Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Ville Paasio

Kiinteistön fyysisen tietoturvallisuuden auditointi

Metropolia Ammattikorkeakoulu
Insinööri (AMK)
Talotekniikka
Insinöörityö
19.3.2021

Tekijä Otsikko Sivumäärä Aika	Ville Paasio Kiinteistön fyysisen tietoturvallisuuden auditointi 25 sivua 3.3.2021
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	talotekniikka
Ammatillinen pääaine	kiinteistöjohtaminen
Ohjaajat	yliopettaja Aune Rummukainen turvallisuusjohtaja Antti Kutila

Tässä opinnäytetyössä käytiin läpi valtionhallinnon vaatimukset koskien kiinteistön fyysistä tietoturvallisuutta hyödyntäen KATAKRI 2015 -auditointityökalua. Kappaleessa kaksi käytiin läpi vaatimukset ja niitä ohjaavat määräykset. Opinnäytetyön tavoitteena oli toteuttaa julkisien asiakirjojen pohjalta edellä mainittu auditointi ja samalla selkeyttää kiinteistöön liittyville osapuolille nykyinen taso rakenteellisen tietoturvallisuuden osalta.

Opinnäytetyössä keskityttiin rakennusteknisiin ratkaisuihin, joilla estetään tiloihin tunkeutuminen, jolloin vältytään tilanteelta, jossa turvallisuuskriittistä aineistoa joutuu asiattomien haltuun. Tilojen osalta käytettiin tilatunnuksia ja opinnäytetyössä ei esitetty kiinteistöön liittyviä tunnistetietoja, jotta kohdetta ei voida yksilöitä viranomaisen toiminnan turvaamiseksi

Osana opinnäytetyötä suoritettiin olemassa olevan viranomaiskohteen osalta auditointi, jossa selvitettiin vaatimusten täyttyminen kohteessa. Tuotiin esiin havainnot tarkasteltavan kohteen osalta. Havaituille puutteille haettiin korjausehdotukset, jotta opinnäytetyötä voidaan hyödyntää rakennusta koskevien korjaustöiden suunnittelussa tulevina vuosina.

Opinnäytetyössä ei selvitetty lukitus-, hälytys-, kulunvalvonta- tai kameravalvontajärjestelmien nykytilaa vaan niitä käsitellään ainoastaan vaatimusten osalta, joita järjestelmille asetetaan. Edellä mainitut järjestelmät on rajattu tarkastelun ulkopuolelle viranomaistoiminnan tietoturvallisuuden takaamiseksi.

Auditoinnin perusteella voitiin todeta, että tarkasteltavan kiinteistön osalta tulee suorittaa korjaavia toimenpiteitä, koskien kaikkia rakenneosia rakennuksessa. Lisäksi kohteen osalta tulee suorittaa lisäselvityksiä ja kohteen tilat tulee järjestää uudelleen vastaamaan vaatimuksia, jotka asetetaan tietoturvallisuudelle.

Avainsanat	tietoturvallisuus, valtionhallinto, tilaturvallisuus

Author	Ville Paasio
Title	Structural audit of facility to estimate risks for information security
Number of Pages	25 pages
Date	3 March 2021
Degree	Bachelor of Engineering
Degree Programme	Building Services Engineering
Professional Major	Facility Management
Instructors	Aune Rummukainen, Principal Lecturer Antti Kutila, Director

The goal of this thesis was to use public documentation on the audition of the physical security of a government building and to illustrate the state of structural security, to all parties to the facility. In order to do this, the physical security requirements set for government buildings were studied with the KATAKRI 2015 auditioning tool. The thesis focused on structural solutions preventing break-ins to the premises and protecting sensitive documents . The building cannot be identified with the information in the thesis.

The final year project included a security audition of the building in order to determine its security demands. Remedies were suggested for all defects so this thesis can be utilized when planning renovationsin future years.

The thesis established that the facility is in a need of several corrective actions to all structural components. Furthermore, the facility needs to be examined more thoroughly, and it must be reorganized to fulfil the requirements of information security.

Keywords	information security, spatial security, government administration

Sisällys

1 Johdanto

Tämän insinöörityön keskiössä on viranomaiskäytössä olevassa kohteessa käsiteltävän tietoturvaluokitellun tiedon koskemattomuuden turvaaminen rakennusteknisin ratkaisuin. Viranomaisten toimintaa ohjataan asetuksin, määräyksin ja lainsäädännöllisin keinoin. Edellä mainitut dokumentit ohjaavat lukijan aina seuraavaan dokumenttiin, ja selkeiden ratkaisuiden hakeminen ei aina ole yksiselitteistä. Insinöörityössä on käyty läpi keskeiset ohjaavat ja velvoittavat määräykset sekä niiden pohjalta laadittu muutosta vaativien kohtien korjausehdotukset.

Insinöörityön idea on lähtenyt allekirjoittaneen henkilökohtaisesta tarpeesta syventää tietämystä viranomaiskohteissa vaadituista rakennusteknisistä suojautumisratkaisuista, samalla saadaan tuotettua aineisto niistä kohdista, jotka edellyttävät toimenpiteitä, jotta tilaturvallisuuden vaatimukset saadaan täytettyä. Työssäni kohtaan päivittäin tilanteita, joissa kaikki osapuolet eivät ole tietoisia voimassa olevista määräyksistä ja vaatimuksista, kiinteistön ylläpidon edustajana ja korjaustöiden tilaajana minulla tulee olla selkeä kuva siitä, miten muutokset ja korjaukset tulee toteuttaa jotta, vaadittu suojaustaso saavutetaan rakenteiden osalta muutosten jälkeenkin.

Insinöörityön suorittamiselle on haettu hyväksyntä rakennuksen omistajalta Senaatti-kiinteistöt oy:ltä ja kiinteistössä toimivalta viranomaistaholta. Kumpikin osapuolista näki tämä insinöörityön tuottavan lisäarvoa, ja insinöörityötä voidaan hyödyntää PTS-suunnittelussa sekä tulevien muutosten suunnittelutehtävissä.

Senaatti-kiinteistöt on valtiovarainministeriön alainen liikelaitos, joka tuottaa tilapalveluita ensisijaisesti valtionhallinnon eri yksiköille. Senaatti-kiinteistöt on perustettu vuonna 1995, vuonna 1999 se muutettiin liikelaitokseksi, nykyisen nimensä liikelaitos sai vuonna 2001. Senaatti-kiinteistöillä on n. 8 900 kiinteistöä ja työntekijöitä n. 400. (6)

2 Tietoturvallisuus

2.1 Keskeiset käsitteet

Tämän insinöörityön keskeisimpiä käsitteitä on esitetty ja selitetty seuraavassa luetelmassa:

VAHTI	Valtiovarainministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä, vuoden 2020 alusta toimii digi- ja väestötietoviraston alaisuudessa (DVV)
VAHTI-Ohjeisto	Valtionhallinnon tietoturvallisuuden johtoryhmän laatima kirjallinen ohjeisto tietoturvallisuudesta
TEMPEST	Lyhenne käsitteestä Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. Hajasäteilyltä suojautumiseen liittyvä toiminta
Säilytysyksikkö	Lukittu paloturvakaappi, laatikosto, kassakaappi tai muu vastaava tietoaineiston säilytystila.
KATAKRI	Viranomaiskäyttöön tarkoitettu tietoturvallisuuden auditointityökalu

2.2 Ohjaavat määräykset ja lainsäädäntö

Jotta tietoturvallisuuden auditointi voidaan suorittaa, tulee ymmärtää tietoturvallisen ympäristön luonne sekä sitä määräävien lakien ja säädöksien yhteys toisiinsa.

Viranomaisten toiminnan ja tilojen suunnittelua ohjaa usea eri asetus, osa turvallisuuden vaatimuksista tulee valtionrajojen ulkopuolelta kuten Euroopan unionin neuvostolta. Euroopan unionin neuvoston päätös 2013/488/EU velvoittaa Suomen viranomaisia toiminnoissaan suojaamaan EU:n toiminnan kannalta sensitiivistä tietoa. (10, s. 2.) Euroopan unionin neuvoston päätös 2013/488/EU on ohjannut toimintaa, jonka pohjalta on laadittu VAHTI-ohjeistus ja KATAKRI- tietoturvallisuuden auditointityökalu viranomaisille. VAHTI-ohjeistossa avataan tarkemmin konkreettisia toimintatapoja ja toteutustapoja joilla saavutetaan haluttu lopputulos.

2.2.1 EU:n neuvoston päätös 488/2013

Euroopan unionin neuvoston päätös 488/2013 EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä on astunut voimaan 23.9.2013.

Tämä päätös asettaa vaatimukset tietoturvakriittiseksi luokitellun aineiston säilytystä ja käsittelyä koskien. Tilojen fyysinen turvallisuus on yksi keino, jolla pyritään estämään suojattavan tiedon joutumista vääriin käsiin. (10, s. 3.)

2.2.2 KATAKRI

EU-neuvoston päätöksen 488/2013 pohjalta on luotu KATAKRI-auditointityökalu, jonka avulla voidaan arvioida vaatimusten mukaisuuden täyttymistä. KATAKRI-auditointityökalusta on aikaisempiakin versioita, mutta tässä opinnäytetyössä käytetään KATAKRI 2015 -auditointityökalua . Uusin versio KATAKRIsta on julkaistu joulukuussa 2020.

KATAKRI on viranomaisille tarkoitettu auditointityökalu, jota käytetään arvioimaan organisaation kykyä suojata salassa pidettävää tietoa. KATAKRI koostuu kansallisien säädöksien ja asetusten minimivaatimuksista. KATAKRIssa ei esitetä tietoturvallisuudelle selkeitä vaatimuksia, siihen kootut vaatimukset juontuvat voimassa olevaan lainsäädäntöön ja kansainvälisiin velvoitteisiin. Keskeiset kansainväliset vaatimukset tulevat EU:n neuvoston turvallisuussäännöistä (2013/488/EU) ja lainsäädäntö perustuu valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010). KATAKRIssa esitettyjen vaatimusten yhteydessä on lähdeviittaus jonka pohjalta saa selvitettyä tarkentavia ohjeita eri kohtiin liittyen.

KATAKRI on vaatimusten osalta jaettu kolmeen osaan. Tietoturvallisuusjohtaminen (T), Fyysinen tietoturvallisuus (F) ja Tekninen tietoturvallisuus (I). Osan (T) tavoitteena on varmistaa organisaation turvallisuusjohtamisen osaaminen, osa-alueessa on kuvattu perustaso, joka tulee saavuttaa. Osassa (F) kuvataan tietojen käsittely-ympäristöä koskevat turvallisuusvaatimukset. Tilat voidaan jakaa kolmeen alueeseen: hallinnollinen alue, turva-alue ja tekninen turva-alue. Osassa (I) käydään läpi tekniselle tietojen käsittelylle asetetut vaatimukset, osa (I) jakautuu kolmeen käsiteltävän tiedon mukaiseen suojaustasoon (STIV, STIII; ja STII), Vaatimusten kuvaukset on kirjattu niin, että ne mahdollistavat erilaisia toimintatapoja. Vaatimusten osalta on myös toteutusesimerkkejä, suosituksia ja hyviä käytäntöjä, joita on myös VAHTI-ohjeissa ja EU:n turvallisuussäännöissä.

> KATAKRI:a voidaan käyttää auditointityökaluna arvioitaessa yrityksen turvallisuusjärjestelyjen toteutumista yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. KATAKRI:a voidaan hyödyntää myös apuna yrityksien sekä viranomaisten muussa turvallisuustyössä ja sen kehittämisessä. (2, s. 3.)

> KATAKRI:a käyttämällä pyritään varmistumaan, että kohdeorganisaatiolla on riittävät turvallisuusjärjestelyt viranomaisen salassa pidettävien tietojen oikeudettoman paljastumisen ehkäisemiseksi kaikissa niissä ympäristöissä, joissa tietoja käsitellään.Tavoitteena on lisäksi varmistaa turvallisuusvaatimusten huomioon ottaminen turvallisuuden hallinnassa. (2, s. 3.)

> Turvallisuusjärjestelyjen suunnittelun ja toteutuksen avulla pyritään varmistamaan uhkiin nähden hyväksyttävä turvallisuustaso. Kohdeorganisaation tulee pystyä osoittamaan turvallisuusjärjestelyjen riittävyys luotettavasti. Turvallisuusjärjestelyjen riittävyyden arvioinnin tulee pohjautua järjestelmälliseen riskienarviointiin. (2, s. 3.)

Turvallisuusriskien hallinnalla on pyrittävä toteuttamaan turvatoimien yhdistelmä, jolla saadaan aikaan tyydyttävä tasapaino käyttäjien vaatimusten, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. KATAKRI:n avulla arvioidaan kohdeorganisaation yleistä kykyä suojata viranomainen salassa pidettävää tietoa. Näin ollen KATAKRI:n avulla tehtyä yritysturvallisuusselvitystä voidaan käyttää niin kotimaisissa kuin kansainvälisissäkin hankkeissa. (2, s. 3.)

Vaikka KATAKRI:ssa kuvatut EU:n neuvoston turvallisuussääntöjen vaatimukset koskevat vain EU:n turvallisuusluokiteltujen tietojen suojaamista, ne edustavat EU:n jäsenvaltioiden yhteisesti hyväksymiä ja käyttämiä salassa pidettävän tiedon suojaamista koskevia perusperiaatteita ja vähimmäisvaatimuksia Euroopassa ja luovat sen vuoksi hyvän perustan salassa pidettävien tietojen suojaamiseksi myös Suomessa. Jäsenvaltiot noudattavat EU:n turvallisuussääntöjä kansallisen lainsäädäntönsä mukaisesti, joten Suomessa EU:n salassa pidettävien tietojen suojaamisessa noudatetaan EU:n vaatimusten lisäksi tietoturvallisuusasetusta. Tietoturvallisuusasetuksen ja EU:n neuvoston turvallisuussääntöjen vaatimukset eivät merkittäviltä osin poikkea toisistaan. Mikäli KATAKRI:iin kirjattu vaatimus koskee pelkästään EU:n salassa pidettävää tietoa, se ilmenee lähdeviitteistä. (2, s. 4.)

KATAKRI:n osa-alueet on laadittu itsenäisiksi kokonaisuuksiksi jotta niitä voidaan hyödyntää myös erikseen. Esimerkiksi osittainen yritysturvallisuusselvitys, joka voidaan tehdä yrityksen toiminnan muuttuessa tai silloin kun auditointi kohdistuu rajattuun osa-alueeseen. Organisaation tulee kuitenkin täyttää T-osion vaatimukset osittaisenkin yritysturvallisuusselvityksen yhteydessä. (2, s. 4.)

KATAKRI:a ei ole tarkoitettu käytettäväksi sellaisenaan julkisen hankinnan turvallisuusvaatimuksena. Julkisessa hankinnassa tarkat turvallisuusvaatimukset tulisi määrittää erikseen ottaen huomioon hankintaa koskevat riskit ja erityistarpeet. (2, s. 4.)

2.2.3 VAHTI-ohje

EU:n turvallisuusluokiteltujen tietojen suojaamista koskevien turvallisuussääntöjen pohjalta on luotu VAHTI-ohjeistus, johon on viranomaiskohtaisia tarkennuksia ja toimintaohjeita. Kohteen viranomaisten tarkennuksia ja toimintaohjeita ei tässä käsitellä, koska niiden tietojen käsittely julkisessa aineistossa vaarantaisi viranomaisen toimintaa. Selvitykset tehdään siis yleisesti tiedossa olevin menetelmin ja haastatteluilla varmistetaan nimenomaisen kohteen osalta suojauksien riittävyys.

VAHTI-ohjeisto on julkisen hallinnon digitaalisen turvallisuuden johtoryhmän luoma kokoelma ohjeita, jotka liittyvät digitaalisen turvallisuuden varmistamiseen ja kehittämiseen julkishallinnossa. Johtoryhmä toimii vastaavien organisaatioiden yhteistyö-, valmistelu-

ja koordinaatioyksikkönä. Voimassa olevia VAHTI-ohjeita on tällä hetkellä 46, ja niiden julkaisuvuodet sijoittuvat välille 2001–2017.

Digitaalinen turvallisuus käsittää tässä yhteydessä digitaalisen aineiston, aineiston säilytyksen, tilat joissa aineistoa käsitellään, laitekannan joilla aineistoa käsitellään, aineistoa käsittelevän henkilökunnan ja henkilöitä, jotka pääsevät edellä mainittujen aineistojen ja tilojen luokse.

VAHTI-ohjeilla ja KATAKRIlla on tiivis vuorovaikutussuhde, tämä nousee esiin välittömästi, KATAKRIn ensimmäisessä hallinnollisen tietoturvallisuuden vaatimuskohdassa viitataan VAHTI 2/2010 -ohjeeseen ”muuna lisätietolähteenä”. KATAKRIssa on avattu VAHTI-ohjeistoa konkreettisin esimerkein, KATAKRIssa on viittaukset ohjaaviin määräyksiin ja ohjeistuksiin, jotta työkalun käytettävyys olisi yksinkertaisempaa erilaisissa kohteissa.

KATAKRIssa mainitaan seuraavat vaatimukset kohdassa T01 Turvallisuusjohtaminen.
1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan.
2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset.
3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan ja niiden toteutumista seurataan säännöllisesti.

VAHTI-ohje 2/2010 tarkentaa liitteen 5 kohdassa 1.1 johtajuudelle asetettavista vaatimuksista seuraavasti:

Perustason vaatimukset
1. Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.
2. Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.
3. Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.

Korotetun tason lisävaatimukset
4. Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.

Korkean tason lisävaatimukset
5. Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma.
6. Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia. (7, s. 10.)

VAHTI-ohjeet on jaettu kahdeksaan luokkaan, joissa käsitellään digitaalisen turvallisuuden osa-alueita.

VAHTI-ryhmittely
- Fyysinen turvallisuus
- Hallinnollinen tietoturvallisuus
- Henkilöstöturvallisuus
- Käyttöturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Tietoliikenneturvallisuus

Julkishallinnossa on noudatettava VAHTI-ohjeita, minkä lisäksi julkishallinnon tietoja käsittelevät yksityiset yritykset on sopimuksella velvoitettu noudattamaan niitä.

Alin viranomaisen tietojenkäsittely-ympäristöille sallittu taso on tietoturvallisuuden perustaso. Tässä ympäristössä voidaan tietosisällön toimivaltaa käyttävän viranomaisen päätöksellä käsitellä selväkielisessä muodossa suojaustason IV edellyttävää tietoa. Korotetun tietoturvallisuustason ympäristössä voidaan vastaavilla valtuuksilla käsitellä tietoa selväkielisessä muodossa aina suojaustasoon III asti. Vastaavasti korkean tietoturvallisuustason täyttävissä ympäristöissä voidaan käsitellä tietoa selväkielisessä muodossa suojaustasoon II asti.

Tällä hetkellä voimassaolevaa toimitilojen tietoturvaohje on VAHTI 2/2013, tätä edeltävä versio oli tietoteknisten laitetilojen turvallisuussuositus VAHTI 1/2002.

2.2.4 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnosta 681/2010 on astunut voimaan 01.10.2010. Asetus on annettu säädöksen laki viranomaisen toiminnan julkisuudesta 621/1999 nojalla. Asetus määrää viranomaisten omassa toiminnassa huomioimaan käsiteltävien aineistojen arkaluonteisuutta ja asettaa vaatimukset aineistojen turvallisuusluokitteluun. Voimassa oleva säädös turvaluokituksesta on valtioneuvoston asetus asiakirjojen turvaluokittelusta valtionhallinnossa 1101/2019. Säädöksellä määrätään eri turvallisuustasojen merkinnät ja niiden vaatimukset.

Säädöksessä 681/2010 määrätään pykälässä 23 siirtymäsäännöksiksi, että valtionhallinnon viranomaisen asetuksen voimaan tullessa käytössä olevien toimitilojen on täytettävä asetuksessa säädetyt vaatimukset tilojen turvallisuudelle viiden vuoden kuluessa asetuksen voimaantulosta (8, 23§).

2.3 Salassa pidettävät tiedot

Laki viranomaisten toiminnan julkisuudesta 621/1999 määrittää selkeästi, mikä tieto on julkista ja mikä voidaan merkitä tietoturvaluokitelluksi aineistoksi (11, 24§). Mikään tieto ei ole automaattisesti salassa pidettävää, tiedot luokitellaan salassa pidettäväksi kulloinkin tapauskohtaisesti viranomaisen toimesta, palveluntuottaja tai elinkeinonharjoittaja ei voi tästä asiasta päättää.

Viranomainen tekee VAHTI-ohjeiden perusteella päätöksen tiedon suojaustasosta ja merkitsee sen ohjeistuksen mukaisesti dokumentteihin. Määräävänä tekijänä tietojen

luokittelussa toimii valtioneuvoston asetus asiakirjojen tietoturvallisuudesta, jonka perusteella tietojen luokittelu tapahtuu. Kun aineiston suojaustaso on päätetty ja tiedossa, tulee sitä käsitellä kyseisen suojaustason edellyttämällä tavalla.

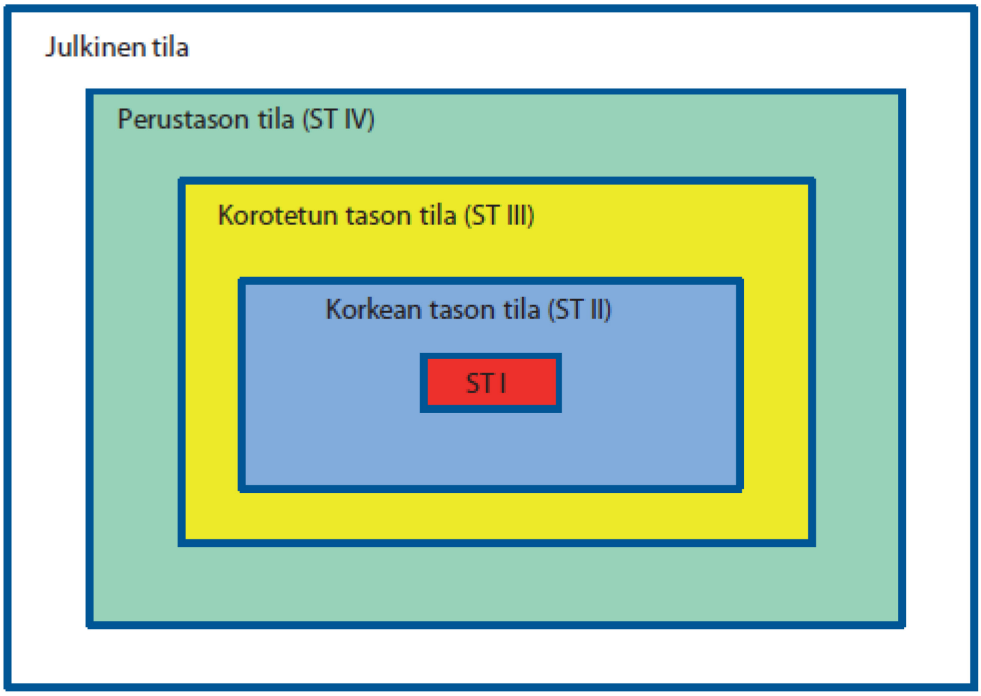
Suojaustasojen IV–II tietoja voidaan käsitellä turva-alueella. Suojaustasojen IV–II tietoja voidaan käsitellä myös hallinnollisella alueella, jos sivullisten pääsy tietoihin on estetty. Suojaustason IV tietoja voidaan säilyttää hallinnollisella alueella. Suojaustasojen III–II tietoja tulee säilyttää turva-alueella. (2, s. 20.)

Hallinnollisen alueen raja:

Aluetta rajaavan aidan tai kuoren seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteilta ei vaadita erityisiä ominaisuuksia.

Hallinnollisen alueen raja ja salassa pidettävän tiedon käsittely- sekä säilytysyksikön rajaava tila tulisi olla lukittavissa lukolla, jonka avainten kopiointi on estetty patenttisuojalla. (2, s. 21.)

VAHTI-ohje 2/2003 jaottelee turvallisuusvyöhykkeet värien mukaan niiden tunnistamisen helpottamiseksi. Kuvassa 1 on vyöhykkeiden tunnusvärit ja lyhenteet.



Kuva 1. Turvallisuusvyöhykkeiden väritunnukset. (1, s. 22.)

2.3.1 Perustason tila ST IV (vihreä alue)

Suojaustason IV, KÄYTTÖ RAJOITETTU (RAJ (R)) mukainen asiakirja sisältää salassa pidettävää tietoa. Tämän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksissä tarkoitetuille yleiselle tai yksityiselle edulle. Asiattomilta pääsy tilaan tulee estää ja henkilöt tulee tunnistaa.

2.3.2 Korotetun tason tila ST III (keltainen alue)

Suojaustason III, LUOTTAMUKSELLINEN (LUOT (L)) asiakirjassa olevan salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksissä tarkoitetuille yleiselle tai yksityiselle edulle

Mikäli suojattavaa tietoa säilytetään tilassa ilman hyväksyttyä säilytysyksikköä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden olla kyseisen suojaustason tiedon säilyttämiseen hyväksyttyä säilytysyksikköä vastaavia. Tällainen säilytysyksikkö on SFS-EN-14450:n luokan S2 turvakaappi tai vastaava. (14 s. 6.) Tällaiseksi suojaksi voidaan katsoa myös esimerkiksi SFS-EN-1627:n luokkaa 4 vastaava rakenteellinen suoja. (2 s. 21.)

Suojaustason III tilaan ei tule päästä ilman myönnettyä lupaa ja sähköistä kulunvalvontaa. Henkilöstön liikkumista tiloissa seurataan lokikirjauksilla. Ulkoiset toimijat saavat työskennellä tilassa viranomaisen valvonnan alaisena tai tapauskohtaisesti viranomaisen päätöksellä itsenäisesti annettujen ohjeistusten mukaisesti.

2.3.3 Korkean tason tila ST II (sininen alue)

Suojaustaso II, SALAINEN (SAL (S)) asiakirjan sisältämän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksissä tarkoitetulle yleiselle edulle

Mikäli suojattavaa tietoa säilytetään tilassa hyväksytyssä säilytysyksikössä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden antaa sellainen rakenteellinen suoja, että niiden kautta alueelle tunkeutuminen on erittäin hidasta ja vaikeaa.

Mikäli suojattavaa tietoa säilytetään tilassa ilman hyväksyttyä säilytysyksikköä, tulee aluetta rajaavien seinä-, katto-, lattia-, ikkuna-, ovi- ja talotekniikan aukkojen rakenteiden olla kyseisen suojaustason tiedon säilyttämiseen hyväksyttyä säilytysyksikköä vastaava. Tällainen säilytysyksikkö on SFS-EN-1143-1:n luokan EII kassakaappi tai vastaava. (15 s. 12.)Tällaiseksi suojaksi voidaan katsoa myös esimerkiksi SFS-EN-1627:n luokkaa 5 vastaava rakenteellinen suoja. (16 s. 24.) Vastaava rakenteellinen suoja voidaan toteuttaa myös siten, että turva-aluetta rajaavat rakenteet muodostavat SFS-EN-1627:n luokkaa 3 vastaavan suojan ja sen lisäksi säilytysyksikköä rajaavan

tilan rakenteet muodostettavat SFS-EN-1627:n luokkaa 4 vastaavan suojan. (2 s. 21 ;16 s. 24.)

Suojaustason II tilojen avaimia tai kulkutunnisteita ei luovuteta vierailijoille tai palveluntuottajan henkilöstölle.

2.3.4 ST I (punainen alue)

Suojaustason I, ERITTÄIN SALAINEN (ERSAL (E)) mukaisen asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle.

2.4 Tilojen käyttäjät

Tilojen käyttäjien toiminta on tietoturvallisuuden toiminnan kannalta tärkein osa-alue, kohteen henkilöstön turvallisuuskoulutus ja perehdytys tulee olla suoritettu riittävällä tasolla. Tilojen käyttäjänä tässä yhteydessä tarkoitetaan kaikkia kohteessa toimivia henkilöitä, kiinteistössä työskentelee jatkuvasti muidenkin organisaatioiden työntekijöitä kuin viranomaisia.

Ensiarvoisen tärkeää on eri organisaatioiden edustajien perehdyttäminen ja saumaton yhteistyö, jotta haluttu turvallisuuskulttuuri ja kaikkien henkilöiden osalta tietoisuus oikeista toimintatavoista on jalkautettua läpi koko organisaatioiden.

2.5 Tunkeutuminen tiloihin

Fyysisen turvallisuuden tarkoituksena on estää salaa tai voimakeinoin tunkeutuminen tiloihin, joissa säilytetään tietoturvallisuuden kannalta kriittistä aineistoa.

Yleisimpiä tunkeutumisväyliä rakennukseen ovat sen rakenteiden heikoimmat osa-alueet, ikkunat, ovet, valmiit aukot rakenteissa ja kevyemmistä rakenneratkaisuista koostuvat kohdat. Edellä mainitut kohdat tulee tarkastaa erityisen huolellisesti ja noudattaa äärimmäistä kriittisyyttä tarkastelussa. Tunkeutuminen pyritään estämään lukituksella, valvonnalla, aitaamalla ja muilla hidastavilla tekijöillä.

Eri rakenneosien kestävyyttä tunkeutumistilanteessa arvioidaan tunkeutumisajalla, joka kestää mahdollisesta tunkeutujalta päästä rakenneosan läpi arkaluonteiseen aineistoon käsiksi. Viranomainen määrittelee tilakohtaisen tunkeutumisajan, joka rakenteiden tulee kestää, jotta vastatoimet ehditään toteuttaa, ennen kuin kriittinen materiaali on tunkeutujan hallussa. Tässä insinöörityössä ei oteta kantaa yksittäisen viranomaisen määrittelemään tunkeutumisaikaan vaan kiinteistöä auditoidaan julkisen aineiston pohjalta, tiedettyjen turvallisuustasojen mukaisesti.

On muistettava, että mikään rakenneratkaisu ei ole täysin tunkeutumisen kestävä, vaan sen tarkoitus on ainoastaan hidastaa tunkeutumista. Elektroninen valvonta ja fyysinen este täydentävät toisiaan, jolloin saadaan enemmin aikaa tunkeutumisen keskeyttämiseksi.

2.6 TEMPEST

Hajasäteily on elektronisten laitteiden lähettämää säteilyä, joka voidaan kaapata, ja siitä voidaan selvittää turvaluokiteltua tietoa. Hajasäteilyltä suojautuminen voidaan toteuttaa oikeilla laitevalinnoilla tai rakenteellisilla ratkaisuilla. Tehokkainta suojautuminen on silloin, kun hyödynnetään kumpaakin vaihtoehtoa.

Suojaustason IV aineiston osalta ei ole erityisiä vaatimuksia hajasäteilyltä suojautumiseen, mutta mikäli tilassa käsitellään suojaustasojen III–II aineistoa, tulee tarvittavat suojaustoimenpiteet ottaa huomioon.

Tilat, joissa käsitellään tietoturvakriittistä aineistoa, tulee suunnitella tilaratkaisuin tukemaan riittävän suojaustason omaavaa laitteistoa. Tilat, joissa käsitellään tietoturvakriittistä aineistoa, tulee sijoittaa rakennuksen sisempiin osiin tai mahdollisuuksien mukaan maanpinnan alapuolelle.

Insinöörityössä käsiteltävän kiinteistön osalta tulee suorittaa hajasäteilyn vyöhykemittaus, jonka pohjalta voidaan suunnitella tarkemmin mahdolliset tarvittavat muutokset. Rakennuksen ympärille suunnitellun aitarakenteen etäisyys korkeamman suojaustason tiloista on n. 40 metriä, jolloin välimatka julkiseen alueeseen tulee huomioida TEMPEST-suunnittelussa.

Hajasäteilyltä suojautumista viranomaiskohteissa ohjaa viestintäviraston laatima ohjeistus vuodelta 2013 sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet.

Suojaustason III tilojen hajasäteilyn vuotomittaukset tulee suorittaa säännöllisesti, vähintään kerran vuodessa. Näin varmistutaan siitä, ettei rakenteissa ole tuona aikana tapahtunut muutoksia, jotka voisivat aiheuttaa tietoturvariskin.

Suojaustasoa III edustavat tilat sijaitsevat 20–100 m:n suojaetäisyydellä mahdollisesti riskialttiiksi arvioidusta hajasäteilyn kaappauspisteestä, tässä tapauksessa valvotun alueen ulkokehällä kulkevasta yleisestä tiestä. Kiinteistön tilat voidaan etäisyyden perusteella luokitella TEMPEST-tilavyöhykkeeseen 1.

Laitesuojausluokitus on Euroopan unionin laatima luokitus, joka jakaa hajasäteilyltä suojatut laitteet luokkiin, joiden mukaan niillä voidaan käsitellä salassa pidettävää tietoa. COST-laitesuojausluokkaan kuuluvat kaupalliset, ei suojausta sisältävät laitteet. Laitesuojausluokka C:hen kuuluvat laitteet ovat vähäisen suojauksen omaavat laiteet, laitesuojausluokka B:hen kuuluvat laitteet ovat keskimääräisen suojauksen omaavia ja laitesuojausluokka A:han kuuluvat laitteet ovat vahvimmin suojattuja.

Kun kyseessä on tila, jossa käsitellään suojaustason III aineistoa ja tila sijaitsee alle 100 metrin suojaetäisyydellä, tilassa tulisi käyttää kriittisen aineiston käsittelyssä ainoastaan

vähintään laitesuojaluokka C:n täyttäviä laitteita. Kuvassa 2 esitetään, minkä laiteluokan konetta tulee kulloinkin käyttää, kun vyöhykkeellä käsitellään esimerkkinä olevan tietoturvaluokan aineistoa. (3, s. 7.)

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

Kuva 2. Hajasäteilyltä suojattujen laitteiden valinta ja tilavyöhykeluokat (3, s. 7).

3 Rakenteellinen tietoturvallisuus kohteessa

3.1 Suojaustasot kohteessa

Kohteena olevassa rakennuksessa on suojaustason III tiloja 10 kpl, muut tilat rakennuksessa ovat suojaustason IV tiloja. Suojaustason III tiloja ovat tilat K01, K02, K03, K04, K05, K013, K016,102,103 ja 104.

3.2 Alue

Alue käsitteenä kattaa sisä- ja ulkotilat, mm. huoneet, laitetilat, varastot, arkistotilat, käytävät, edellä mainittujen muodostaman kokonaisuuden tai muun rakennuksen osan.

Viranomaisen tekemän uhka-arvion perusteella voidaan alueella liikkumista rajoittaa aidoilla, porteilla ja muilla ajoesteillä. Uhka-arvion perusteella otetaan kantaa myös alueen vaatimaan kameravalvontaan. Nykytilanteessa kohteen ulko-alueilla liikkumista ei ole rajoitettu, kohteen toiminnan vuoksi tulee ulko-alue olla rajattu aidalla ja aluetta tulee valvoa jatkuvasti kamerajärjestelmällä. Ulkoalueen rajaaminen mahdollistaa sen tehokkaamman valvonnan ja alueella kulkemisen seurannan.

3.3 Aidat

Kohteessa ei tällä hetkellä ole aidalla rajattua ulko-aluetta; aidan suojaava merkitys korostuu kohteessa sen sijainnin vuoksi. Suojattava alue on julkista tilaa, siksi aidalle ei ole suoria vaatimuksia. Kohteen aidan osalta tulisi kuitenkin noudattaa vähintään suojaustason IV tilojen vaatimukset täyttävää ratkaisua.

Kiinteistön aidan korkeus tulee siis olla minimissään 2,4 metriä, aidan verkon silmäkoko saa olla maksimissaan 40x40 mm, aitauslangan tulee olla minimissään 3 mm paksua, aidan yläreunaan tulee asentaa 2 kappaletta piikkilankaa ja aidan alareunaan tulee asentaa yksi piikkilanka. Piikkilangan tulee olla 2x16 mm sinkittyä terästä, ja aidan alareunan maksimikorkeus maasta saa olla 50 mm. (1, s. 30.)

3.4 Ulkopinnat

Kiinteistön ulkopintojen, myös ylä- ja alapohjan, tulee olla rakenteeltaan ja kestävyydeltään toteutettu niin, ettei tiloihin voida niiden kautta tunkeutua ilman että se havaitaan viranomaisen määrittelemässä vasteajassa. Seinäelementtien tulee olla asennettu niin, ettei niitä voida irrottaa rakennuksen ulkopuolelta. Seinärakenteissa tulee suosia vahvoja rakenneratkaisuja kuten teräsbetoni tai raudoitettu valuharkko. Rakennuksen uloimpaan kuoreen rajoittuvien rakenteiden tulee kestää SSF 1047:n luokan 3 murtokestävyydelle asetetut ajalliset vaatimukset tunkeutumiselle.

Kohteena olevan kiinteistön osalta tämä ei toteudu. Ulkoseinien rakenteen muuttaminen olemassa olevassa rakennuksessa on käytännössä mahdoton tehtävä, ainoaksi järkeväksi vaihtoehdoksi jää tällöin rakennuksen ulkoseinien vahvistaminen sisäpuoleisilla ratkaisuilla. Soveltuvana ratkaisuna voidaan käyttää Gyproc IBS -murtosuojalevyllä suojattua teräsrakenteista kipsilevyseinää. Rankana toimii Gyproc GFR -vahvistusranka, kipsilevyseinä vahvistetaan molemminpuolisella IBS-2-levyllä, levykerrosten saumat sijoitetaan eri rangoille. Metallilevyllä vahvistettu seinärakenne täyttää Finanssialan keskusliiton murtosuojaluokan 3 vaatimuksen, sillä saadaan aikaiseksi myös hyvä vaimennus hajasäteilyyn liittyen. (1, s. 27.)

Suojaustason III tilat tulee siirtää vyöhykeajattelun mukaisesti Suojaustason IV tilojen sisälle, tällöin suojaustaso III tilat eivät sijaitse ulkopintojen välittömässä yhteydessä.

3.5 Sisäseinät

Sisäseiniin kohdistuviin rakennevaatimuksiin vaikuttavat muut turvallisuustoteutukset ja rakenteiden toteutustapa. Sisäseinän toimiessa julkisen tilan ja korotetun tilan välisenä tilan jakajana sen tulee täyttää suuremmat vaatimukset kuin sen ollessa turvallisuusvyöhykkeen sisäinen väliseinä. Seinän tulee muut rakenteet huomioiden kumuloida vasteaikaa, jolloin sisempänä vyöhykkeellä olevaan tilaan tunkeutuminen hidastuu.

Tarkastelun kohteena olevassa kiinteistössä väliseinän ovat rakenteeltaan tavanomaisia väliseiniä eli puukoolattuja villaeristettyjä kevytrakenteisia väliseiniä. Tällaisten seinien rakenteellinen murtosuojaus on olematon.

Tilakokonaisuuden suunnitteluvaiheessa tulee huomioida erityisesti seuraavat kohdat: asiakaspalvelutilan seinärakenteiden osalta tulee kiinnittää huomiota äänenvaimennukseen, tilaa voidaan käyttää nykyiseen tarkoitukseen ilman että seinärakenteita massiivisesti muutetaan, mutta suojaustason IV tiloista tulee estää äänen kantautuminen julkiseen tilaan. Jos 1. kerroksen tiloja tullaan käyttämään suojaustason III työtehtäviin, tulee asiakaspalvelutilan väliseinä rakentaa ulkopintoja vastaavaan tasoon.

Vyöhykkeiden väliset seinät tulee rakentaa niin, ettei ääni kantaudu vyöhykkeeltä toiselle. Tämä tulee huomioida kaikissa läpivienneissä, kuten ilmanvaihdon ja kaapelointien läpivientikohdissa. Salassa pidettävät asiat eivät saa suusanallisen keskustelun välityksellä kulkeutua ymmärrettävinä turvallisuusvyöhykkeen ulkopuolelle. (1, s. 28.)

3.6 Ala- ja yläpohjat

Ala- sekä yläpohjan rakenteisiin kohdistuu samat vaateet kuin seinärakenteisiin. Rakenteiden vaatimukset tunkeutumisajalle riippuvat siitä, minkälaista käytössä olevaa tilaa niillä rajataan. Mikäli tilassa käsitellään useammin kuin satunnaisesti suojaustasojen II tai I tietoja, lattiarakenteessa suositellaan käytettävän esimerkiksi erillistä pintavalua tyypillisen ontelolaattarakenteen päällä. Samoin ylös nostettujen lattioiden ja alas laskettujen kattojen osalta tulee välitilojen olla teknisen valvonnan piirissä. (1, s. 28.)

Kiinteistön alapohjan rakenteet eivät kohteen osalta ole se todennäköisin tunkeutumistie, rakenne on rakennuksen iän mukaan tavanomainen ja valetun betonilattian rakenteellinen kestävyys on riittävä täyttääkseen suojaustason IV ja suojaustason III tilojen vaatimukset.

Rakennuksen yläpohjarakenteissa on huomattava tietoturvariski. Tiloihin voidaan tunkeutua yläpohjarakenteen läpi verrattain lyhyessä ajassa ja lähes ilman työkaluja. Vesikatteen muuttaminen murtovarmemmaksi vaatisi merkittäviä rakenteellisia muutoksia, joiden toteuttaminen on järkevää vasta vesikatteen uusinnan yhteydessä jos tuolloinkaan. Lähtökohtaisesti hyvänä rakenteellisena vaihtoehtona toimii teräsbetonilaatta. Mikäli katevaihtoehtona halutaan käyttää muuta materiaaliratkaisua, tulee rakenteen olla kerroksittainen ja riittävän kestävä. (5, s. 107.)

Vesikaton välitilaan johtaa kaksi lukitsematonta kulkutietä, toinen rakennuksen katolta ja toinen rakennuksen eteläseinustalta. Kumpikin kulkutie on sijoitettu niin, että niiden läheisyyteen pääsee ilman tikkaita tai muunlaista nostoapuvälinettä. Välitilan tulee olla jatkuvasti elektronisen valvonnan piirissä.

3.7 Ovirakenteet

Ovet ovat yleisimpiä murtautumisteitä rakennukseen. Suomen viranomaisten tekemien tunkeutumistestien perusteella kansainväliset normit täyttävät ovet eivät välttämättä kykene takaamaan riittäviä vasteaikoja kaikissa tilanteissa. Oviasennukset rakenteineen tulee toteuttaa siten, että niiden tunkeutumisen vasteaika myötäilee muuta ympäröivää rakenneratkaisua. (1, s. 28.)

Ovien asennus tulee suorittaa erityistä huolellisuutta noudattaen, ovien materiaali ja asennus standardin SFS-EN-1627 mukaisesti takaa riittävän kestävyyden. (16, s. 13.)

Ovien osalta pätee sama vaatimus kuin muitakin rakenneosia, salassa pidettävästä tiedoista käytävä keskustelu ei saa välittyä viereisiin tiloihin niille, joilla ei ole tietoon oikeutta (2, s. 28).

Kiinteistön ulko-ovet eivät täytä edellä mainittuja vaatimuksia. Ovet tulee uusia ja uudisasennusten yhteydessä tulee varmistaa karmien kiinnitysalustan vaatimustenmukaisuus. Tarvittavilta osin kiinnitysalusta tulee vahvistaa vastaamaan vaatimuksia.

Uusien ulko-ovien tulee täyttää murtoluokan 3 vaatimukset: ovien karmit on kiilattava; oven saranapuolelle tulee asentaa vähintään kolme murtosuojatappia; tapit tulee olla valmistettu teräksestä, jonka minimihalkaisija on 6 mm ja ulkonema vähintään 12 mm; ovi tulee olla huullettu; käyttölukon puoleinen käyntiväli saa olla maksimissaan 5 mm. Lisäksi mikäli uudet ovet ovat ikkunalliset, tulee ikkunoiden lasin olla luokan P6B murtosuojalasia tai ikkuna on suojattava rullakalterilla; sisäpuolinen suojausluokka on 4, ulkopuolinen suojausluokka on 3.

3.8 Lukitusjärjestelyt

Kiinteistönlukituksen kuvaaminen ei ole mahdollista tiedon arkaluontoisuuden takia. Laki viranomaisten toiminnan julkisuudesta 621/1999 6 luku 24§ 7 estää sen yksiselitteisesti.

Lukitusjärjestelmät tulee toteuttaa standardin SFS 7020 / SFS 5970 mukaisesti. (2, s. 23).

Rakennuksen ulko-ovet on varustettava Finanssialan keskusliiton vaatimukset täyttävällä turvalukituksella. Lukkojen sarjoitus tulee suunnitella kohteen käyttötarkoituksen mukaisesti. Avainten ja kulkutunnisteiden tulee olla yksilöllisesti merkittyjä ja niiden jako tulee dokumentoida. Avainten ja kulkuoikeuksien hallintajärjestely tulee olla dokumentoitu ja järjestelyä tulee valvoa. Vastuuhenkilöstöllä tulee olla hallussaan luettelo jaetuista avaimista, tilan lukostokaavio ja avainkortit. Turvallisuusvyöhykkeen jakamattomia avaimia tulee säilyttää asianmukaisessa kassakaapissa tai holvissa. Varmuuslukitusta suunniteltaessa tulee huomioida myös poistumistiereitit. Pelastuslaitoksen pääsy kohteelle on sovittava pelastusviranomaisen kanssa. Pelastuslaitoksen reittiavaimia säilytetään valvotuissa putkilukoissa. Kiinteistön ulkopuolella olevalla reittiavaimella ei saa päästä suoraan korotetun tai korkean vyöhykkeen (KELTAINEN/SININEN) tiloihin, vaan suunnitellun hyökkäysreitin varrelle, kiinteistön sisälle järjestetään toinen valvottu putkilukko, joka mahdollistaa palokunnan pääsyn korotetun tai korkean vyöhykkeen tiloihin. KELTAISELLE tai SINISELLE turvallisuusvyöhykkeille johtavat ovet on varustettava sähköisellä kulunvalvonnalla. KELTAISELLE tai SINISELLE turvallisuusvyöhykkeelle johtavat, turvallisuusvyöhykkeiden väliset luukut tai hätäpoistumistiet on varustettava avattavin kalterein ja valvottava tunkeutumisen ilmaisujärjestelmillä. Toteutus ei saa estää luukun tai hätäpoistumistien toimintaa. (1, s. 29.)

3.9 Ikkunarakenteet

Ikkunarakenteet ovat ovirakenteiden lisäksi todennäköisimpiä tunkeutumisreittejä rakennukseen; tämän vuoksi ikkunoiden osalta on laadittu turvallisuusnormeja. Suomalaisten viranomaisten tekemien tunkeutumistestien perusteella norminmukaisuus ei aina riitä takaamaan tavoiteltuja vasteaikoja. Ikkunoiden niitä ympäröivine rakenteineen tulee olla niin kestäviä, että niillä saavutetaan riittävä vasteaika tunkeutumistapahtuman aikana. Ikkunoiden karmien kiinnitykseen, karmien kestävyyteen ja lukitusjärjestelmien lujuuteen tulee kiinnittää riittävästi huomiota. Ikkunan lukituksen ja salpojen tulee olla standardin SFS 7020 mukaiset. Ikkuna-aukkojen karmirakenteet tulee toteuttaa niin, ettei turvalasia

pystytä irrottamaan karmista eikä karmia pystytä kevyillä käsityökaluilla irrottamaan seinästä. Tämä edellyttää teräskarmia, joka on kiinnitetty lujasi ympäröivään seinärakenteeseen. (13, s. 8.)

Osassa kohteen toisen kerroksen ikkunoista ikkunan alareuna on yli neljän metrin korkeudessa. Tällöin tiloihin tunkeutuminen kyseisten ikkunoiden kautta edellyttää työskentelyä tikkailla tai muulla nostoapuvälineellä. Niissä tiloissa, joiden ikkuna sijaitsee alle neljän metrin korkeudessa ja joissa säilytetään vähintään suojaustason III tietoa, tulee ikkuna-aukot varustaa kaltereilla tai normin SFS EN 356 mukaisella P6B-luokan täyttävällä suojalasilla. (17, s. 6.) Nämä ikkunat eivät saa olla avattavia. Tiloissa, joissa käsitellään suojaustason IV aineistoa ja joiden ikkunat sijaitsevat alle neljän metrin korkeudessa, tulee ikkunoihin asentaa murtosuojakalvot, jotka täyttävät vähintään normin SFS EN 356 luokan P1A vaatimukset. (1, s. 30.)

Kiinteistön ikkunoiden kautta tapahtuva salakatselu tulee estää, joko suojakalvoilla tai sälekaihtimilla. Tiloihin ei saa olla näköyhteyttä silloin, kun tilassa käsitellään suojaustasolle IV tai sitä korkeammalle luokiteltua tietoa. Salakatselun estämiseen tule kiinnittää erityistä huomiota etenkin asiakaspalvelutilan ja viranomaistilan välisessä palvelutiskissä. (2, s. 27.)

3.10 Aukot rakenteissa

Tarkasteltavan kiinteistön lämmönjakohuoneeseen saapuvat lämpöputket on ohjattu seinärakenteen läpi vanhasta ilmanottoaukosta. Rakenne tulee kokonaisuudessaan käydä läpi ja aukko peittää sisäpuolelta teräsbetoniin ankkuroitavalla ritilällä tunkeutumisen estämiseksi.

3.11 Ilmanvaihto

Eri suojaustasojen välisten rakenteiden läpimenot tulee varustaa ääniloukuin ja suojaustason III tiloihin johtavat kanavat tulee kummaltakin puolilta seinää rakentaa materiaaleista, jotka eivät sisällä metallia. Näin vähennetään hajasäteilyn riskiä rakenteiden läpi. Eri kerrosten väliset ilmanvaihtokuilut tulee valvoa elektronisella tunkeutumisenilmaisulla sekä varmistaa, etteivät äänet tilojen välillä kulkeudu kuilujen kautta. (1, s. 28.)

4 Tulokset

Tarkasteltavan kiinteistön osalta tulee suunnitella tilaratkaisut niin, että suojaustaso III tilat siirrettäisiin rakennuksen sisäosiin ja mahdollisuuksien mukaan maanpinnan alapuolelle. Nykyisten rakenteiden muuttaminen yksittäisten, eri kohtiin rakennusta sijoittuviin suojaustason III tilojen osalta on kustannuksiltaan suurempi kuin koko rakennusta koskeva tilanmuutos. Opinnäytetyön aikana selvisi, ettei käytännössä mikään tila tällä hetkellä täysin täytä VAHTI-ohjeiston mukaisia vaatimuksia salassa pidettävän aineiston käsittelylle. Ikkuna-, ovi- ja ulkoseinärakenteet eivät täytä SFS-EN-1627:n luokkaa 4. (16, s. 24.) Tämän vuoksi suojaustason III tilat tulee sijoittaa suojaustason IV tilojen sisäpuolelle uudisrakennettuihin tiloihin, ensisijaisena vaihtoehtona kellarikerroksen tilojen muuttaminen rakenteiltaan suojaustasoa III vastaaviksi ja toimintojen siirtäminen kyseisiin tiloihin.

Tietoliikenteen laitetila voidaan säilyttää nykyisellä paikallaan. Tila vaatii merkittäviä muutoksia: tilan kaikki pinnat mukaan lukien ovirakenne tulee suojata metalliverkolla/levyllä hajasäteilyn minimoimiseksi, tilan ilmanvaihtokanavat tulee vaimentaa RF-suodattimilla, ilmanvaihtokanavat tilaan tulee katkaista metriä ennen tilaa ja tilan seinän läpäisevä kanavaosa tulee toteuttaa kanavamateriaalilla joka ei sisällä metallia, soveltuvana ratkaisuna Uponorventilation.

Asiakastilat tulisi selkeästi eriyttää muusta toiminnasta, ja näistä tiloista ei saa olla suoraa näköyhteyttä suojaustason IV tiloihin.

Tilaratkaisun suunnitteluvaiheessa tulee huomioida radiosignaalien vaimennustarve suojatason III tilojen osalta sekä rakennusmateriaalit ja rakenneratkaisut tulee valita niin, että niillä saadaan riittävä vaimennus radiosignaalien osalta.

5 Päätelmät

Kohteen osalta monessa asiassa on parannettavaa. Tulee kuitenkin huomioida että, moni asia on jo valmiiksi hyvällä tasolla, kohteessa työskentelevien osapuolien henkilökunnilla on hyvä turvallisuuskulttuuri, ja sitä aktiivisesti kehitetään parempaan suuntaan. Kohteen ikä asettaa selkeitä rajoitteita sille, että kaikki rakenteelliset asiat olisivat samalla tasolla kuin uudessa kiinteistössä.

Opinnäytetyön aikana suoritettu tarkastelu viranomaiskohteissa tulisi suorittaa määräajoin, ja sen tulisi olla osana normaalia kiinteistönpidon prosessia. Varsinkin vanhempien, jo vuosia käytössä olleiden kohteiden osalta, tarkastelulla voidaan paikallistaa korjaustoimenpiteitä vaativat kohdat. Samoin määräykset voivat muuttua, jolloin kiinteistön tietoturvallisuus tulisi auditoida uudelleen.

Kiinteistöjen rakenne- ja tilaratkaisujen tulee olla hyvin dokumentoituna, jotta niiden auditointi olisi vaivatonta ja korjaavat toimenpiteet voidaan suunnitella helpommin. Erityisesti rakenneratkaisuiden vaatimustenmukaisuus tulee dokumentoida hyvin, ja tiloista olisi hyvä laatia omat tilakortit tietoturvallisuuden osalta. Ohjaavat säädökset ovat erittäin lakitekstipainotteista, ne vaativat tuekseen selkeämpää ohjeistusta ja esimerkkejä jotta määräykset voidaan toteuttaa kohteissa. Parhain hyöty auditoinnista saadaan, kun sen suorittaa työryhmä, jonka jäsenet kukin edustavat omaa osaamisaluettaan, ja ryhmää koordinoi tilaturvallisuuteen hyvin perehtynyt projektipäällikkö.

Opinnäytetyössä toteutetun auditoinnin tuloksena saatiin kartoitettua tietoturvallisuuden puutteet kohteen osalta. Jotta korjaavat toimenpiteet ovat järkevästi toteuttavissa, tulee kokonaisuus suunnitella uudelleen. Suunnittelun tueksi tulee kiinteistön rakenteiden osalta tehdä lisäselvityksiä, mm. hajasäteilymittaus. Opinnäytetyötä voidaan käyttää suunnittelua avustavana dokumenttina kyseisen kohteen osalta.

Lähteet

1 VAHTI 2/2013. Toimitilojen tietoturvaohje. Ministeriöille, virastoille ja laitoksille. 2020. Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriö. Verkkoaineisto. Digi- ja viestintävirasto. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22013-toimitilojen-tietoturvaohje Päivitetty 9.6.2020. Luettu 02.09.2020

2 Katakri 2015 Tietoturvallisuudenauditointityökalu viranomaisille. 2015. Helsinki. Valtiovarainministeriö

3 Sähkömagneettisen hajasäteilyn aiheuttamien tietoturvariskien ehkäisyn periaatteet. 2013. Helsinki. Viestintävirasto

4 Rakenteellinen murtosuojaus III. 2017. Helsinki. Finanssiala ry

5 Fennelly Lawrence J. 2017. Effective physical security. Amsterdam. Butterworth-Heinemann

6 Tietoa meistä. 2021. Verkkoaineisto. Senaatti-kiinteistöt 2021. https://www.senaatti.fi/tietoa-meista/. Luettu 08.01.2021

7 VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriö. Verkkoaineisto. Digi- ja viestintävirasto. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta Päivitetty 9.6.2020. Luettu 09.09.2020

8 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 2010. 681/2010.

9 Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 2019. 1101/2019.

10 EU: Neuvoston päätös, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuusäännöistä. 2013. 2013/488/EU

11 Laki viranomaisten toiminnan julkisuudesta. 1999. 621/1999

12 SFS 5970. Rakennushelat. Kiinteästi asennettavat lukot ja riippulukot. Murronkestävyys. Vaatimukset ja testausmenetelmät. 2015. Helsinki: Suomen standardisoimisliitto SFS ry

13 SFS 7020. Rakennushelat. Kiinteästi asennettavat lukot ja riippulukot. Murronkestävyys. Luokitus. 2015. Helsinki: Suomen standardisoimisliitto SFS ry

14 SFS-EN-14450:2017:en. Secure storage units. Requirements, classification and methods of test for resistance to burglary. Secure safe cabinets. 2017. Helsinki: Suomen standardisoimisliitto SFS ry

15 SFS-EN-1143-1:2019:en. Secure storage units. Requirements, classification and methods of test for resistance to burglary. Part 1: Safes, ATM safes, strongroom doors and strongrooms. 2019. Helsinki: Suomen standardisoimisliitto SFS ry

16 SFS-EN-1627:en. Pedestrian doorsets, windows, curtain walling, grilles and shutters. Burglar resistance. Requirements and classification. 2012. Helsinki: Suomen standardisoimisliitto SFS ry

17 SFS-EN-356. Rakennuslasit. Suojalasitus. Murtautumisyrityksen kestävyyden testaus ja luokitus. 2001. Helsinki: Suomen standardisoimisliitto SFS ry