöhykkeen ulkopuolelle. Arvioidaan tarve huonetilan tai laitteiden suojaamiseksi TEMPEST-vastatoimin, samoin kuin tarve EMP-/HPM-suojaukselle.	tuen. EU: vasta-toimet riskianalyysiin perustuen EU CONFIDENTIAL –tasolta alkaen.	

https://www.finlex.fi/data/normit/41654/Toimitilojen_tietoturvaohje_VAHTI_2_2013_netti.pdf

Kuusi tuumaa vahvistettua sementtiä antaa nimellisen kahdenkymmenen (20) desibelin (dB) vaimennuksen. Kun tarkistettava tila on määritelty etäisyydeltään valettu betoni lattia tai katto antaa n. 20 dB vaimennuksen lisäten yhden vyöhykeluokituksen kyseiseen suuntaan. Tuo on, kun tarkastettava tila yhden metrin mutta vähemmän kuin 20 metriä (Vyöhyke A) tarkastettavan tilan luokitus muuttuu vyöhykkeeksi B tai kun tarkastettava tila on 20 metriä mutta vähemmän kuin 100 metriä (vyöhyke B) tarkastettavasta tilasta tulee vyöhyke C jne. Tämä siksi, että vyöhykkeet ovat 16 dB erillään. Kahdeksan tuumaa paksu vahvistettu betoniseinä antaa n. 12 dB vaimennuksen tai 3/4 vyöhykettä. Tiiliseinä antaa n. 4 dB vaimennuksen tai ¼ vaimennuksen. (Air Force Manual 33-214, Volume 2, 2001, Emission security countermeasures reviews).

Valtioneuvoston 1.7.2010 antama asetus 681/2010 tietoturvallisuudesta valtionhallinnossa on yksi keskeisistä asetuksista sisältäen säännöksiä turvaluokitellun tiedon käsittelystä. Säännökset sisältävät vaatimuksia eri turvaluokituksen omaavien dokumenttien käsittelyn suhteen, säännökset sisältävät vaatimuksia myös TEMPEST-suojaukseen liittyen. Turvaluokitukset on kuvattu tarkemmin alla kolmannen (3.) luvun yhdeksännessä (9.) pykälässä. Lyhyesti voidaan kuitenkin todeta, että turvaluokitukset ovat asteikolla IV – I, tasoilla II ja I tulee huomioida TEMPEST- suojautuminen (Kansallinen turvallisuusauditointikriteeristö 2011).

11 Johtopäätökset

Tiedustelu (hajasäteilyhyökkäkseen soveltuvien) mittauslaitteiden kokonaishinnasta lähetettiin sähköpostitse viidelle (5) eri radiolaitteiden jälleenmyyjäyritykselle. Kaksi (2) yritystä ei vastannut kyselyyn lainkaan, yksi (1) yrityksistä vastasi toteamalla, että heidän yrityksensä valikoimassa ei ole TEMPEST-mittauksiin sopivia laitteita. Yksi (1) yrityksistä pyysi jatkolähet-

tämään tiedustelun yrityksen sähköpostin sijaan yrityksen blogisivustolle, mikä ei ole tarkoituksenmukaista työn ollessa kesken. Ainoastaan yhden yrityksen edustaja osoitti vastauksessaan tietämystä ja vankkaa ammattimaisuutta pyytäen lisätietoja opinnäyteytyöhön liittyen ennen vastauksen antamista. Rohde & Schwarz konsernin Sales and Support Engineer (myynti- ja tuki insinööri) Jouni Salmi vastasi yrityksen sähköpostiin lähetettyihin kysymyksiin saatuaan ensin itse vastauksia tämän työn lähtökohdista, tavoitteista ja tilaajasta. Salmen vastauksesta käy ilmi hänen vankka ymmärryksensä hajasäteilyhaavoittuvuuksiin liittyen. Salmen vastauksesta valittiin tähän työhön relevantein osuus, mikä on kuvattu jäljempänä.

Hajasäteilyä hyväksikäyttävistä tietovarkauksista on saatavilla hyvin vähän tietoa, koska itse tietovarkaudesta ei jää mitään jälkiä. Todennäköisesti epäilyjä tällaisistä tietovarkauksista tai niiden yrityksistä on olemassa, mutta niiden todistaminen on erittäin vaikeaa. On myös todennäköistä, että hajasäteilyä hyväksikäyttävän hyökkäyksen kohteeksi jounutut taho ei halua julkisesti myöntää joutuneensa hyökkäyksen kohteeksi, koska näin menetellessään kohteeksi joutunut taho myöntäisi samalla mahdollisesti laiminlyöneensä tai joka tapauksessa epäonnistuneensa suojautumistoimenpiteiden osalta. Tämä ei luonnollisesti ole kohteeksi joutuneen tahon etujen mukaista, sillä sen maine mahdollisten asiakkaiden tai yhteistyökumppanien silmissä luotettavana toimijana kärsisi. Käytännössä hajasäteilyä hyväksikäyttävän tietovarkauden todistaminen vaatisi miltei sen, että hyökkääjä jäisi kiinni itseteossa siten, että hänet todistettavasti tavattaisiin hyökkäyksen kohteena olevan päätelaitteen signaalin kantoetäisyydeltä erityislaitteiston kanssa, tästäkin huolimatta on mahdollista, että tapaus salattaisiin edellä mainituista syistä.

Tämän työn tutkimuskysymyksiin voidaan lopuksi vastata, että ns. "keskivertokansalainen" ei kykene osaamisensa puolesta käyttämään hajasäteilyhyökkäykseen soveltuvaa laitteistoa. On kuitenkin syytä pitää mielessä, että motivoitunut ja viestintäkoulutusta saanut henkilö tai ryhmä esimerkiksi pitkälle edenneitä radioamatöörejä omaa jo kohtalaiset mahdollisuudet laitteiden käyttämiseen hajasäteilyä hyväksikäyttäviin hyökkäyksiin, etenkin jos mittavat taloudelliset resurssit omaava muu taho rahoittaa ryhmitttymän toimintaa peitelläkseen omaa osuttaan hyökkäyksessä. Vastaus kysymykseen voiko keskivertokansalaisen taloudellisilla resursseilla hankkia hajasäteilyhyökkäykseen soveltuvia laitteita ei ole yksiselitteinen. Korkealaatuisten ja hyvillä ominaisuuksilla varustettujen laitteiden osalta hintahaarukka on laaja, useasta kymmenestä tuhannesta eurosta aina ammattikäyttöön tarkoitettujen laitteiden hintojen lähennellessä yhteensä sataa tuhatta (100 000) euroa. On kuitenkin huomattava, että tarvittavan laitteiston voi hankkia myös huomattavasti halvemmalla kuin maksamalla useita kymmeniä tuhansia euroja. Rohde & Schwarz konsernin Sales and support engineer Jouni Salmen vastaus kysymykseen (kykeneekö "keskivertokansalainen suorittamaan hajasäteilyhyökkäyksen "keskivertokansalaisen" budjetilla hankittavissa olevilla laitteilla: "Muutaman satasen satsauksella pääsee jo näkemään jotain, mutta systeemi ei mitenkään ole lähelläkään

yhteiskuntavastaisen keskivertokansalaisen operoitavissa. Tälläisen harrastajatason systeemin käyttäjän pitää olla erityisen teknisesti pätevä". Lisäksi internetistä löytyy julkaisuja, joissa hajasäteilyhyökkäyksiä on simuloitu esimerkiksi yliopiston tiloissa siten, että hyökkäyksen kohteena oleva tietokone on viereisessä huoneessa kuin hyökkääjä laitteineen. Esimerkkinä voidaan mainita, Motherboard vice julkaisun "How White Hat Hackers Stole Crypto Keys from an Offline Laptop in Another Room" mukaan tutkijat saivat hankittua laitteet noin kolmella tuhannella (3000) Yhdysvaltain dollarilla (https://motherboard.vice.com/en_us/article/xygdwq/how-white-hat-hackers-stole-crypto-keys-from-an-offline-laptop-in-another-room).

Lisäksi on huomioitava, että mikäli hyökkääjällä ei ole käytettävissään merkittäviä taloudellisia resursseja, hyökkäystä suunnittelevalle jää silti vaihtoehtoja laitteiden hankkimiseen edullisesti. Hyökkäystä suunnitteleva voi hankkia laitteet käytettynä tai tilaamalla laitteet markkina-alueensa ulkopuolelta esim. Kaukoidästä edullisemmin. Tämä on tilanne tätä työtä kirjoitettaessa ja tilanne voi muuttua tulevaisuudessa tekniikan kehittyessä ja tarvittavan laitteiston hintojen mahdollisesti alentuessa. Kaikki tarvittavat laitteet ovat kuitenkin täysin laillisesti hankittavissa esimerkiksi radiolaitteiden valmistajilta, tai hyvin varustelluilta jälleenmyyjiltä. Lisäksi voidaan vielä kertauksen omaisesti todeta, että mittauksella on aivan kriittinen merkitys suojaustoimia suunniteltaessa uusiin tiloihin tai tiloihin, joissa on tehty rakenteellisia muutoksia.

Lopuksi voidaan todeta, että tämä työ vastaa Senaattikiineistön sille asettamiin tutkimuskysymyksiin yllämainituin vastauksin. Niin kutsuttu"keskivertokansalainen" ei omaa sellaista osaamista, että hän kykenisi toteuttamaan hajasäteilyhyökkäystä tuloksekkaasti.Tämän työn selvityksen mukaan nykyhetkellä nk. "keskivertokansalainen" omaa suurella todennäköisyydellä sellaiset taloudelliset varat tai ainakin kykenee hankkimaan itselleen sellaiset varat helposti, että hän saa hankittua tarvittavat laitteet hajasäteilyhyökkäyksen suorittamiseksi. On kuitenkin tärkeää tiedostaa, että halvimpien laitteiden ominaisuudet riittänevät mahdollisesti vain helpoissa olosuhteissa suoritettaviin hajasäteilyhyökkäyksiin, esimerkkinä toimistotiloissa tjms. hyökkäyksen onnistumisen kannalta "optimimaalisissa" olosuhteissa. Kalliimmilla, ammattikäyttöön valmistetuilla laitteilla voidaan päästä hyökkääjän kannalta haluttuihin tuloksiin myös haastavimmissa olosuhteissa esim. suurempi etäisyys, enemmän vaimennusta tjms.

12 Luotettavuuden arviointi

Opinnäytetyön tavoitteena oli vastata kappaleen 1.2 (tutkimusmenetelmät, raportin rakenne, sekä opinnäytetyössä käytetyt lähteet) tutkintakysymyksiin ja vastausten kautta tuottaa Senaattikiinteistölle mahdollisimman hyödynnettävää tietoa hajasäteilyhyökkäyksiltä suojautumiseksi. Tiedonkeräämiseen (aineisto ja haastattelut) kohdennettiin tarkoituksella kansallisel-

le asiantuntijalle. Myös aineiston osalta hänen ohjauksensa oli keskeisessä roolissa sillä tavoitteena oli kerätä asiantuntijahaastatteluja tukevaa aineistoa laajalti ja lähteistä joiden luotettavuus katsottiin korkeaksi. Reliabialiteetilla viitataan tarkastelun kohteena olevan tutkimuksen toistettavuutta. Ts. tutkimuksen tulokset ovat samat riippumatta kuinka monta kertaa tai kuka tutkimuksen suorittaa. Reliabiteetin tarkastelu on oleellinen osa tutkimustyötä ja sen tavoite on kuvata sitä onko tutkimuksen tulokset ja johtopäätökset luotettavia.

Asiantuntijahaastattelua tarkasteltaessa voidaan todeta, että asiantuntijana toiminut henkilö on Viestintävaroston erikseen nimeämä valtakunnallinen vastuuhenkilö liittyen Tempestiin suojauksiin ts. hänen ammattitaitonsa tarkastelun kohteena olevan aiheen tiimoilta on oletettavasti valtakunnallisesti vertailtuna aivan huippuluokkaa. Haastateltavia asiantuntijoita on tässä työssä käytännössä ollut vain yksi (1) mihin voitaisiin lähtökohtaisesti suhtautua kriittisesti. Haastateltavia tulisi pyrkiä saamaan useampia, jotta tutkimukseen saataisiin mahdollisimman laajalti asiantuntijoiden näkemyksiä. Tässä työssä se ei kuitenkaan ollut mahdollista kappaleessa 1.2 kuvatuista tekijöistä johtuen. Tässä työssä kuitenkin korostui haastateltavan henkilön valtakunnallisesti tunnustettu asiantuntijuus, myös tutkimustyössä käytettyjen lähteiden valikoitumisen suhteen. Tutkimustyössä on kiinnitetty erityistä huomiota lähteiden korkealuokkaisuuteen, sekä toissijaisesti lähteiden kattavuuteen. Suuri osa käytetyimmistä lähteistä ovat viranomaisohjeita, määräyksiä.

13 Kehitysehdotuksia:

TEMPEST-työpisteen pöytään kiinnitetään muovitaskuun paperi mikä on kaikkien nähtävillä. Ko. paperiin vaaditaan kulloinkin työpisteellä työskentelevän henkilön allekirjoitus, jolla hän vahvistaa paperin ohjeet esim. ettei työpisteen koneeseen saa kiinnittää, asentaa mitään lisälaitteita, eikä tehdä mitään muutoksia. Samoin ennen TEMPEST-tilaan menoa tulee näkyville asettaa selvät merkinnät, että tilaan ei saa edes viedä matkapuhelinta, usb muistitikkua tms. mitään tallennusvälinettä jne. Kaikkien tilassa työskentelevien tulee käydä perehdytys läpi ja allekirjoittaa se. Tilassa käytettävä tietokone voidaan lisäksi koteloida siten, että siihen ei ole mahdollista asentaa muistitikkuja tjms.

Lisäksi henkilökunnalle tulee antaa koulutusta TEMPEST-uhista ja siihen liittyvistä muista tiedustelu-uhista (hyökkääjän näkökulma), jotta henkilökunta osaa tunnistaa mikäli oma organisaatio joutuu tiedustelun kohteeksi, sekä luoda toimintamallit mikäli tälläista toimintaa havaitaan. Toimintamallien tulee sisältää ainakin seuraavia asioita: turvallisuuspoikkeamaraportointi, ilmoitusvelvollisuudet, vastuuhenkilöt, sekä välittömät toimenpiteet. TEMPEST-suojauksen tarpeen tulee perustua riskiarvioon.

Lähtökohtana voidaan todeta, että organisaation tulee matalalla kynnyksellä ottaa yhteys oman organisaation turvallisuusorganisaatioon joka voi puolestaan konsultoida viestintäviraston ammattilaisia, sekä muita turvallisuusviranomaisia (SUPO, Puolustusvoimat). Kansallinen ohjeistus on olemassa, ohjeistus määrittelee mm. TEMPEST-suojaukseen liittyvät vähimmäisvaatimukset. Jonkun verran jää kuitenkin organisaation harkinnan varaan, harkinnan tulisi aina perustua systemaattiseen riskiarvioon. Huomioitavia seikkoja ovat: yksityiskohtainen toimitila- ja tarvesuunnittelu, vaimennus - ja vyöhykemittaukset, tehtyjen toimepiteiden dokumentointi, poikkeamaraportointi, TEMPEST-laitteiden hankintakanavat, henkilöstön perehdytys ja koulutus, sekä näiden seuranta, rakenteellinen tilan jakaminen vyöhykkeisiin, rakennusten pohjapiirustukset (sekä näiden suojaaminen), laitteiden elinkaari hankintahetkestä, käyttöön ja huoltotilanteisiin ja lopulta laitteen poistoon tulee olla suunniteltu ja hallittu.

Lähteet

Dorothy E. Denning, ISBN 0-201-43303-6, 1999 ACM Press, New York, Information warfare and security

Kaj Granlund, Langaton tiedonsiirto, 1. Painos elokuu 2001, Docendo Finland Oy, WS Bookwell Porvoo 2001

Lehto Arto, Radioaaltojen maailma, Tammer-Paino, Tampere 2006, Otatieto, Oy yliopistokustannus University Press Finland Ltd.

Lindell Ismo, Radioaaltojen eteneminen, 4. tarkastettu painos, Otatieto Oy, Hakapaino Oy, Helsinki 1996

Puolustusministeriö, ISBN: 978-951-25-2011-0, 2009, Kansallinen turvallisuusauditointikriteeristö

Räisänen, Lehto, Radiotekniikan perusteet, ISBN 951-672-309-8, 2001, Yliopistokustannus/Otatieto

Valtiovarainministeriö, Juvenes Print- Suomen Yliopistopaino Oy, 2013. Toimitilojen tietoturvaohje

Viestintäviraston sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien aiheuttamien tietoturvariskien ehkäisyn periaatteet 15.11.2013 Dnro: 1305/653/2013

Valtanen Esko, fysiikan taulukkokirja, ISBN 978-952-9867-30-1, Genesis- Kirjat Oy, Gummerus Kirjapaino Oy, Jyväskylä

Air Force Manual 33- 214, Volume 2, 2001, Communications and Information, Emission security countermeasures reviews, US Airforce
http://www.dtic.mil/dtic/tr/fulltext/u2/a403686.pdf

www.consilium.europa.eu/figeneral-secretariat/corporate-policies/classified-2013/488/EU

www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/tempest/

Heinrich Herz biography, 2018, Encyclopaedya Britannica
https://www.britannica.com/biography/Heinrich-Hertz

Hertz
https://en.wikipedia.org/wiki/Hertz

Information Assurance Security Guidelines on Accrediation of EU Tempes Companies
http://data.consilium.europa.eu/doc/document/ST-16267-2012-INIT-en/pdf
corporate policies information assurance tempest

Kansallinen turvallisuusauditointikriteeristö (2015)

http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) rakenteellinen turvallisuus, osa-alue F200

http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) tietoliikenneturvallisuus, osa-alue I300. http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Maxwellin yhtälöt
https://fi.wikipedia.org/wiki/Maxwellin_yhtälöt

https://motherboard.vice.com/en_us/article/xygdwq/how-white-hat-hackers-stole-crypto-keys-from-an-offline-laptop-in-another-room

https://www.senaatti.fi/tietoa-senaatista/palvelumme/toimitilapalvelut/

Sähkömagneettinen spektri, Korpela Jukka 2002, http://jkorpela.fi/smag.html

Teknisen tietoturvallisuuden ohjeisto EU:n TEMPEST – yritysten hyväksymisestä (IASG 07-04) / EU LIMITE

Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010)
https://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Viestintävirasto, Dnro: 1305/653/2013, Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet
https://www.viestintavirasto.fi/attachments/Kansallinen_TEMPEST-ohje.pdf

https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/strategia/luottamustalisaamassa.html

https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat.html

William E. Cobb, Major, USAF, United States Air Force air university, air force institute of technology institute, Exploitation of unintentional information leakage from integrated circuits, US 2011
http://citeseerx.ist.psu.edu./viewdoc/download?doi=10.1.1.467.5808&rep=rep1&type=pdf

Julkaisemattomat lähteet

Tauriainen, A. 2017, Johtavan tarkastajan haastatteluja. Viestintäviraston tiloissa. Helsinki.

Salmi, J. 2018, vastaus sähköpostitiedusteluun, S-posti jouni.salmi@rohde-schwarz.com
7.3.2018

Kuviot

Taulukot

Liite 1:

Alla on lista EU:n hyväksymistä yrityksistä:

Siltec Sp z o.

Country: Poland
Osoite: E. Orzeszkowej 5 str. 02-374 Warsaw
Website: www.siltec.com.pl
Contact: info@sitec.pl
NTA contact: tomasz.przada.dbti@abw.gov.pl

SST

Country: UK
Address: Brunel Court, Waterwells GL2 2AL Gloucester, Gloucesterhire
Website: www.sst.ws
Contact: richard.mundy@sst.ws
NTA contact: tempest@cesg.gsi.gov.uk

Eurotempest Nederland BV

Country: Netherlands
Address: Zandstraat 20 5683PL Best
Website: www.ospl.nl
Contact: info@ospl.nl
NTA contact: tempest@nlncsa.nl

Intracom Defence Electronics
Country: Greece
Address: 21 km Markopoulou Ave/19400 Koropi
Website: www.intracomdefence.com
Contact: kmel@intracomdefence.com
NTA contact: edep10@nis.gr
• Degree of self certification: The authority of self-certification of a prototype of an IASG 7-03 level A equipment

TEMPEST-suojautumiseen liittyvät kansainväliset ja kansalliset velvoitteet

TEMPEST- suojautumiseen liittyvä viitekehys koostuu kansallisista ja kansainvälisistä velvoitteista. Euroopan Unionin päätös 2013/488/EU. Euroopan Unionin neuvoston liite 4, infomation assurance. CAA salaustuotehyväksynnät (tuotteet oltava TEMPEST-suojattuja) Euroopan Unionin hyväksymä lista (EU secret). NTA National Tempest Authority (kansallinen nimetty vastuuhenkilö) Viestintävirasto, NSA National Security Auhtority Ulkoministeriö, IASG Security guidelines list of accredited tempest companies (EU), Natolla on oma vastaava listansa hyväksytyistä yrityksistä (Nato secret), Tietoturvasopimus NATO:n ja Suomen välillä 8/2013. AC

2013/488/EU
EU:n neuvoston annex 4. information assurance
CAA salaustuotehyväksynnät(tuotteet TEMPEST suojattuja) EU lista EU secret
NTA National TEMPEST authority (nimetty henkilö), Viestintävirasto
NSA National security authority, ulkoministeriö
IASG security guidelines list of accredited TEMPEST companies (EU)
Natolla oma lista (nato secret)
Tietoturvasopimus NATO:n ja Suomen välillä 8/2013
AC-35-D/1038
Kansallinen viitekehys valtioneuvoston asetus tietoturvasta
VAHTI 2/2013