LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Toimitilat tietoturvallisuuden korotetulle tasolle valtionhallinnossa

Ronkainen, Maija

2016 Laurea

Laurea-ammattikorkeakoulu

Toimitilat tietoturvallisuuden korotetulle tasolle valtionhallinnossa

Maija Ronkainen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Elokuu, 2016

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Maija Ronkainen

Toimitilat tietoturvallisuuden korotetulle tasolle valtionhallinnossa

Vuosi 2016 Sivumäärä 57

Valtionhallinnon organisaatiot, joissa käsitellään salassa pidettäviä tietoja jotka aiheuttavat paljastuessaan tai väärin käytettäessä vahinkoa yleiselle tai yksityiselle edulle, ovat velvollisia luomaan tietojen käsittelylle tavallista tiukemmat suojaustoimenpiteet. Tämä opinnäytetyö on suunnattu kaikille sellaisille organisaatioille, joita tämä velvoite koskee, sekä toimeksiannon antaneelle salassa pysyvälle kohdeorganisaatiolle.

Tämän opinnäytetyön tarkoituksena oli luoda yksi valtionhallinnon organisaatioiden hyödynnettäväksi tarkoitettu toimenpidesuunnitelma ja yksi kohdeorganisaation hyödynnettäväksi tarkoitettu salassa pidettävä toimenpidesuunnitelma siitä, miten organisaation toimitilat saadaan tietoturvallisuuden korotetulle tasolle. Korotetun tason vaatimukset määräytyvät VAHTI 2/2013 toimitilojen tietoturvaohjeen sekä tietoturva-asetuksen (681/2010) pohjalta. Säädösympäristö luo tälle työlle muutenkin vahvan viitekehyksen, minkä lisäksi tutkimusmenetelmänä käytetyn kirjallisuuskatsauksen pohjalta erinäiset kirjalliset lähteet ja kriteeristöt ovat vaikuttaneet tietoperustaan.

Muita tutkimusmenetelmiä olivat haastattelut ja benchmarking. Haastatteluilla hankittiin tietoa kohdeorganisaation tilanteesta ja edellytyksistä toimitilojen tietoturvallisuuden suhteen, ja benchmarkingilla etsittiin hyviä käytäntöjä ja kokemuksia muista valtionhallinnon organisaatioista. Tuloksien perusteella rakennettiin toimenpidesuunnitelmat.

Tuloksissa käy ilmi, että toimitilojen tietoturvallisuuden korottamisessa tulisi ottaa vahvasti huomioon riskiarviointi eikä noudattaa sokeasti VAHTI-kriteeristöjä. Lisäksi on tärkeää huomioida henkilöstön merkitys toimitilojen turvallisuuden ylläpidossa, sillä fyysiset suojaustoimenpiteet ovat tehokkaimmillaan, kun henkilöstö toimii oikein. Nämä asiat on pyritty huomioimaan toimenpidesuunnitelmissa. VAHTI-säännösympäristö muuttuu vuoden vaihteessa, ja se tulee varmasti tarjoamaan tälle työlle monia jatkokehitysmahdollisuuksia.

Asiasanat: Riskiarvio, Suojaustaso, Tietojen luokittelu, Toimitilaturvallisuus

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor's Thesis

Maija Ronkainen

Reaching a higher information security protection level in the premises of the State Administration

Year 2016 Pages 57

Organizations that are in the State Administration are obliged to protect their information with more significant actions if they process information that would cause damage when revealed. This thesis is aimed at those organizations and additionally to the target organization which gave this assignment. The target organization's name is not revealed in this thesis.

The purpose of this thesis was to create one public action plan for the organizations of the State Administration and another confidential action plan for the target organization which will not be published. The purpose of the action plans is to show how an organization can get their premises to higher information security protection level. The requirements of the higher level come from VAHTI 2/2013 instructions and from the information security regulation (681/2010). The regulatory environment in addition to the literature review create a strong frame of reference to this thesis.

Other research methods in this thesis are interviews and benchmarking. The interviews were held to collect information about the information security status of the target organization. Benchmarking was used to collect good ideas and experiences from other organizations in the State Administration. The results of these research methods were the baseline of the action plans.

The results show that risk assessment should have a bigger part in the process when trying to reach higher information security protection level in the premises. Therefore organizations should not follow blindly VAHTI instructions. The results also show the significance of the actions of personnel. The physical protection methods are at their best only when the personnel acts accordingly. These factors have shaped the action plans and in the future, when VAHTI instructions go through some big changes, they will likely provide many possibilities for further development.

Keywords: Information classification, Physical security, Protection level, Risk assessment

Sisällys

1 Johdanto

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa tuli voimaan 1.10.2010, ja sen mukaan viranomaisten käytössä olevien toimitilojen tulee täyttää asetuksen tilaturvallisuutta koskevat vaatimukset viiden vuoden kuluessa sen voimaantulosta (L681/2010, 23§). Todellisuudessa monissa valtionhallinnon organisaatioissa ei kuitenkaan olla vielä tällä tasolla, vaikka aikaraja on mennyt umpeen viime vuonna. Jotta organisaatiot saavuttaisivat korotetun tietoturvatason toimitiloissaan helpommin, on luotu ohjeistus, jossa on kriteeristöt joita noudattamalla tälle tasolle päästään. VAHTI 2/2013 toimitilojen tietoturvaohje -nimellä kulkeva ohje näyttää turvallisuusvaatimukset, jotka pitää täyttää, että korotetulle tasolle päästään. Siinä ei ole kuitenkaan kuvailtu toimenpiteitä, joilla nämä vaatimukset täytetään. Niiden puutteesta syntyi tarve tälle opinnäytetyölle.

Tutkimusongelma on, miten tietoturvallisuuden perustasolta päästään korotetulle tasolle toimitiloissa. Opinnäytetyö keskittyy erääseen valtionhallinnon organisaatioon, jolla on useita toimitiloja ympäri Suomen jotka ovat eri tasoilla toimitilojensa tietoturvallisuuden suhteen. Organisaatiossa halutaan yhtenevät edellytykset jokaisen toimipisteen turvalliselle tietojenkäsittelylle, sekä koko henkilöstö osaaviksi ja vastuullisiksi tietojen käsittelijöiksi. Kohdeorganisaation lisäksi keskitytään valtionhallintoon kokonaisuutena, ja luodaan käytäntöjä, jotka sopivat usean valtionhallinnon organisaation toimitilojen tietoturvallisuuden korottamiseen. On kuitenkin huomioitava, että valtionhallinnossa on hyvin monen tyyppistä toimintaa, joten tämä opinnäytetyö ei pysty aivan jokaisen tarpeeseen vastaamaan.

Opinnäytetyön aluksi käydään läpi kohdeorganisaatiolta saatua toimeksiantoa sekä opinnäytetyöhön vaikuttavia taustatekijöitä, jotka määrittyvät muun muassa lainsäädännöstä ja muusta tietoperustasta. Lisäksi käydään läpi kohdeorganisaation nykytilannetta VAHTI 2/2013 -ohjeen pohjalta. Opinnäytetyöhön on haastateltu sekä kohdeorganisaation sisäisiä asiantuntijoita, että benchmarking-tarkoituksessa henkilöitä muista organisaatioista, joilla on aiheeseen liittyvää kokemusta. Näiden haastattelujen tuloksia, sekä niiden ja tietoperustan pohjalta tehtyjä toimenpidesuunnitelmia käydään työn loppupuolella läpi. Viimeisenä on pohdinnallinen osuus, jossa avataan prosessin aikaisia onnistumisia ja kehittämispaikkoja.

2 Tutkimusongelma ja taustatekijät

Tämän opinnäytetyön toimeksiantona on kehittää toimenpidesuunnitelma siitä, kuinka erään valtion viraston toimitiloissa päästään VAHTI 2/2013 toimitilojen tietoturvaohjeen mukaiselle, tietoturvallisuuden korotetulle tasolle rakenteiden, valvontajärjestelyjen ja henkilöstön toimintatapojen osalta. Tutkimusongelma onkin, miten toimitiloissa päästään tietoturvallisuuden

perustasolta korotetulle tasolle. Opinnäytetyö on prosessikuvaus siitä, miten toimenpidesuunnitelma syntyy, ja liitteenä on itse toimenpidesuunnitelma työn toimeksiantajan hyödynnettäväksi sekä yleispätevä toimenpidesuunnitelma valtion virastojen hyödynnettäväksi. Toimeksiantajalle menevä suunnitelma jää salaiseksi perusteenaan julkisuuslakiin kirjattu kohta, jossa salassa pidettäviin asiakirjoihin luokitellaan muun muassa henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat (L621/1999, 24§). Valtion virastoille suunnattu suunnitelma on julkinen.

2.1 Keskeiset käsitteet

Tässä käydään läpi tämän opinnäytetyön keskeisempiä ja yleisimmin käytettyjä käsitteitä. Käsitteet on avattu tässä kohtaa lyhyesti yleiskuvan antamiseksi, osaa niistä on tarpeen vaatiessa avattu myöhemmässä vaiheessa tarkemmin. Tässä läpi käydyt käsitteet toistuvat jatkuvasti läpi opinnäytetyön, ja opinnäytetyön tuotos perustuu kyseisten asioiden ympärille.

Rakenteet tarkoittavat tässä opinnäytetyössä toimitilaturvallisuuden osaa, jossa rakennuksen ominaisuuksilla pyritään vaikuttamaan turvallisuuteen. Rakenteissa otetaan huomioon ovet, ikkunat, seinä-, lattia- ja kattorakenteet sekä lukitukset (VAHTI 2/2013, 37-39).

Salassa pidettävä tieto on sellaista tietoa, joka on laissa viranomaisen toiminnan julkisuudesta määritelty salassa pidettäväksi, tai joka on viranomaisen toimesta määrätty salassa pidettäväksi tai josta on lailla säädetty vaitiolovelvollisuus. Tällaisia tietoja voivat olla esimerkiksi valtionhallinnon liikelaitoksen liiketoimintaa koskevat tiedot tai valtionhallinnon organisaation henkilöstön turvallisuutta koskevat tiedot. (L621/1999, 22§.)

Suojaustasot ovat luokkia, joihin tiedot luokitellaan sen mukaan, minkälaisia tietoturvallisuusvaatimuksia niiden käsittelyssä on tarpeen noudattaa. Suojaustasot ovat välillä IV-I, joista IV-tasolla tiedon oikeudettomasta paljastumisesta on lievimmät seuraukset, kun taas I-tasolla vakavimmat. (L681/2010, 8§.)

Valtionhallinto koostuu valtion keskushallinnosta, aluehallinnosta sekä paikallishallinnosta. Valtionhallinnon päätehtävänä on yhteiskuntarauhan ja turvallisuuden ylläpitäminen sekä keskushallinnon järjestäminen. (Valtion hallintojärjestelmä 2016.)

Valvontajärjestelyt tarkoittavat tässä opinnäytetyössä toimitilaturvallisuuden osaa, jossa erilaisilla elektronisilla järjestelmillä sekä vartioinnilla pyritään vaikuttamaan toimitilaturvallisuuteen. Tällaisia ovat kameravalvonta, rikosilmaisimet, kulunvalvonta sekä erilaiset vartioinnin muodot kuten aula- tai piirivartiointi (VAHTI 2/2013, 41).

2.2 Fyysinen turvallisuus osana organisaation riskienhallintaa

Fyysinen turvallisuus on osa organisaatioturvallisuutta. Organisaatioturvallisuuden osa-alueita ovat toimitila- ja kiinteistöturvallisuus, tietoturvallisuus, väärinkäytösten ja poikkeamien hallinta, varautuminen ja kriisinhallinta, pelastusturvallisuus, henkilöstöturvallisuus, ympäristöturvallisuus, työturvallisuus sekä tuotannon ja toiminnan turvallisuus (EK 2016). Fyysinen turvallisuus koskettaa melkein jokaista organisaatioturvallisuuden osa-aluetta, vaikka se enimmäkseen mielletäänkin kiinteistö- ja toimitilaturvallisuudeksi. Fyysinen turvallisuus on organisaation henkilöstön, järjestelmien ja tietojen suojaamista. Siinä huomioon otettavia asioita ovat muun muassa palo- ja pelastusturvallisuus, murtovahinkojen torjunta, erilaiset valvontajärjestelmät sekä henkilöstön työturvallisuus. Fyysisen turvallisuuden tarkoituksena on turvata organisaation häiriötön toiminta kaikissa tilanteissa. (Vahti ylläpito 2009.)

Organisaation fyysisen turvallisuuden tulisi keskittyä siihen, miten fyysisten tilojen sisäpuolella olevat suojattavat kohteet pysyvät turvassa. Jos jätetään pois palo- ja pelastusturvallisuuteen liittyvät asiat, voidaan vielä tarkemmin määritellä, että fyysisen turvallisuuden tarkoitus on pitää organisaation tiedot, järjestelmät ja henkilöstö suojassa ulkopuolisilta uhkilta. Parhaaseen tulokseen tässä päästään, kun uhkilta suojaudutaan useilla päällekkäisillä suojausmenetelmillä. John Perdikaris (2014, 137) kutsuu tätä nimellä ”multibarrier approach”. Käytännössä tämä tarkoittaa sitä, että tiloihin kuulumattoman henkilön pääsy sinne hidastetaan tai estetään ensin fyysisten rakenteiden, sitten teknisten hälytys- ja valvontajärjestelyiden sekä kulunvalvonnan ja lopulta vartiointihenkilökunnan toimesta (Perdikaris 2014, 137-140). Suomeksi tästä lähestymistavasta käytetään usein termiä kehäajattelu. Sen lähtökohtana on, että mitä hitaampaa, riskialttiimpaa ja kalliimpaa tiloihin tunkeutuminen on sinne kuulumattomilta henkilöiltä, sitä suuremmaksi kasvaa kynnys yrittää sekä riski kiinnijäämisestä (Perdikaris 2014, 137).

Toimitilaturvallisuus on osa fyysistä turvallisuutta. Sillä tarkoitetaan kaikkia rakenteellisia ja valvonnallisia järjestelmiä, joilla varmistetaan tilojen ja tietojen pysyminen oikeutettujen henkilöiden hallinnassa. Vaikka kiinteistön omistaja usein hoitaa tilojen rakenteisiin liittyvät asiat, on kuitenkin vastuu tilojen riittävästä suojaamisesta organisaatiolla itsellään (Vahti ylläpito 2009). Toimitilojen turvallisuustaso on siis arvioitava oma-aloitteisesti organisaatiossa, ja tarvittavat muutokset vietävä eteenpäin. Vaikka monet turvallisuuspalvelut voidaan nykyään hankkia ulkoisilta organisaatioilta, ei riskienhallintaa kuitenkaan voida ulkoistaa. (VAHTI 2/2010, 38.)

Laaksonen, Nevasalo ja Tomula (2006) puhuvat Yrityksen tietoturvakäsikirjassa fyysisen tietoturvallisuuden hallinnasta. He painottavat etenkin fyysisen toimintaympäristön säännöllistä uudelleenarviointia osana tehokasta tietoturvallisuuden hallintaa (2006, 125). Turvallisuuden

parantaminen ei siis lopu siihen, kun tavoitellulle tasolle ollaan päästy. Samaa mieltä on Gillies (2012, 78), jonka mukaan turvallisuuden parantaminen on jatkuvaa oppimista ja ympäristön mukana muovaantumista. Gilliesin (2012, 147) mukaan jatkuvan parantamisen tulee olla fyysisessä turvallisuudessa sekä osana turvallisuustoimenpiteitä, että niiden arviointia. Tästä voi päätellä, että suojaustoimenpiteiden riittävyyden arvioinnin lisäksi tulee säännöllisesti arvioida, käytetäänkö niiden mittaamiseen toimivia keinoja.

2.3 Toimitilojen tietoturvallisuus

VAHTI 2/2013 toimitilojen tietoturvaohje toimii tämän opinnäytetyön kehyksenä koko projektin ajan. Kyseisessä ohjeessa on määritelty tärkeimmät toimitiloja koskevat turvallisuusasiat, joita noudattamalla organisaation tietoja pystytään käsittelemään mahdollisimman turvallisesti. Ohje katsoo fyysistä turvallisuutta nimenomaan tietojen suojaamisen näkökulmasta, eikä siinä ole otettu kantaa muihin fyysisen turvallisuuden osiin, kuten paloturvallisuuteen. Tällä opinnäytetyöllä vastataan nimenomaan tietoturvallisuuden korottamisen tarpeisiin, joten ohje koettiin sopivaksi tarkoitukseen. Ohjeessa toimitilat on jaettu turvallisuusvyöhykkeisiin sen mukaan, minkä tason tietoja niissä käsitellään. (VAHTI 2/2013, 19-21.)

VAHTI 2/2013 -ohje on suositus, eikä näin ollen kehota noudattamaan sokeasti jokaista siinä olevaa vaatimusta. Ohjetta on tarkoitus muovata oman organisaation tarpeiden mukaiseksi. Ohjeen vaatimukset ovat myös melko yleispiirteisiä, mikä antaa tilaa organisaation omien tarpeiden huomioimiseen. Nämä tekijät edistävät melko joustavan pohjan luomista sopivien suojauskeinojen kartoittamiselle. Yleisenä ohjenuorana kuitenkin on, että mitä korkeamman tason tietoja tiloissa käsitellään, sitä tarkempia suojaustoimenpiteitä vaaditaan. VAHTI 2/2013 –ohje määrittelee toimitilansa niin, että suojaustason IV tietoa käsitellään perustason toimistotiloissa, suojaustason III tietoa korotetun tason toimistotiloissa ja suojaustason II tietoa korkean tason työskentely- tai neuvottelutiloissa. (VAHTI 2/2013, 19-21, 26).

Vaikka VAHTI 2/2013 -ohjeessa on jonkin verran joustavuutta, sitä tuo toimitilaturvallisuuteen lisää toinen samankaltainen ohjeistus, eli puolustusministeriön laatima Katakrin kolmas versio. Puolustusministeriön (2015, 16) mukaan fyysisen turvallisuus lähtee liikkeelle suunnittelusta, ja siinä tulee ottaa huomioon tiedon suojaustasot, rakennuksen ominaisuudet ja sen turvallisuusdokumentaation luottamuksellisuus, tietojenkäsittelyyn tarkoitetut välineet ja järjestelmät, käsiteltävien tietojen määrä, sekä kuinka usein tietyn tasoisia tietoja tiloissa käsitellään. Nämä ovat pitkälti samoja asioita kuin VAHTI 2/2013 –ohjeessa, mutta Katakri tuo niihin tueksi hieman lisätietoa muista lähteistä. Katakrissa (2015, 17) painotetaan lisäksi kokonaisvaltaista ajattelua turvatoimia suunniteltaessa. Sen mukaan suunnitteluvaiheessa on huo-

mioitava rakennusten ympäristö ja rakenne, sekä tulee olla tietoinen todennäköisimmistä uhkista. VAHTI 2/2013 -ohjeessa näitä asioita ei ole painotettu samassa mittakaavassa, jolloin sen kriteeristölle annetaan enemmän valtaa toimipisteen ominaispiirteiden kustannuksella.

Katakrin näkemystä tukevat myös Ihamäki, Liukkonen ja Savolainen julkaisussaan Kiinteistö- ja tilaturvallisuuden tasot. Heidän mukaan (2014, 7) soveltuvimmat suojauskeinot löytyvät vasta, kun on selvitetty todennäköisimmät uhkat, jotka kohdistuvat kiinteistöön ja sen toimintaan sekä ympäristöön. Samassa julkaisussa (2014, 9) todetaan myös, että kiinteistön käyttäjät tulee perehdyttää sekä sen rakenteellisiin, että toiminnallisiin ominaisuuksiin. Henkilöstön toiminnalla on siis merkityksensä fyysisten suojaustoimenpiteiden tukena. Tälle annetaan sekä VAHTI 2/2013 -ohjeessa että Katakrissa hyvin vähän huomiota.

Henkilöstön toimintaa painottaa myös Peltier (2013, 117) toteamalla, että tiedon suojaaminen ja hallinta on jo valmiiksi vaikeaa, mutta ihmisten virheet tekevät siitä entistä hankalampaa. Peltier ehdottaa (2013, 127-129) useita keinoja henkilöstön turvallisuustietoisuuden parantamiseksi, kuten ohjeistuksia, säännöllisiä koulutuksia, tietoiskuja turvallisuuden kauhutarinoista, muistutuksia turvallisuuskäytännöistä sekä palkitsemis- ja rangaitsemiskäytäntöjä. Jotkin keinoista eivät välttämättä sovellu valtionhallintoon, mutta kaikille niille yhteistä on niiden jatkuvuus. Turvallisuustietoisuuden ylläpito on jatkuvaa, koko ajan muuttuvaa toimintaa, jossa avainasemassa on motivaatio (Peltier 2013, 145).

Motivaatiota lisää johdon sitoutuminen asiaan. Paavo Porvari käsittelee väitöskirjassaan Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa (2012) johtamisen merkitystä tietoturvallisuuden inhimillisiin haavoittuvuuksiin. Porvarin mukaan (2012, 135) johdon tulisi aktiivisesti tutkia organisaation tietoturvallisuustietoisuutta ja tietoturvallisuuskulttuuria tulisi pystyä mittaamaan. Fyysistä turvallisuutta pystytään mittaamaan helpommin kriteeristöjen avulla, mutta turvallisuustietoutta varten täytyy keksiä uusia menetelmiä.

2.4 Salassa pidettävät tiedot valtionhallinnossa

Kohdeorganisaatio käsittelee säännöllisesti sellaisia tietoja, jotka laissa viranomaisten toiminnan julkisuudesta (L621/1999) on määritelty salassa pidettäviksi. Tällaisia ovat kyseisen lain mukaan esimerkiksi asiakirjat, jotka sisältävät tietoa valtion laitosten liike- tai ammattisalaisuudesta tai liiketoimintaan liittyvistä asioista jotka paljastuessaan aiheuttaisivat taloudellista vahinkoa tai haittaisivat kilpailuasemaa. Toinen esimerkki samasta pykälästä on henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyitä koskevat asiakirjat. (L621/1999, 24§.)

Merkittävä osa tiedosta joka kohdeorganisaatiossa, tai valtionhallinnossa ylipäätään, liikkuu sisäisesti, on salassa pidettävää. Salassa pidettävä tieto on luokiteltava vielä erikseen sen mukaan, kuinka paljon sen paljastuminen aiheuttaisi vahinkoa. Tiedon laatija on aina vastuussa tästä. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (L681/2010) määrittää tiedon luokiteltavaksi neljään luokkaan niissä olevan salassa pidettävän materiaalin perusteella niin, että mitä korkeampi suojaustaso, sitä suurempaa vahinkoa tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa. Suojaustasolla IV vahingot ovat pienimmät, ja suojaustasolla I suurimmat. (L681/2010, 9§.)

Kohdeorganisaatiossa käsiteltävistä salassa pidettävistä tiedoista suurin osa on suojaustasoa IV tai III. Tällaisia tietoja saavat käsitellä vain sellaiset henkilöt, joiden työn suorittamisen kannalta ne ovat välttämättömiä. Samassa asetuksessa (L681/2010, 14§) annetaan vaatimuksia myös salassa pidettävän tiedon fyysisestä suojauksesta ja niitä käsittelevien henkilöiden tunnistamisesta. Juuri tiedon luokittelu on perustana toimitilojen tietoturvallisuudenkin luokittelulle. Koska kohdeorganisaatiossa käsitellään sekä perus- että korotetun tason tietoja, tulee toimitilojenkin olla korotetulla tasolla. Tähän antaa ohjeita VAHTI 2/2013 –ohje, jonka avulla kohdeorganisaatioon tehtyjen arviointien tuloksia käsitellään seuraavaksi.

2.5 Toimitilojen arviointi VAHTI 2/2013 -kriteeristön avulla

Kuten aiemmin on mainittu, kohdeorganisaatiossa käsitellään muutoin kuin satunnaisesti suojaustason III tietoja, joten sen toimitilojen kuuluu olla korotetulla turvallisuusvyöhykkeellä. VAHTI 2/2013 –ohjeesta löytyy taulukko siitä, mitä asioita tulisi korotetun tason tiloissa ottaa huomioon. Taulukossa käsiteltäviä osa-alueita ovat alue, rakenteet, tilahallinta, valvontajärjestelyt ja tietotekniset laitetilat. Tästä taulukosta on muokattu kohdeviraston käyttöön sopivampi taulukko kriteereineen, jolla kohdeviraston toimitiloja on kartoitettu. Kohdevirastolle suunnitellussa taulukossa (Liite 1, esimerkki erääseen toimipisteeseen tehdystä arvioinnista) osa-alueina ovat rakenteet, valvontajärjestelyt sekä turvallisuustietoisuus ja toimintatavat. Osa-alueita valitessa ja muokatessa on otettu huomioon sekä kohdeorganisaation suurimmat tarpeet ja aukot korotetun tason tietoturvallisuutta tavoiteltaessa, että valtionhallinnon organisaatioihin liittyvät yleispiirteet. Esimerkiksi ympäröivää aluetta käsittelevä osio on otettu pois, sillä suurin osa valtion organisaatioista toimii kaupunkiympäristöissä rakennuksissa, joissa on muitakin toimijoita.

Rakenteet-osiossa käsitellään seinä-, ikkuna- ja ovirakenteita, lukituksia ja kassakaappien vaatimuksia. Nämä asiat on haluttu ottaa kohdeorganisaation taulukkoon mukaan, sillä ne ovat olennaisia, kun halutaan suojata tieto fyysisiltä, organisaation ulkopuolelta tulevilta varkausyrityksiltä, jotka koetaan nyt ajankohtaisiksi (Kohdeorganisaation turvallisuuspäällikkö 2016). Seinärakenteissa kiinnitetään huomiota vahvistuksiin ja rakenteiden äänieristävyyteen.

Tämä on tärkeää erityisesti jos organisaation sisäseinän ulkopuolella oleva tila ei kuulu samalle organisaatiolle. Ovien vaatimuksissa on tärkeää, että oviympäristöllä on sama vahvuus kuin ympäröivillä seinärakenteilla. Äänieristyksellä on tässäkin tärkeä merkitys. Ovet tulee vyöhykkeiden ulkorajalla varustaa turvalukituksella, ja vyöhykkeen rajalla tulee käyttää kulunvalvontaa. Ikkunoita ei tulisi pystyä avaamaan alakerroksissa, ja niissä tulisi olla suojakalvot tai vahvistettu lasi. Lisäksi ikkunoissa tulisi olla verhot tai sälekaihtimet. (VAHTI 2/2013, 37-39.)

Valvontajärjestelyt-osiossa käsitellään kulunvalvontaa, tunkeutumisenilmaisinjärjestelmiä, kameravalvontaa ja vartiointia. Valvontajärjestelyt koetaan kohdeorganisaatiossa ehdottoman tärkeiksi sekä organisaation ulkopuolelta, että sisäpuolelta tulevia riskejä hallitessa (Kohdeorganisaation turvallisuuspäällikkö 2016). Tiloissa tulee olla tallentava kameravalvonta sekä tunkeutumisenilmaisinjärjestelmä, joka valvoo ovia, aukkoja ja ikkunoita. Järjestelmiä tulee testata säännöllisin väliajoin. Kameravalvonnassa tulee ottaa huomioon, ettei kuvattaessa pääse näkymään salassa pidettävää tietoa. Laki yksityisyyden suojasta työelämässä määrää, että henkilöstöä tulee myös tiedottaa valvonnasta yt-käsittelyllä. Vartiointi täydentää teknisiä järjestelmiä. Vartioinnin vasteajan tulee olla sellainen, että tunkeutumisesta on suuri kiinnijäämisen riski. Vasteaika tulee testata. (VAHTI 2/2013, 41.)

Kolmas osio, eli turvallisuustietoisuus ja toimintatavat, käsittelee turvallisuusdokumentaatiota, henkilöstön koulutusta ja toimintaa salassa pidettäviä asioita käsiteltäessä. Nämä asiat on otettu mukaan, sillä ilman henkilöstön tietoisuutta ja organisaation turvallisuusorientoituneisuutta rakenteellisten ja teknisten toimenpiteiden vaikuttavauus heikkenee (Kohdeorganisaation turvallisuuspäällikkö 2016). Turvallisuusdokumentaatiolla tarkoitetaan esimerkiksi dokumentointia järjestelmien testauksesta. Henkilöstön koulutuksella mitataan heidän tietoisuuttaan siitä, miten salassa pidettäviä asioita tulisi käsitellä. (VAHTI 2/2013, 37,41.)

Taulukon joka kohdasta on mahdollisuus saada 0-2 pistettä. Jos vaatimus ei täyty, saa 0 pistettä, jos se täyttyy osin, saa yhden pisteen, ja jos se täyttyy täysin, saa täydet kaksi pistettä. Jokaisesta kolmesta osa-alueesta lasketaan keskiarvo. 1,5- 2 pistettä tarkoittaa matalaa riskitasoa, 1-1,5 pistettä keskimääräistä riskitasoa ja 0-1 pistettä korkeaa riskitasoa. (VAHTI 2/2013, 35.)

2.6 Nykytilanne

Kohdeorganisaatiolla on noin kolmekymmentä toimipistettä ympäri Suomen, ja enemmistö toimitiloista on VAHTI 2/2013 –ohjeen mukaisella perustasolla. Tämä tarkoittaa, että näissä toimitiloissa ei saisi käsitellä kuin satunnaisesti korotetun tason tietoja. Viraston toiminnan

luonteesta johtuen tällaisia tietoja käsitellään kuitenkin säännöllisesti. (Kohdeorganisaatio 2016.)

Tein toisen opintoihini kuuluvan työharjoittelun samaan virastoon, mihin tämäkin opinnäytetyö kohdistuu. Harjoittelun aikana tehtäviini kuului käydä toimipisteissä kartoittamassa niiden tilaturvallisuus VAHTI 2/2013 –ohjeen perusteella. Kävin tekemässä kartoitukset kahdeksassa eri toimipisteessä. Tarkasteltavia osa-alueita olivat tekemäni mukautetun taulukon perusteella rakenteet, valvontajärjestelyt sekä turvallisuustietoisuus ja toimintatavat. Kartoitusten perusteella viraston toimitilojen nykyisestä turvallisuustasosta sai melko laajan kuvan.

Kartoitettujen toimitilojen joukossa oli sekä isoja että pieniä toimistoja. Suurimmassa työskentelee parhaimmillaan noin kolmesataa henkeä, ja pienimmässä noin kymmenen. Vierailluista kahdeksasta toimipisteestä kaksi täyttää tällä hetkellä korotetun tason vaatimukset. Kartoitetut toimitilat sijaitsevat ympäri Suomen. (Kohdeorganisaatio 2016.) Seuraavaksi kerrotaan yleisimmistä ongelmista nykytilanteen turvallisuuteen liittyen.

Suurimmat kartoituksissa havaitut puutteet olivat toimipisteiden rakenteellisessa turvallisuudessa. Toimitilat sijaitsevat usein maatasossa, jolloin ikkunoiden tulisi olla vahvistettua lasia eikä niitä pitäisi pystyä avaamaan. Tämä ei kuitenkaan toteutunut missään toimipisteessä. Ovien, jotka johtavat toimitiloihin, tulisi olla vahvistettuja. Joissain toimipisteissä oli kuitenkin lasiovia tai tavallisia vahvistamattomia ovia. Sama koskee näiden ovien lukkoja. Lukkojen tulisi olla vahvennettuja, mutta joissakin toimipisteissä oli tavalliset käyttölukot.

Valvontajärjestelyissä oli myös jonkin verran puutteita toimipisteestä riippuen. Suurin puute, joka tuli useassa paikassa vastaan, oli tunkeutumisenilmaisinjärjestelmän sekä kameravalvontajärjestelmän puuttuminen kokonaan. Kahdessa toimipisteessä ei ollut myöskään kulunvalvontaa, vaan työpaikalle tultiin kovilla avaimilla, tai tiloihin pääsi jopa ilman avainta. Vartioinnin vasteaikaa ei testattu suurimmassa osassa toimipisteitä.

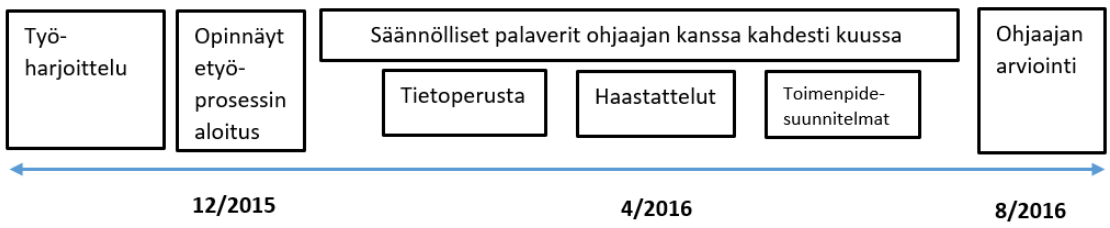
Turvallisuustietoisuudessa ja toimintatavoissa oli eroja toimipisteestä riippuen. Yleisin puute oli turvallisuusdokumentaation, eli esimerkiksi valvontajärjestelmien testauksen dokumentoinnin puuttuminen. Salassa pidettävistä asioista keskusteltaessa ei aina myöskään ymmärretty sulkea ovea, tai niistä puhuttiin jaetussa toimistohuoneessa niin että muillakin oli mahdollisuus kuulla. Salassa pidettäviä dokumentteja ei aina säilytetty kassakaapissa.

2.7 Yhteistyö kohdeorganisaation kanssa

Yhteistyöstä kohdeorganisaation kanssa sovittiin jo ennen opinnäytetyön aloittamista. Harjoittelussani suoritin toimitilakartoituksia, joten opinnäytetyön tekeminen aiheen parissa tuntui

luontevalta. Harjoittelu auttoi solmimaan hyviä kontakteja organisaation kanssa, joita hyödynnettiin koko opinnäytetyöprosessin ajan.

Opinnäytetyöni ohjaaja kohdeorganisaation puolelta oli mukana harjoittelun aikana tekemissäni toimitilakartoituksissa, joten kokemusta yhteistyöstä oli jo ennen opinnäytetyöprosessia. Ohjaajan kanssa sovittiin säännölliset tapaamiset, joiden aikana käytiin läpi työn edistymistä ja organisaation toiveita sen suhteen. Kohdeorganisaatiossa tapahtui henkilöstön ja toimitilojen osalta muutoksia, joista näissä tapaamisissa sai hyvää tietoa. Ohjaaja antoi myös muiden yhteyshenkilöiden nimiä, joilta sai sisäistä toimenpidesuunnitelmaa varten tietoja organisaation tilanteesta. Sisäiset haastattelut saatiin sovittua helposti. Aihe koettiin tärkeäksi, joten riskienhallintapäällikkö, tietoturvapäällikkö ja turvallisuuspäällikkö löysivät aikaa haastatteluille. Yhteistyöprosessi kohdeorganisaation kanssa on kuvattu kuviossa 1.



Kuvio 1: Yhteistyö organisaation kanssa

3 Opinnäytetyön toteutus

Tämä opinnäytetyö on toiminnallinen opinnäytetyö. Toiminnallinen opinnäytetyö on ammattikorkeakoulussa käytettävä vaihtoehto tutkimukselliselle opinnäytetyölle. Toiminnallisella opinnäytetyöllä tavoitellaan käytännön toiminnan ohjeistamista, opastamista, järjestämistä tai järkeistämistä ja se voi olla esimerkiksi ohje, ohjeistus, opastus tai tapahtuman järjestäminen (Vilkka & Airaksinen 2003, 9). Tähän työhön liittyy kaksi toimenpidesuunnitelmaa, jotka ovat omanlaisiaan ohjeistuksia, joten toiminnallinen lähestymistapa koettiin sopivaksi niiden toteuttamiseen. Vilkka ja Airaksinen (2003,10) toteavat myös, että toiminnallisen opinnäytetyön tulisi olla työelämälähtöinen, käytännönläheinen, tutkimuksellisella asenteella toteutettu ja riittävällä tasolla alan tietojen ja taitojen hallintaa osoittava. Tämä työ etenee yhteistyössä työelämän kanssa, ja aihetta tullaan lähestymään myös tutkimuksellisesta näkökulmasta.

Tämän opinnäytetyön tutkimusmenetelmät ovat kvalitatiivisia. Kvalitatiivisessa eli laadullisessa tutkimuksessa pyritään Hirsjärven, Remeksen ja Sajavaaran (2012, 161) mukaan tutkimaan kohdetta mahdollisimman kokonaisvaltaisesti. Siinä todellisuus nähdään moninaisena kokonaisuutena, jossa tapahtumat ovat kuitenkin toisistaan riippuvaisia.

Opinnäytetyössä luodut toimenpidesuunnitelmat, joista toinen kohdistuu kohdeorganisaatiolle ja toinen valtion virastoille, tuottavat jotakin uutta organisaatioiden hyödynnettäväksi. Hirsjärvi ym. (2012, 164) toteavat, että tyypillisesti kvalitatiivisessa tutkimuksessa pyrkimyksenä on paljastaa odottamattomia seikkoja, eli löytää jotain uutta mieluummin kuin todentaa olemassa olevia totuuksia. Niinpä laadullinen tutkimus ja siihen liittyvät tiedonkeruumenetelmät sopivat tähän opinnäytetyöhön.

Kvalitatiivisessa, eli laadullisessa tutkimuksessa suositaan sellaisia tiedonkeruumenetelmiä, joissa tutkittavien näkökulmat pääsevät esille, ja joissa kohdejoukko valitaan tarkoituksenmukaisesti eikä satunnaisotannalla (Hirsjärvi ym. 2012, 164). Tässä opinnäytetyössä käytettävät menetelmät, eli kirjallisuuskatsaus, haastattelut ja benchmarking ovat laadullisia menetelmiä. Näillä menetelmillä pyritään varmistamaan mahdollisimman kokonaisvaltaisen ja monipuolisen tiedon saanti.

3.1 Kirjallisuuskatsaus

Kirjallisuuskatsaus luo tälle opinnäytetyölle teoreettisen pohjan. Kirjallisuuskatsauksen avulla voidaan kehittää uutta teoriaa, arvioida olemassa olevaa teoriaa, rakentaa kokonaiskuvaa jostakin aihepiiristä, tunnistaa ongelmia ja tarkastella jonkin teorian historiallista kehitystä (Salminen 2011, 3). Tässä opinnäytetyössä kirjallisuuskatsauksella pyritään erityisesti kokonaiskuvan rakentamiseen organisaatioiden tietoturvallisuudesta etenkin toimitiloissa.

Tässä tapauksessa kirjallisuuskatsaus on laadultaan kuvaileva. Salmisen (2011, 6) mukaan kuvaileva kirjallisuuskatsaus on yleisin käytetty kirjallisuuskatsauksen muoto. Siinä ei ole tiukkoja sääntöjä, ja aineiston rajaamista ei rajoiteta. Tutkittavaa asiaa voidaan sen avulla kuvata laaja-alaisesti. Kuvaileva kirjallisuuskatsaus sopii käsiteltävään aiheeseen, sillä tietoturvallisuus tutkittavana asiana tarjoaa tietoa useista eri lähteistä. Kuvailevalla lähestymistavalla varmistutaan parhaiten siitä, että saatu tieto on monipuolista ja antaa hyvän kokonaiskuvan.

Kirjallisuuskatsauksella on tässä työssä rooli myös muiden tutkimusmenetelmien käytössä. Hirsjärven ym. (2012, 144) mukaan teoria ohjaa uuden tiedon etsinnässä ja samaan aikaan jäsentää kerättyä aineistoa. Tässä opinnäytetyössä haastattelujen ja benchmarkingin teemat syntyivät kirjallisuuskatsauksessa syntyneen teorian pohjalta. Haastatteluista ja benchmarkingista saatujen tulosten johtopäätöksiä myös verrattiin tähän teoriapohjaan. Kirjallisuuskatsauksessa on käytetty monipuolisia kirjallisuuslähteitä sekä erilaisia ohjeita ja kriteeristöjä, kuten VAHTI 2/2013 -ohjetta ja Katakrin kolmatta versiota. Säädösten näkökulmasta kirjallisuuskatsauksessa vaikuttaa eniten Valtioneuvoston asetus tietoturvallisuudesta valtionhallin-

nossa sekä laki viranomaisten toiminnasta julkisuudessa. Säädösympäristössä vaikuttavana lakina on näiden lisäksi esimerkiksi laki kansainvälisistä tietoturvavelvoitteista (L588/2004), jossa määritellään tiedon suojaamiseen liittyvät periaatteet kansainvälisissä sopimuksissa ja määräyksissä.

3.2 Haastattelu

Hirsjärvi ym. (2012, 205) toteavat, että haastattelun suurin etu on se, että aineiston keruuta voidaan säädellä tilanteen mukaan. Esimerkiksi aiheiden järjestystä voi säädellä, ja esittää lisäkysymyksiä. Yleisiä syitä haastattelun valinnalle ovatkin mahdollisuus syventää saatuja tietoja ja selventää saatavia vastauksia. Haastattelu valitaan usein myös, jos tiedetään aiheen tuottavan vastauksia monitahoisesti ja moniin suuntiin. (Hirsärvi ym. 2012, 205-207.)

Edellä mainituista syistä myös tässä opinnäytetyössä käytetään haastattelumenetelmää. Haastatteluilla on tarkoitus selvittää mitä tarpeita kohdeorganisaation sisällä on tietoturvallisuuden kehittämisen osalta, ja miten muissa organisaatioissa on saatu parannettua tietoturvatasoa. Aihe on sellainen, että siitä saa keskusteltaessa enemmän materiaalia kuin esimerkiksi kyselylomakkeella. Haastateltaessa esiin tulee uusia asioita, joita varten voi esittää uusia kysymyksiä. Asiat, jotka tulevat esiin etukäteen laadittujen kysymysten ulkopuolella saattavat olla jopa tärkeimpiä.

Haastattelutyyppejä on useita. Omaan tutkimukseeni sopii parhaiten teemahaastattelu. Teemahaastattelu on lomake- ja avoimen haastattelun välimuoto, jolle Hirsjärven ym. (2012, 208) mukaan on tyypillistä, että aihepiirit ovat selvillä mutta tarkat kysymykset ja niiden järjestys eivät. Teemahaastattelussa voidaan edetä paremmin haastateltavan ehdoilla, ja alan asiantuntijoilta saa paljon arvokasta tietoa, jota ei välttämättä tiukasti strukturoidulla kysymyspatteristolla saisi.

Haastattelut voidaan toteuttaa yksilöhaastatteluina, parihaastatteluina tai ryhmähaastatteluina. On huomattu, että ryhmähaastatteluissa haastateltavat keskustelevat usein luontevammin ja vapautuneemmin, mutta toisaalta myös yksilöhaastatteluista on saatu monia samankaltaisia tuloksia (Hirsjärvi ym. 2012, 210). Tätä opinnäytetyötä varten tehdyt haastattelut ovat yksilöhaastatteluja. Haastateltavat ovat oman alansa ammattilaisia ja aiheet käsittelevät työasioita. Voidaan olettaa, että aiheisiin ei liity erityisiä latauksia, ja siispä yksityishaastattelu on sopiva ympäristö niistä puhumiseen.

Tässä opinnäytetyössä haastateltavina olivat organisaation riskienhallintapäällikkö, tietoturvapäällikkö sekä turvallisuuspäällikkö. Haastatteluiden teemat muodostuivat kirjallisuuskatsauksen tietoperustasta. Teemoja olivat muun muassa tietoturva-asetuksen vaatimusten täyt-

tyminen kohdeorganisaatiossa, organisaation nykyinen suojaustaso sekä rakenteellinen turvallisuus, valvontajärjestelyt ja henkilöstön toimintatavat kohdeorganisaatiossa. Näiden teemojen avulla selvitettiin kohdeorganisaation nykytilannetta, jotta tiedetään mikä on lähtökohta, ennen kuin tilojen turvallisuutta aletaan korottaa. Teemoja ja tietoperustaa, jonka perusteella ne valikoituivat, on kuvattu taulukossa 1. Haastattelut nauhoitettiin, ja nauhoitusten perusteella rakennettiin keskeiset aihealueet, joiden alle vastaukset koottiin. Haastatteluiden tuloksista ja analysointimenetelmistä kerrotaan tuloksia käsittelevässä luvussa.

Sisäiset haastattelut		**Benchmarking**	
Teemat	**Pohja tietoperustasta**	**Teemat**	**Pohja tietoperustasta**
Lain vaatimusten täyttyminen tällä hetkellä	Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010	Tilaturvallisuuskriteeristöt ja niiden riittävyys	VAHTI 2/2013, KATAKRI 2015
Suojaustasot	Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010	Rakenteellinen turvallisuus	VAHTI 2/2013
Rakenteellinen turvallisuus	VAHTI 2/2013	Valvontajärjestelyt	VAHTI 2/2013
Valvontajärjestelyt	VAHTI 2/2013	Ihmisten toimintatavat	Kiinteistö- ja tilaturvallisuuden tasot 2014, Peltier 2013
Ihmisten toimintatavat	Kiinteistö- ja tilaturvallisuuden tasot 2014, Peltier 2013	Resurssien käyttö	Perdikaris 2014
Tavoitetun tason ylläpito	Peltier 2013, Gillies 2012	Riskien arviointi	KATAKRI 22015, Kiintiestö- ja tilaturvallisuuden tasot 2014
		Sidosryhmät	Porvari 2012
		Tavoitetun tason ylläpito	Peltier 2013, Gillies 2012

Taulukko 1: Teemat ja tietoperusta

3.3 Benchmarking

Benchmarkingissa eli esikuva-arvioinnissa verrataan Ojasalon, Moilasen ja Ritalahden (2014, 186) mukaan omaa tutkimuskohdetta toiseen kohteeseen, joka on jo tehnyt saman asian ja suoriutunut siitä hyvin. Siinä etsitään parhaita käytänteitä muista organisaatioista, ja pyritään muokkaamaan ne omaan toimintaan sopivaksi, eli tuotetaan jotain uutta. Tässä opinnäytetyössä benchmarkingin avulla pyritään tuomaan hyviä käytänteitä kohdeorganisaatioon sekä yleiseen toimenpidesuunnitelmaan sellaisilta organisaatioilta, joissa tietoturva-asioita on menestyksekkäästi onnistuttu korottamaan.

Benchmarkingista saadaan parhaiten hyöty irti suorittamalla hyvin suunniteltu vierailu kohdeorganisaatioon, jonka aikana käydään läpi etukäteen tarkkaan suunniteltuja kysymyksiä (Ojasalo ym. 2014, 186). Tätä opinnäytetyötä varten tehdyissä vierailuissa organisaatioiden tietoturvahenkilöitä haastateltiin teemahaastattelun keinoin. Haastattelurunkoon mietittiin tarkkaan kysymykset, joihin haluttiin ehdottomasti vastaukset, mutta teemahaastattelun hengessä haastateltavalle annettiin tilaa kertoa myös kysymyspatteriston ulkoisia asioita.

Tämän opinnäytetyön benchmarking –osuudessa haastateltiin kolmea henkilöä, jotka ovat olleet tekemisissä valtionhallinnon korotetun tason tilaturvallisuusprojektien kanssa. Benchmarking –haastatteluilla pyrittiin selvittämään muiden organisaatioiden kohtaamia onnistumisia ja haasteita. Haastattelujen teemoja, jotka muodostuivat tietoperustasta, olivat toimitilaturvallisuuskriteeristöt, rakenteellinen turvallisuus, valvontajärjestelyt sekä henkilöstön toimintatavat muissa organisaatioissa, sekä riskien arviointi osana tilojen tietoturvallisuuden kehittämistä. Lisäksi haluttiin selvittää, millaisia vaiheita muilla organisaatioilla on ollut tilojen korottamisessa korotetulle tasolle, ja millaisia haasteita niissä on ollut. Näillä teemoilla saatiin vastauksia, joiden perusteella rakennettiin askeleet toimenpidesuunnitelmiin. Teemat ja tietoperusta johon ne pohjautuivat, löytyvät taulukosta 1.

4 Tulokset

Haastatteluista ja benchmarkingista saatua tietoa alettiin analysoida teemoittelun keinoin. Teemoittelussa haastatteluaineistosta etsitään toisiaan yhdistäviä ja toistuvia teemoja. Teemojen alle kootaan haastatteluista ne kohdat, joissa kyseisistä teemoista puhutaan. Teemoittelu on yleinen analysointikeino teemahaastattelujen analysoinnissa. (Saaranen-Kauppinen & Puusniekka 2006.) Tämän opinnäytetyön haastattelut olivat teemahaastatteluja, joten teemoittelu tuntui luonnolliselta ja toimivalta tiedon analysointimenetelmältä.

4.1 Haastattelujen tulokset

Kohdeorganisaation sisäisissä haastatteluissa teemoiksi muodostuivat erityisesti organisaation vaatimustenmukaisuus tilaturvallisuuden osalta, organisaation nykyinen suojaustaso, rakenteelliset ja valvonnalliset turvajärjestelyt sekä ihmisten toimintatapoihin vaikuttaminen. Lisäksi keskusteltiin turvallisuustoimenpiteistä, joita tilaturvallisuuden korotetulle tasolle pääseminen vaatisi, sekä korotetun tason ylläpitoon liittyvistä toimenpiteistä. Haastateltavina olivat organisaation riskienhallintapäällikkö, turvallisuuspäällikkö ja tietoturvapäällikkö.

Haastatteluissa puhuttiin siitä, täyttyykö kohdeorganisaatiossa Valtioneuvoston asetuksessa tietoturvallisuudesta määritetyt tilaturvallisuutta koskevat vaatimukset. Yleinen mielipide jokaisella oli se, että puutteita löytyy vielä ja toimipisteet ovat eri tasoilla tämän suhteen. Se, kuinka merkittäviksi puutteet koettiin, vaihteli haastateltavien välillä. Riskienhallintapäällikkö oli sitä mieltä, että koska vaatimusten täyttymisestä ei ole turvallisuusdokumentaatiota, ei niiden voida katsoa täyttyneen. Turvallisuuspäällikön näkemyksen mukaan asetus täyttyy pääosin muutamia poikkeuksia lukuun ottamatta. Tietoturvapäällikön mielestä vaatimukset täyttyvät suurissa ja keskeisissä toimipisteissä, mutta ei pienemmissä.

Haastatteluissa keskusteltiin myös siitä, millä suojaustasolla kohdeorganisaation koetaan tällä hetkellä olevan. Tämänkin suhteen kaikki olivat sitä mieltä, että suuria vaihteluja on toimipistekohtaisesti. Riskienhallintapäällikkö arvelisi, että tilat ovat pääosin perustasolla, mutta niihin tarvitaan järjestelmällistä riskikartoitusta asian selvittämiseksi. Turvallisuuspäällikkökin arvioi tilojen olevan suurimmaksi osaksi perustasolla, ja korotetulla tasolla keskeisimpien toimitilojen suhteen. Tietoturvapäällikkö arveli tilojen jäävän jopa vähän perustason alapuolelle. Hänkin huomauttaa, että auditoinnit ovat kuitenkin kesken.

Jokainen haastateltava koki, että rakenteellisessa turvallisuudessa on jonkin verran puutteita, mutta painopisteet olivat erilaisissa asioissa. Riskienhallintapäällikön mukaan suurin puute on siinä, ettei tiedetä tarpeeksi nykyisistä rakenteista, koska niitä ei ole kartoitettu. Tämän takia on vaikea lähteä miettimään parannuksiakaan. Turvallisuuspäällikön mielestä jo suomalaiset rakennusvaatimukset luovat hyvän pohjan turvallisuudelle monissa toimipisteissä, mutta parannettavaa on vielä esimerkiksi ovien ja ikkunoiden suojauksessa. Tietoturvapäällikön mukaan korotetun tason tilaratkaisuja ei ole tarpeeksi, eikä III-tason tietoja voida näin ollen turvallisesti ja joustavasti käsitellä työpaikalla.

Valvontajärjestelyissä ongelmalliseksi koettiin se, että useissa toimipisteissä on eri virastoja ja asiakkaita, ja sen takia valvontajärjestelyissä on epäselvyyksiä. Tietoturvapäällikön mielestä kulunvalvonta on vaihtelevalla tasolla, ja se onkin tällä hetkellä kriittisin puute. Riskienhallintapäällikön mukaan toimitiloissa toimineet aiemmat virastot ovat tehneet päätökset valvontajärjestelmien hankkimisesta, ja heidän järjestelmät ovat siirtyneet kohdeorganisaatiolle

eivätkä ole välttämättä riittäviä. Turvallisuuspäällikkö on vartioinnin osalta samaa mieltä, vartiointisopimuksen on usein tehnyt jokin muu virasto, eikä siitä olla tarpeeksi hyvin selvillä. Hän kokee puutteeksi myös sen, että osa toimipisteistä on käytössä enää vähän aikaa, joten niiden valvontaan ei ole panostettu.

Ihmisten toimintatapoihin vaikuttamisesta keskusteltaessa kaikilla haastateltavilla oli selkeä näkemys siitä, että koulutusta turvallisuusasioista tarvitaan lisää ja sen tulisi olla järjestelmällisempää. Koulutusta pitäisi olla kaikkien mielestä säännöllisemmin ja sitä tulisi kohdistaa enemmän. Riskienhallintapäällikkö painotti lisäksi, että toimintakulttuurin pitäisi olla sellainen, että jokainen saa puuttua, jos huomaa turvallisuusasioita laiminlyötävän. Sekä turvallisuuspäällikkö että tietoturvapäällikkö ottivat puheeksi myös ohjeistukset. Molempien mielestä yleisten ohjeiden lisäksi pitäisi olla kohdennettuja ohjeita toimipisteille. Johdon merkitys henkilöstöön vaikuttamisessa oli kaikkien mielestä merkittävä. Johdon tulee antaa tuki ja enemmän resursseja kouluttamista varten, ja iskostaa turvallisuusajattelu osaksi päivittäisjohtamista.

Haastatteluissa kävi ilmi, että henkilöstöllä ja johdolla on suuri merkitys myös silloin, kun halutaan ylläpitää hyvää toimitilaturvallisuutta. Tietoturvapäällikön mukaan henkilöstön asenteeseen ja tietoisuuteen oikeista toimintatavoista tulee kiinnittää jatkuvasti huomioita ja niitä tulee pyrkiä kehittämään. Turvallisuuspäällikön mielestä johdon tulee sitoutua siihen, että henkilöstöä koulutetaan jatkuvasti näistä asioista.

4.2 Benchmarkingin tulokset

Benchmarkingissa haastateltiin kolmen sellaisen organisaation edustajia, joissa tietoturvallisuustasoa toimitiloissa on onnistuttu korottamaan. Ensimmäinen haastateltava oli nimettömänä pysyvä turvallisuuspäällikkö (Turvallisuuspäällikkö 1) eräästä valtionhallinnon organisaatiosta, jossa kartoitettiin toimitilojen nykytaso ja tehtiin toimenpidesuunnitelmat nykytason korottamisesta. Organisaatiolla on useita toimipisteitä ympäri Suomen niin toimistokäyttöön kuin erityistiloiksikin. Toinen haastateltava oli Netum Oy:n Arto Kangas, joka on ollut mukana useissa sekä valtionhallinnon että yksityisen sektorin projekteissa, joissa toimitilojen tietoturvallisuutta on pyritty korottamaan. Kolmas haastateltava oli Senaatti-kiinteistöjen turvallisuuspäällikkö Tuomas Lehmusmetsä. Hän on ollut johtamassa useita organisaationsa toimitilojen tietoturvallisuuden korottamiseen tähtääviä projekteja. Haastateltavilta kysyttiin muun muassa heidän käyttämistään työkaluista ja kriteeristöistä, yleisimmistä puutteista ja haasteista, resursseista, ja koko prosessiin liittyvistä vaiheista.

Kaikki haastateltavat ovat käyttäneet toimitilaprojekteissaan VAHTI 2/2013 –ohjetta. Ohje on koettu pääosin tarpeeksi kattavaksi. Turvallisuuspäällikkö 1:en mukaan VAHTI-ohje on pääosin tarpeeksi kattava, mutta sen lisäksi toimitilaprojektissa on käytetty omia lisäyksiä. Kankaan

mukaan VAHTI-ohjeessa puhutaan välillä liian yleismaailmallisesti etenkin riskienarviointiin liittyvistä asioista, mutta se on pääosin toimiva. Lehmusmetsä kokee kyseisen ohjeen hyväksi suunnitteluohjeeksi, jos keskitytään vain tietojen suojaamiseen. Toteuttamisvaiheessa ohje ei ole hänen mielestään tarpeeksi yksityiskohtainen.

Toimitilojen rakenteellisen turvallisuuden parantamisesta keskusteltaessa sekä Kangas että Lehmusmetsä osasivat nimetä asioita, jotka toistuvasti ovat olleet ongelmana useissa toimipisteissä. Kankaan mukaan haasteena on muistaa huomioida kokonaiskuva rakenteellista turvallisuutta parannettaessa. Esimerkiksi jos seiniä on päätetty vahvistaa, on saatettu kuitenkin unohtaa kokonaan äänieristys. Lehmusmetsän mukaan rakenteellisen turvallisuuden ongelmat ovat usein lähtöisin toimitilan sijainnista. Jos se sijaitsee alimmassa kerroksessa ja sisälle on mahdollista päästä suoraan kadulta, on rakenteellinen turvallisuus jo lähtökohtaisesti heikommassa tilassa tietojen suojaamisen näkökulmasta. Lisäksi oviympäristöjen ratkaisut saattavat usein kustannuksiltaan nousta liian korkeiksi, ja äänieristyksen kanssa on ongelmia, jos tilat jaetaan muiden virastojen kanssa.

Valvontajärjestelyjen suhteen kaikki haastateltavat olivat huomanneet toistuvia ongelmia. Turvallisuuspäällikkö 1:en tekemän kartoituksen mukaan sekä kulunvalvonta että rikosilmoitinlaitteisto puuttui noin puolista hänen organisaationsa toimipisteistä. Kankaan mukaan valvontajärjestelyissä on usein haluttu säästää niin, että vaikka hienoja järjestelmiä on otettu käyttöön, on joitakin alueita jätetty valvomatta, ja näin ollen jätetty mahdollisuus tiloihin tunkeutumiseen. Lehmusmetsän mukaan valvontajärjestelmien sopimusten hallinnassa on haasteita, sillä usean viraston toimipisteissä sopimusten alkuperistä ei ole aina tietoa.

Henkilöstön toimintatavat toimitilaturvallisuuteen liittyen ovat turvallisuuspäällikkö 1:en mielestä hänen organisaatiossaan kunnossa. Organisaation tulosalueiden tulostavoiteasiakirjoihin on kuvattu, miten tulosalueilla on vastuu henkilöstön perehdytyksestä, tietoisuuden lisäämisestä ja ohjeistuksesta tietoturvallisuuden suhteen, ja kaikkiin toimipisteisiin on nimetty tietoturvavastaava, joka vie aktiivisesti näitä asioita eteenpäin. Kangas on huomannut, että ihmisten toimintatavoissa on ongelmia. Hänen mukaansa ihminen pyrkii tekemään asiat mahdollisimman helpolla tavalla, minkä takia tietoturva-asioita usein saatetaan laiminlyödä. Ohjeistuksilla ja koulutuksilla tähän voidaan kuitenkin vaikuttaa, ja avainasemassa on koko organisaation sitouttaminen esimerkiksi sopimusten avulla. Lehmusmetsän mukaan ihmisten toimintatavat ovat suurin tekijä toimitilojen tietoturvallisuudessa. Turvallisuuskäytännöt pysyvät kuitenkin harvoin pitkään ihmisten mielissä, joten niitä tulee käydä jatkuvasti läpi.

Kaikkien haastateltavien mukaan prosessi, jonka tavoitteena on korottaa tilojen tietoturvallisuutta, lähtee liikkeelle luokittelupäätöksestä. Kankaan mukaan organisaation tulee ymmär-

tää velvollisuutensa luottamuksellisen tiedon käsittelyssä ennen prosessin jatkamista. Luokittelupäätöksen jälkeen turvallisuuspäällikkö 1:en organisaatiossa tehtiin kartoitus kahdeksaan tarpeeksi heterogeeniseen toimipisteeseen, joka sisälsi tilojen katselmoinnin ja haastattelut. Tulosten perusteella laadittiin kirjallinen kysely kaikkiin toimipisteisiin, johon noin 70 prosenttia vastasi. Näiden vastausten perusteella tehtiin toimenpidesuunnitelmat kriittisten poikkeamien osalta, ja loput puutteet kirjattiin toimitilastrategiaan. Kankaan mukaan tiloissa on tarpeen suorittaa myös jälkitarkastuksia pitkälläkin aikavälillä, jos vaadittavat muutokset ovat suuria.

Lehmusmetsän mukaan prosessissa tulee ottaa koko ajan vahvasti huomioon riskien arviointi ja tilannekuva. Tulee huomioida toimitilojen fyysinen ympäristö, organisaation oman toiminnan mahdolliset muutokset, sekä muutokset toimintaympäristössä ja vastuuverkostoissa. Tilannekuvan tulee olla erityisesti johdolla, sillä heillä on loppukädessä vastuu. Jos näitä ei oteta huomioon, ei toimenpiteitä osata välttämättä kohdistaa tärkeimpiin paikkoihin. Riskiarviota painottaa myös Kangas, jonka mukaan organisaation täytyy itse oma-aloitteisesti tietää ja selvittää tarpeensa ennen kuin muutoksia toimitiloihin tehdään.

Prosessissa alusta loppuun mukana olevia osapuolia tulee kaikkien haastateltavien mielestä olla ainakin sekä hallinnollista että teknistä tietoturvallisuutta osaavat tahot sekä toteutuksesta vastaava alihankkija. Lisäksi Kangas ja Lehmusmetsä painottavat, että tiloissa jokapäiväisesti työskentelevien näkökulma tulisi myös kuulla. Esiin nostettiin myös kiinteistöstä vastaavan rooli, ja Kankaan mielestä johdon tulisi myös olla mukana prosessissa.

Sekä Turvallisuuspäällikkö 1 että Kangas olivat sitä mieltä, että eniten rahallisia resursseja menee rakenteellisiin muutoksiin. Myös Lehmusmetsän mukaan nämä ovat suurimpia kertakustannuksia, mutta hän huomautti, että pidemmällä aikavälillä valvontajärjestelyt voivat olla kalliimpia. Sekä Lehmusmetsän että Kankaan mukaan henkilöstöön vaikuttaminen on halvinta, vaikka siitä saattaakin syntyä pidemmällä aikavälillä hieman kustannuksia. Lehmusmetsän kustannuslaskentaan käytettäviä periaatteita käydään toimenpidesuunnitelmassa tarkemmin läpi.

Kun halutulle tietoturvallisuuden tasolle toimitiloissa ollaan päästy, tulee tasolla myös pysyä. Turvallisuuspäällikkö 1 ja Kangas pitävät hyvänä keinona ylläpidon liittämistä osaksi organisaation turvallisuuden vuosikelloa. Lehmusmetsän mukaan toimitilan tilannetta tulee tarkastella vuosittain juurikin tilannekuvanäkökulmasta. Pitää tarkastella, onko tilanne muuttunut, ja pystytäänkö nykyisillä keinoin enää suojaamaan tietoa siinä tilanteessa. Kaikkien mielestä henkilöstön tietoisuudella on tavoitetun tason ylläpidossa suuri merkitys, ja sen kehittämisen tulee olla jatkuvaa.

4.3 Johtopäätöksiä

Haastattelujen ja benchmarkingin tuloksia analysoimalla syntyi johtopäätöksiä, joiden perusteella toimenpidesuunnitelmat rakennettiin. Johtopäätöksiin vaikuttivat tutkimusmenetelmillä saatu tieto sekä tietoperustasta muodostuneet asiat.

Yksi keskeisempiä johtopäätöksiä on riskiarvioinnin tärkeys. Sisäisissä haastatteluissa kävi ilmi, että kohdeorganisaatiossa on hyvin eritasoisia toimitiloja eikä kaikkien turvallisuusjärjestelyistä olla edes selvillä. Uusia turvallisuustoimenpiteitä ei voida määrittää, ennen kuin tiedetään mitkä ovat nykyiset tarpeet. Tätä tulosta tukee myös aiemmin mainittu Ihamäen ym. (2014, 7) huomio, jonka mukaan on tehtävä uhka-arvio ennen varsinaisia toimenpiteitä. Benchmarkingissa ilmeni, että riskiarvioinnin lisäksi tulee huomioida tilannekuva kokonaisuudessaan. Turvallisuustoimenpiteet tulee suhteuttaa siihen, millainen on sekä fyysinen ympäristö että toimintaympäristö, ja kriteeristöjä on sovellettava näitä vasten.

Toinen tärkeä päätelmä on henkilöstön toimintatapoihin vaikuttamisen tärkeys, kun tavoitellaan tilaturvallisuuden korotettua tasoa. Sekä sisäisten haastattelujen että benchmarkingin tulosten perusteella henkilöstön toimintatavat ovat tärkein tekijä, vaikka rakenteiden ja valvontajärjestelyidenkin perustan tulee olla kunnossa. VAHTI 2/2013 –ohjeessa ei oteta paljon kantaa henkilöstön toimintaan, vaan keskitytään enimmäkseen fyysiseen suojaukseen. Muusta tietoperustasta löytyy kuitenkin henkilöstön merkitystä puoltavia väitteitä, esimerkiksi Ihamäen ym. (2014, 9) mukaan henkilöstö tulee perehdyttää turvallisuusjärjestelmien käyttöön ja Peltier (2013, 127-129) luettelee mahdollisuuksiksi esimerkiksi tietoiskut, koulutukset ja ohjeistukset. Niin kuin haastateltavatkin totesivat, muista turvallisuusjärjestelyistä ei ole hyötyä, jos henkilöstö ei toimi ohjeiden mukaan.

Benchmarking –haastatteluissa kävi ilmi, että dokumentoinnin merkitys on suuri, kun pyritään korottamaan tilojen tietoturvallisuutta. Tietoturvallisuuden opettaminen henkilöstölle tulisi olla kirjattuna osaksi päivittäisjohtamista, ja esimerkiksi vuosikelloon merkitsemällä se tulee myös osaksi saavutetun tason ylläpitoa. Toimenpidesuunnitelmassa ei siis pidä unohtaa hallinnollisia asioita, sillä niillä organisaatio saadaan sitoutettua jatkuvaan parantamiseen. Jatkuvaa parantamista painottaa myös aiemmin mainittu Gillies (2012, 147), jonka mukaan sekä fyysistä turvallisuutta että siihen liittyviä arviointimenetelmiä tulisi arvioida säännöllisesti uudelleen.

Kohdeorganisaation haastateltavat henkilöt työskentelevät samassa organisaatiossa ja osittain samanlaisilla tehtäväkentillä, mutta heillä oli kuitenkin näkemyseroja organisaation nykytilasta. Tähän vaikuttaa varmasti haastatteluissakin mainittu toimipisteiden turvallisuustasojen vaihtelevuus sekä lähtötason epäselvyys, kun riskejä ei ole laajamittaisesti kartoitettu. Toi-

menpidesuunnitelmaa ajatellen olisi kuitenkin tärkeää, että vastuutahojen yhteistyö ja tiedonkulku sujuisi ongelmitta, jotta ratkaisuja tehdessä linjaukset eivät ole ristiriidassa keskenään. Linjauksista ja niiden hyväksymisestä on loppujen lopuksi vastuussa organisaation johto, ja sen täytyykin olla alusta asti sitoutunut. Porvarin (2012, 147) mukaan johdon sitoutuminen lisää henkilöstön motivaatiota sitoutua tietoturvallisuuden parantamiseen. Toimenpidesuunnitelmassa tulee siis ottaa kantaa siihen, mitkä ovat parhaat käytännöt niin johdon kuin henkilöstönkin sisäisen yhteistyön kannalta.

Eräs keskeinen asia, mikä sekä sisäisten haastattelujen, benchmarkingin että asiaan muuten perehtymisen perusteella voidaan laskea johtopäätökseksi, on VAHTI 2/2013 –ohjeen osittainen riittämättömyys, kun pyritään korottamaan tietoturvatasoa organisaatiossa. Osa haastateltavista sanoi, että se on riittävä puutteiden kartoittamiseen, ja hyvä suunnitteluvaiheen ohjeena, ja sitä se onkin. Mutta kun päästään toteutusvaiheeseen, ohjeen ongelmia alkaa nousta esiin. Siinä annetaan tarkkoja kriteerejä siitä, millaisia rakenteiden ja järjestelmien tulee olla, mutta jos niitä kaikkia lähtisi toteuttamaan, kustannukset nousisivat vaikka parasta hyötyä ei saataisi mahdollisesti kuitenkaan irti. Ohjeessa on kuitenkin pyritty tekemään selväksi, että kaikkea ei pidä sokeasti noudattaa, ja riskiarviokin on siellä mainittu. Riskiarviointia ei ole kuitenkaan avattu enempää, joten sen arvo jää melko pieneksi. Jotta tilojen tietoturvatasoa pystytään korottamaan kustannustehokkaasti ja organisaatiota parhaiten tukevalla tavalla, tulisi riskien arvioinnilla ja tilannekuvalla olla suuri merkitys. Kun ne ovat oikeasti hallussa, voidaan resursseja ja sitä myötä suojaustoimenpiteitä sijoittaa oikeisiin paikkoihin. Toimenpidesuunnitelmassa tulee siis ottaa huomioon, että jokainen toimipiste on oma kokonaisuutensa, ja vaikka VAHTI 2/2013 –ohje toimiikin kehyksenä, suojaustoimenpiteitä pitää lähteä toteuttamaan yksilöllisten tarpeiden perusteella.

5 Toimenpidesuunnitelmat

Opinnäytetyön tuotoksina syntyi kaksi toimenpidesuunnitelmaa siitä, miten organisaation toimitilojen tietoturvallisuus nostetaan korotetulle tasolle. Toinen toimenpidesuunnitelma laadittiin kohdeorganisaatiolle, ja se jää salaiseksi, kun taas toinen on yleisesti valtionhallinnon organisaatioiden hyödynnettävissä. Toimenpidesuunnitelmien runko rakennettiin suurilta osin benchmarking-haastatteluista ja tietoperustasta muodostuneiden tulosten ja johtopäätösten perusteella. Kohdeorganisaation salaiseksi jäävän toimenpidesuunnitelman sisältöön vaikutti organisaation sisäiset haastattelut. Seuraavaksi käydään kohta kohdalta läpi, miksi jokainen kohta valittiin toimenpidesuunnitelmaan. Julkinen toimenpidesuunnitelma löytyy liitteestä 2. Jotta myös salaiseksi jäävästä toimenpidesuunnitelmasta saisi käsityksen, on seuraavissa luvuissa kerrottu myös lyhyesti, miten toimenpidesuunnitelman vaiheet etenivät kohdeorganisaatiossa.

5.1 Luokittelupäätös

Toimitilojen tietoturvallisuuden korottaminen lähtee liikkeelle tietojen luokittelupäätöksestä. Tietoturva-asetus (681/2010) edellyttää, että kaikkien valtionhallinnon organisaatioiden on pitänyt päästä tietoturvallisuuden perustasolle 30.9.2013 mennessä. Siitä, kun organisaatio on tehnyt luokittelupäätöksen, on vielä viisi vuotta aikaa päästä tietoturvallisuuden korotetulle tasolle (681/2010, 23§). Luokittelupäätöksen ajankohta siis määrittää aikataulun takarajan toimitilojen nostamiseksi perustasolta korotetulle tasolle.

Benchmarking-haastatteluissa todettiin, että luokittelupäätös on toimenpidesuunnitelman alku. Koska tietoturva-asetus sitä edellyttää, se ei ole organisaatiolle vapaaehtoinen asia. (Kangas 2016.) Tämän ilmi tuomista organisaation johtoportaalle voi siis suositella, sillä lain edellyttämälle prosessille voi kiinnostusta ja resursseja tulla helpommin kuin suosituspohjaiselle hankkeelle.

Kohdeorganisaatiossa luokittelupäätös tehtiin vuonna 2014. Tietoturvallisuuden perustaso on saavutettu vuoden 2015 lopussa. Korotetun tason saavuttamisen takaraja on 2019. Organisaatiossa on käynnissä kokonaisturvallisuuden kehittämishanke, johon nämä asiat kuuluvat, ja riskienhallintapäällikkö on hankkeen omistaja. (Kohdeorganisaation intra 2016.)

5.2 Sidosryhmien tunnistaminen ja sitouttaminen

Jotta prosessia toteutettaisiin alusta loppuun sitoutuneesti, täytyy organisaation tunnistaa sen avainhenkilöt jo alkuvaiheessa (Kangas 2016). Johtopäätöksissä kävi ilmi, että dokumentoinnilla on tärkeä merkitys organisaation sitouttamisessa, joten avainhenkilöt on syytä merkitä ylös. Toimenpidesuunnitelmaan henkilöt on nimetty suunnitteluvaiheeseen, toteutusvaiheeseen sekä ylläpitovaiheeseen. Vaikka kaikki eivät olisi aivan alusta asti mukana, varmistetaan prosessin eteneminen nimeämällä heidät jo alkuvaiheessa.

Organisaation tietoturvallisuudesta tai riskienhallinnasta vastaava taho on yleensä vahvana tahona mukana koko prosessin ajan, ja usein myös sen käynnistäjä ja omistaja. Johtoryhmän tulee olla mukana niin, että heiltä saadaan hyväksyntä prosessille, ja heitä informoidaan säännöllisesti. Lisäksi tarvitaan tiloissa työskenteleviä henkilöstön edustajia, joilta saadaan tietoa siitä, millaista niissä työskentely käytännössä on. (Lehmusmetsä 2016.) Muita prosessissa mukana olevia henkilöitä ovat esimerkiksi kiinteistöpuolen edustaja, alihankkijat rakennuspuolelta ja teknisten järjestelmien osalta sekä ulkoiset auditoijat tilojen auditointeja varten (Erään valtionhallinnon organisaation turvallisuuspäällikkö 2016).

Kohdeorganisaatiossa turvallisuuden kehittäminen kuuluu riskienhallintapäällikön vastuulle. Kiinteistöpäällikkö on aina keskeinen taho kohdeorganisaation toimitilaprojekteissa, niin tässäkin tapauksessa. Tilojen nykytilan kartoituksessa on ollut mukana turvallisuuspäällikkö. (Kohdeorganisaatio 2016.) Kohdeorganisaation toimenpidesuunnitelmaan nimettiin näiden henkilöiden lisäksi vastuullisiksi henkilöiksi ulkoinen auditoija, johtoryhmä hyväksyjän roolissa sekä alustavasti kiinteistön omistajan edustaja ja alihankkijat rakennus- ja valvontapuolelta.

5.3 Nykytilan kartoitus

Ennen kuin voidaan määritellä keinoja, joilla toimitilat saadaan tietoturvallisuuden korotetulle tasolle, täytyy olla selvillä niiden nykyisestä tilanteesta (Kohdeorganisaation riskienhallintapäällikkö 2016). Valtionhallinnossa on monenlaisia organisaatioita, joten tässä toimenpidesuunnitelmassa käytetty menetelmä nykytilan kartoitukseen on vain yksi monista vaihtoehdoista. Jokainen organisaatio joutuu tekemään sen vähän eri tavalla ominaispiirteistä, kuten koosta riippuen, mutta tärkeintä on saada käsitys suurimmista puutteista jokaisella osa-alueella. Haastateltujen Lehmusmetsän ja Kankaan mukaan (2016) tilojen katselmoinnin lisäksi täytyy haastatella henkilöstöä, sillä kaikki asiat eivät ole nähtävissä tiloissa. Toimenpidesuunnitelmaa ajatellen organisaatioissa, joissa on useita toimipisteitä, hyvä vaihtoehto on katselmoida riittävän monipuolinen otanta toimitiloja, ja samalla haastatella niiden työntekijöitä.

Kohdeorganisaatiossa kartoitettiin kahdeksan erilaisen toimipisteen rakenteisiin ja valvontajärjestelyihin liittyvät asiat VAHTI 2/2013 -ohjeeseen pohjautuen, jonka lisäksi selvitettiin henkilöstöltä kyselemällä ihmisten toimintatapoihin liittyviä asioita (Kohdeorganisaation turvallisuuspäällikkö 2016). Kartoitusten tulokset koottiin toimenpidesuunnitelman mukaisesti, ja ne menevät johtoryhmän tarkasteltaviksi.

5.4 Riskiarvio ja tilannekuva

VAHTI 2/2013 -ohjeen vaatimustaulukkoa apuna käyttämällä kartoituksessa saadaan selville jokaisen osa-alueen riskitaso. Johtopäätöksissä ilmeni, että tämän lisäksi tulee kuitenkin tehdä perusteellinen riskiarvio ja verrata sitä tilannekuvaan. VAHTI-ohjeen taulukko ei anna yksinään tarpeeksi tietoa siitä, mitä toimenpiteitä on järkevä toteuttaa. Riskiarvioon päätettiin ottaa työkaluksi riskien todennäköisyyksien ja seurauksien vaikuttavuuden arviointi.

Riskien todennäköisyyttä arvioitaessa on otettava huomioon toimitilojen ympäristö sekä organisaation toiminnan luonne. On huomioitava esimerkiksi, sijaitseeko toimitila kaupunkiympäristössä, jossa on seinänaapureita vai onko se omassa rakennuksessaan rauhallisella alueella. Lisäksi organisaation toiminnan luonne määrittelee usein, millaiset riskit ovat todennäköisimpiä (VAHTI 2/2013, 45). Joissain suurin riski voi olla omaisuusrikollisuus, kun taas toisissa rikollisella toiminnalla pyritään pääsemään organisaation tietoihin käsiksi.

Riskiarviossa tulisi ottaa huomioon myös organisaation tilannekuva (Lehmusmetsä 2016). Tässä opinnäytetyössä sillä tarkoitetaan organisaatioon vaikuttavia tekijöitä, jotka määrittävät sen nykytilaa ja tulevaisuutta. Tilannekuvaan vaikuttavat tekijät voivat olla organisaation sisäisiä tai ulkopuolelta vaikuttavia asioita. Sisäisiä tekijöitä voivat olla esimerkiksi organisaation muutto toisiin toimitiloihin, suuret rekrytoinnit tai toiminnan luonteen muuttuminen ja ulkoisia esimerkiksi yleinen taloustilanne tai muutokset alihankintaketjuissa (Lehmusmetsä 2016).

Kohdeorganisaation kohdalla kaikista kahdeksasta kartoitetusta toimipisteestä tehtiin toimenpidesuunnitelman mukainen yhteenveto, jonka perusteella riskien vakavuus ja todennäköisyys arvioitiin siihen soveltuvalla, toimenpidesuunnitelmasta löytyvällä työkalulla. Tulosten perusteella riskit laitettiin järjestykseen. Lista kuitenkin muuttui, sillä tilannekuva huomioon ottaessa jotkin riskeistä päätettiin hyväksyä ilman toimenpiteitä ja osa koettiin merkittävämmiksi toiminnan luonne huomioitaessa.

5.5 Kustannusarvio

Toimenpidesuunnitelmassa päätetään riskiarvion perusteella, mitä muutoksia tullaan tekemään, jotta toimitilojen tietoturvallisuutta saadaan korotettua. Ennen kuin ne voidaan toteuttaa, muodostui suunnitelmaan kuitenkin vielä yksi välivaihe, eli kustannusarvio. Kustannukset tulevat olemaan hyvin erilaisia riippuen organisaatiosta ja sen tarpeista. Ne voidaan jakaa elinkaarikustannuksiin sekä kertainvestointeihin. Elinkaarikustannuksissa jokin hankinta aiheuttaa säännöllisiä, pitkäaikaisia kustannuksia, kun taas kertainvestoinneissa kustannukset tulevat heti kerralla (Lehmusmetsä 2016).

Haastatteluissa kaikkien mielestä rakenteelliset muutokset olivat kalleimpia kertainvestointeja. Esimerkiksi toimitilojen seinä- tai kattorakenteiden muokkaaminen voi tulla kalliiksi, mutta kun muutokset on tehty, ei kustannuksia enää synny. Rakenteiden elinkaarikustannukset ovat siis pieniä. Valvontajärjestelyiden kertainvestoinnit ovat usein halvempia kuin rakenteiden. Elinkaarikustannuksia syntyy kuitenkin säännöllisesti, sillä järjestelmät tarvitsevat ylläpitoa ja huoltoa, ja tämän lisäksi kustannuksia tulee esimerkiksi vartiointifirmojen palvelumaksuista. Ihmisten toimintatapoihin vaikuttamisesta tulee pienimmät kustannukset kertainvestointina. Koulutukseen liittyvät asiat vaativat kuitenkin jatkuvaa ylläpitoa, joten elinkaarikustannuksia syntyy. (Lehmusmetsä 2016.)

Valtionhallinnon kiinteistöistä vastaavien Senaatti-kiinteistöjen turvallisuuspäälliköllä on kustannusten laskemiseen periaatteet toimitilaprojekteissa, ja niitä voi soveltaa hyvin sekä kohdeorganisaatioon, että useisiin valtionhallinnon organisaatioihin. Toimitilaprojektissa kustannukset jakautuvat niin, että rakenteellisen turvallisuuden parantamiseen menee noin 3 prosenttia hankkeen kokonaiskustannuksista. Arviossa otetaan huomioon vain tietoturvallisuuden

parantamiseen tähtäävät rakennemuutokset, ei esimerkiksi paloturvallisuuteen tai lumikuormaan liittyviä asioita. Valvontajärjestelyt maksavat 10 euroa neliötä kohden kertainvestointina, mutta elinkaarikustannuksia syntyy palvelumaksuista ja huoltokustannuksista. Henkilöstön toimintatapoihin tarvitaan yksi ihminen 800 työntekijää kohden. Tällä tarkoitetaan kokopäiväistä henkilöä, jonka vastuulla on henkilöstön kouluttamiseen ja tietoisuuden ylläpitoon liittyvät asiat. Syntyvät kustannukset tarkoittavat siis tällaisen henkilön palkkakustannuksia. Joillakin organisaatioilla tällainen henkilö on jo valmiiksi, jos kyseiset asiat kuuluvat esimerkiksi riskienhallintapäällikön tehtäviin. Kustannuksiin vaikuttaa tämän lisäksi myös se, paljonko koulutuksiin osallistumalla menetetään työaikaa. Tämä vaihtelee organisaatioittain paljon. (Lehmusmetsä 2016.)

Kohdeorganisaation toimenpidesuunnitelmaan laskettiin kustannusarviot, ja niissä valvontajärjestelyt tulevat kalleimmiksi sekä elinkaarikustannuksina että kertainvestointeina. Joihinkin toimipisteisiin täytyy hankkia kokonaan uudet valvontajärjestelmät, ja kaikissa niiden ylläpitoon menee säännöllisesti rahaa. Toiseksi eniten kustannuksia syntyi rakenteellisista muutoksista, mutta nämä ovat kertaluontoisia. Äänieristys ja lukitukset olivat tärkeimmät rakenteelliset muutokset. Ihmisten toimintatapoihin vaikuttamisesta vastaa organisaation riskienhallintapäällikkö (Kohdeorganisaation turvallisuuspäällikkö 2016). Kustannuksia koulutuksista syntyi menetetystä työajasta, mutta ne ovat vuositasolla pieniä.

5.6 Toteutus

Kun kustannusarviot on tehty ja hyväksytetty johdolla, on toteutuksen vuoro. Tarvittavat toimenpiteet ovat jo ylätasolla tiedossa. Voidaan esimerkiksi tietää, että tarvitaan uusi kameravalvontajärjestelmä. Toimenpidesuunnitelmaan kuitenkin päätettiin avata toimenpiteet yksityiskohtaisemmalla tasolla, jotta niiden laajuus olisi varmasti selvillä. Näin ollen yksi toimenpide voisi olla esimerkiksi kameravalvontajärjestelmien kilpailutus. Kangas sanoi haastattelussaan (2016), että toimenpiteille on määriteltävä myös vastuuhenkilöt sekä aikataulut henkilöstön sitouttamiseksi.

Kohdeorganisaation edustajia haastatellessa (2016) selvisi, että kaikilla oli hieman eri käsitys organisaation nykytilasta. Johtopäätöksissä todettiin, että toimenpidesuunnitelmissa tulee varmistaa, että kaikilla on sama näkemys tehtävistä toimenpiteistä. Toimenpidesuunnitelmaan onkin merkitty, että projektin edetessä tulee olla säännöllisiä palavereita, joissa tehtyjä ja edessä olevia toimenpiteitä ja ilmenneitä haasteita käydään yhdessä läpi. Palavereille on hyvä lyödä aikataulu lukkoon samalla kun toteutusvaiheessa määritellään toimenpiteet. Organisaation johtoa on säännöllisesti tiedotettava projektin etenemisestä (Kangas 2016).

Kohdeorganisaation toimenpidesuunnitelman toteutusvaihe on toteutettu siltä kannalta, että kustannusarvio oltaisiin hyväksytty johtoryhmässä. Jos siihen kuitenkin tulee muutoksia, täytyy toimenpidesuunnitelmaakin muokata. Toimenpiteissä korostuvat valvontajärjestelmiin ja henkilöstön kouluttamiseen liittyvät asiat. Rakenteellisen turvallisuuden osalta muutoksia on vähemmän. Toimenpideluetteloon määriteltiin säännölliset palaverit kahden viikon välein, joissa käydään läpi etenemistä sekä haasteita organisaation sisäisten hankkeeseen osallistujien kesken. Tämän lisäksi lisättiin kuukausittainen palaveri, johon osallistuvat myös alihankkijat sekä kiinteistön omistaja. Näistä palavereista tiedotetaan johtoryhmälle. Näillä keinoin pyritään varmistamaan tehokas tiedonkulku ja yhteisissä tavoitteissa pysyminen.

5.7 Auditointi

Kun määritellyt toimenpiteet on tehty tavoitellulle tasolle pääsemiseksi, täytyy tarkistaa, että tavoite on oikeasti täyttynyt kaikilta osin. Tätä varten tehdään jälkitarkastus. Jälkitarkastukseen kannattaa hankkia ulkoinen auditoija, joka tarkistaa tilat uusin silmin. (Kangas 2016.) Toimenpidesuunnitelmaa laadittaessa kuitenkin huomattiin, että ulkoinen auditoija pystyy keskittymään lähinnä fyysiseen turvallisuuteen, eikä henkilöstön toimintatapoihin. Henkilöstön käyttäytymisen ja heidän turvallisuustietoisuutensa mittaamiseen täytyi keksiä toisia tapoja. Turvallisuustietoutta voi testata esimerkiksi verkkokoulutuksiin liittyvillä verkkotenteillä. Auditoinnin tuloksia tulee peilata riskiarvioon (Lehmusmetsä 2016).

Kohdeorganisaatiossa auditointi tullaan toteuttamaan ulkoisen auditoijan kautta. Tämä on merkitty osaksi toimenpideluetteloa. Henkilöstön toimintatapojen mittaaminen kirjataan vuosikelloon. Organisaatiossa pyritään ottamaan käyttöön säännöllinen verkkokoulutus, jossa testattaisiin osallistujien osaamista myös tenttien muodossa.

5.8 Ylläpito

Kun tavoite on hyväksytysti saavutettu, ja ollaan päästy tietoturvallisuuden korotetulle tasolle toimitiloissa, keskitytään jatkossa tavoitetun tason ylläpitoon. Ylläpidolle tulee määritellä vastuuhenkilö, ja siihen kuuluvat tehtävät tulee kirjata osaksi organisaation riskienhallinnan tai tietoturvallisuuden vuosikelloa (Erään valtionhallinnon organisaation turvallisuuspäällikkö 2016). Kaikkein aktiivisinta ylläpitoa vaatii ihmisten toimintatapoihin vaikuttaminen. Johtopäätöksissä tämä nousi tärkeimmäksi toimitilaturvallisuuden osa-alueeksi, ja siinä tulee ottaa huomioon sekä ohjeet, koulutukset että tietoiskut. Ohjeiden ajantasaisuus tulee tarkistaa vähintään vuosittain, ja lisäksi jos organisaatiossa tai tilannekuvassa tapahtuu merkittäviä muutoksia (Lehmusmetsä 2016). Koulutus tilaturvallisuuteen liittyen kuuluu jokaisen uuden työntekijän perehdytykseen, ja lisäksi pakollisia koulutuksia tulisi olla vähintään vuosittain. Kohdeorganisaation riskienhallintapäällikön (2016) mukaan rakenteellinen turvallisuus tulee kartoittaa joka toinen vuosi ja valvontajärjestelyt vuosittain. Jos toiminnassa tai ympäristössä

tapahtuu merkittäviä muutoksia, niin useammin. Ylläpidossakin on oleellista tilannekuvan säilyttäminen, ja sen muutoksiin reagoiminen vaadittaessa (Lehmusmetsä 2016).

Kohdeorganisaatiossa riskienhallintapäällikkö vastaa prosessin ylläpidosta. Vuosikelloon kirjataan vuosittaiset tilaturvallisuuskoulutukset sekä kahden vuoden välein rakenteellisen turvallisuuden arviointi. Perehdytyssuunnitelmaan on kirjattu turvallisuuskoulutus omaksi osakseen, ja jatkossa siinä käsitellään myös tilaturvallisuuteen liittyviä asioita.

6 Pohdinta

Tämän opinnäytetyön tavoitteena oli luoda toimivat ja selkeät toimenpidesuunnitelmat siitä, miten sekä kohdeorganisaatiossa, että valtionhallinnossa yleisesti päästään tietoturvallisuuden korotetulle tasolle toimitiloissa. Opinnäytetyön tavoitteena oli myös selkeästi kuvata sitä työstämisprosessia, jolla näitä toimenpidesuunnitelmia kohti edettiin. Kohdeorganisaatiossa ohjaajanani toimineen henkilön arvio opinnäytetyöstä löytyy liitteestä 3.

Tuloksena syntynyt valtionhallintoon tarkoitettu toimenpidesuunnitelma onnistuu mielestäni tuomaan esille ne asiat, jotka tulee käydä läpi tämän kaltaisessa toimitilaprojektissa. Organisaatioille oli valmiiksi tarjolla tietoa siitä, miten asioiden pitäisi korotetulla tasolla olla, mutta ei niinkään tietoa niistä askeleista, jotka sinne päästäkseen täytyy ottaa. Toimenpidesuunnitelman myötä organisaatioilla on käytössään työkaluja ja ohjeita prosessin suunnitteluun, toteutukseen ja ylläpitoon.

Kohdeorganisaatiolle suunnattu, salassa pidettävä toimenpidesuunnitelma onnistuu mielestäni näyttämään valmiin paketin, jonka avulla päästään kohti korotetun tason tiloja organisaatiossa. Toimenpidesuunnitelma on laadittu saman kaavan mukaisesti kuin julkinenkin versio, ja se on täydennetty niin pitkälle kuin on pystytty. Jos organisaatiolta tulee sille hyväksyntä, voidaan sitä alkaa toteuttamaan, ja muussa tapauksessa sitä voidaan käyttää pohjana ja ohjenuorana tulevaisuudessa.

Opinnäytetyössä on mielestäni onnistuttu selkeästi kuvaamaan prosessin etenemistä. Siinä on käyty läpi alkuasetelma ja siihen vaikuttaneet tekijät, käyttämäni tutkimusmenetelmät ja niillä saamani aineisto, sekä tulokset joita aineistoa analysoimalla syntyi. Valitut tutkimusmenetelmät sopivat työhön, sillä sain niillä monipuolista tietoa sekä kohdeorganisaation nykytilasta, että valtionhallinnon organisaatioiden menetelmistä tilaturvallisuuden parantamiseen. Tietoperusta antoi hyvän pohjan tutkimusmenetelmien hyödyntämiselle. Tuloksia analysoimalla nousi esille työn kannalta hyödyllisiä asioita, kuten riskiarvion tärkeys ja henkilöstön toiminnan suuri merkitys fyysisten suojauskeinojen tukena. Nämä kaikki on onnistuttu mielestäni kuvaamaan loogisella ja ymmärrettävällä tavalla.

Parannettavaakin toki jäi. Valtionhallinnolle suunnatun toimenpidesuunnitelman haasteena oli, että sillä ei millään pystytä ihan jokaisen organisaation tarpeisiin vastaamaan virastojen toiminnan moninaisuudesta johtuen. Tämän takia toimenpiteet piti määritellä hyvin yleisellä tasolla ja painopiste oli hallinnollisissa asioissa, eikä niinkään esimerkiksi yksittäisissä turvallisuustoimenpiteissä. Organisaatiot joutuvat siis edelleen itse tekemään ajatustyötä, kun määrittävät millaisia turvallisuushankintoja ja käytäntöjä juuri heidän virastossaan kaivattaisiin.

Työn toimeksiannossa toivottiin VAHTI 2/2013 -ohjeen käyttöä, mutta opinnäytetyön edetessä nousi esiin havaintoja, joiden perusteella se ei välttämättä ole paras kriteeristö toimitilojen tietoturvallisuuden korottamiseen. Sen vaatimuksia ei tulisi ainakaan sokeasti noudattaa, vaan lisäksi tarvitaan kattavaa ja jatkuvaa riskiarviointia ja tilannekuvan tarkastelua, jotta voidaan tehdä todenmukaisia päätelmiä siitä, mitä toimenpiteitä kannattaa oikeasti toteuttaa. VAHTI -ohjeistuksiin on tulossa vuoden vaihteessa muutoksia, joissa nämä asiat otetaan toivottavasti huomioon. Toimenpidesuunnitelmissa on pyritty painottamaan riskiarviota ja tilannekuvaa, mutta tämän työn tuloksia voisi VAHTI-rakenteen muuttuessa jatkokehittää luomalla toimenpidesuunnitelma, jossa vaatimukset ja riskiarviointi kulkevat koko ajan käsi kädessä.

Kaiken kaikkiaan opinnäytetyöllä on päästy vastaamaan siihen tarpeeseen, mihin alusta asti on ollut tarkoitus vastata. Kohdeorganisaatiossa se tarjoaa keinon päästä lähemmäksi toimitilojen korotettua tietoturvatasoa, ja nostaa esiin tärkeitä, mutta helposti unohtuvia asioita kuten henkilöstön kouluttamista. Työ antaa myös valtionhallinnon organisaatioille toimenpidesuunnitelman lisäksi tietoa siitä, mitä organisaatioilta odotetaan toimitilojen tietoturvallisuuden suhteen. Toivon, että tarjottuja tietoja hyödynnetään, jotta valtionhallinnon tietojenkäsittely olisi jatkossa entistä turvallisempaa.

Lähteet

Painetut lähteet

Gillies, A. 2012. Data Protection for Slightly Bigger Companies. Bearswood Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. Helsinki: Kustannusosakeyhtiö Tammi.

Ihamäki, R., Liukkonen, J. & Savolainen, E. 2014. Kiinteistö- ja tilaturvallisuuden tasot. Tampere: Tammerprint Oy.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

L588/2004. Laki kansainvälisistä tietoturvavelvoitteista.

L621/1999. Laki viranomaisen toiminnan julkisuudesta.

L681/2010. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro.

Peltier, T. 2013. Information Security Fundamentals. Boca Raton: CRC Press.

Perdikaris, J. 2014. Physical security and environmental protection. Boca Raton: CRC Press.

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Espoo: Aalto-yliopisto.

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Sähköiset lähteet

Elinkeinoelämän keskusliitto. 2016. Yritysturvallisuus. Viitattu 5.6.2016. http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Puolustusministeriö. 2015. Kansallinen turvallisuusauditointikriteeristö. Viitattu 1.3.2016. http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. Teemoittelu. Viitattu 10.5.2016. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_4.html

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Viitattu: 10.2.2016. http://www.uva.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Vahti ylläpito. 2009. Fyysinen turvallisuus. Viitattu 1.4.2016. https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus

VAHTI 4/2013. Henkilöstön tietoturvaohje. Viitattu 11.5.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10229

VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Viitattu 10.4.2016. https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta

VAHTI 2/2013. Toimitilojen tietoturvaohje. Viitattu 1.3.2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10128&groupId=10229

Valtio ja kunnat. 2016. Valtion hallintajärjestelmä. Viitattu 5.7.2016. https://www.suomi.fi/suomifi/suomi/valtio_ja_kunnat/valtion_hallintojarjestelma/index.html

Julkaisemattomat lähteet

Erään organisaation riskienhallintapäällikkö. 2016. Haastattelu. 23.5.2016. Helsinki.

Kangas, A. 2016. Konsultin haastattelu 23.5.2016. Helsinki.

Lehmusmetsä, T. 2016. Turvallisuuspäällikön haastattelu 10.6.2016. Helsinki.

Kohdeorganisaation riskienhallintapäällikkö. 2016. Haastattelu 5.4.2016. Helsinki.

Kohdeorganisaation tietoturvapäällikkö. 2016. Haastattelu 18.4.2016. Helsinki.

Kohdeorganisaation turvallisuuspäällikkö. 2016. Haastattelu 12.4.2016. Helsinki.

Kuviot

Taulukot

Liitteet

Liite 1: Esimerkki toimipisteestä (Mukautettu VAHTI 2/2013, 37-39,41)

ARVIOITAVA OSA-ALUE: RAKENTEET

VAATIMUS	PISTEET	HUOMIOITAVAA
Ulkoseinät lujaa betonia tai muuta vastaavan lujuuden omaavaa rakennetta	2	
Väliseinät (kun turvallisuusvyöhyke rajoittuu niihin) normaalia toimistokäyttöön hyväksyttyä harkkoseinää tai vahvistettua levyseinää	2	
Seinärakenteita ei voi irrottaa tilan ulkopuolelta	2	
Äänieristys estää asiattomia kuulemasta tiloissa käytyjä keskusteluja	2	
Alle 4 metriä maatasosta olevissa ikkunoissa suojalasitus	1	Ikkunat ovat yläkerroksissa, mutta joihinkin ikkunoihin pääsee alakatolta
Alle 4 metriä maatasosta olevia ikkunoita ei pysty avaamaan	1	Ikkunat ovat yläkerroksissa, mutta joihinkin ikkunoihin pääsee alakatolta
Ikkunoissa on sälekaihtimet	0	
Vyöhykkeen rajalla on turvaovi tai viranomaisten erillisvaatimusten mukaisesti vahvistettu vastaavan murtosuojan antava palo-ovi	1	2. kerroksessa vaatimukset täyttäviä, 3. kerroksessa ei
Aukot on suljettu kaltereilla tai vahvoilla terässäleiköillä	0	
Alempien turvallisuusvyöhykkeiden hätäpoistumistiet eivät kulje vyöhykkeen kautta	2	
Salassa pidettävät asiakirjat säilytetään kassakaapissa	0	
Kassakaapin murtosuoja EURO II (EN 1143-1)	2	
Kassakaapin paloturva 60 P tai 60 DIS (VDMA 24491) tai yhdistelmäkaappi 60P + 60 diskette	2	

Pisteytys:
2 pistettä = vaatimus täytetty
1 piste = lievä poikkeama vaatimuksesta
0 pistettä = vaatimusta ei ole täytetty

Vyöhykkeen rajalla oleva lukitus: käyttölukko heloineen ja vastalevyineen sekä hakatelljellä varustettu varmuuslukko vastalevyineen/muu saman murto- ja tiirikointilujuuden antava rakenne ja riittävät valvontajärjestelyt.	2	
Vyöhykkeen sisällä käyttölukot	0	Ovia pidetään auki
YHTEENSÄ	1,266667	

ARVIOITAVA OSA-ALUE: VALVONTAJÄRJESTELYT

VAATIMUS	PISTEET	HUOMIOITAVAA
Vyöhykkeen rajalla käytetään sähköistä kulunvalvontaa.	2	
Kulkuoikeuksien hallinnointi on viranomaisten hallinnassa, tai jos se on ulkoistettu, siitä on solmittu turvallisuussopimus	2	
Ovet on valvottu tunkeutumisenilmaisinjärjestelmällä	2	
Aukot on valvottu tunkeutumisenilmaisinjärjestelmällä	1	
Ikkunat on valvottu tunkeutumisenilmaisinjärjestelmällä	2	
Turvallisuusvyöhykettä valvotaan tallentavalla kameravalvonnalla	2	
Palvelintilaa valvotaan tallentavalla kameravalvonnalla	2	
Vartioinnin vasteaika on sellainen, että kiinnijäämisriski on merkittävä	2	ei tietoa
Vasteaika on testattu	0	
YHTEENSÄ	1,666667	

ARVIOITAVA OSA-ALUE: TURVALLISUUSTIETOISUUS JA TOIMINTATAVAT

VAATIMUS	PISTEET	HUOMIOITAVAA

Tunkeutumisenilmaisinjärjestelmän testauksesta ja hallinnoinnista on turvallisuusdokumentaatio	0	Rikosilmoitinjärjestelmää uusitaan
Vartioinnin vasteajan testauksen tulokset on dokumentoitu	0	
Henkilöstölle on koulutettu, että julkisissa tiloissa ei saa keskustella salassa pidettävistä asioista	2	
Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa salassa pidettävistä asioista	1	Ovia pidetään paljon auki
Monimuotoisessa työympäristössä keskustelut salassa pidettävistä asioista käydään riittävästi äänieristetyssä tilassa	2	
YHTEENSÄ	1	

	KOROTETUN TASON PISTEET
RAKENTEET	1,266666667
VALVONTAJÄRJESTELYT	1,666666667
TURVALLISUUSTIETOISUUS JA TOIMINTATAVAT	1
YHTEENSÄ	1,311111111

Matala riskitaso: 1,5-2 pistettä
Keskimääräinen riskitaso: 1-1,5 pistettä
Korkea riskitaso: 0-1 pistettä

Liite 2: Toimenpidesuunnitelma valtionhallinnon organisaatioille

Toimitilat tietoturvallisuuden korotetulle tasolle - toimenpidesuunnitelma

Ronkainen, Maija

2016 Laurea

Laurea-ammattikorkeakoulu

Toimitilat tietoturvallisuuden korotetulle tasolle - toimenpidesuunnitelma

Maija Ronkainen
Turvallisuusalan koulutusohjelma
Toimenpidesuunnitelma
Elokuu, 2016

Sisällys

1 Johdanto

Tässä toimenpidesuunnitelmassa käydään kohta kohdalta läpi, mitä tekijöitä tulisi ottaa huomioon, kun valtionhallinnon organisaatiossa pyritään toimitiloissa tietoturvallisuuden korotetulle tasolle. Suunnitelma on yleisluontoinen, eikä välttämättä sovellu jokaiseen organisaatioon. Suunnitelmaan on kuitenkin pyritty luomaan liikkumavaraa, jonka puitteissa suuri osa valtionhallinnon organisaatioista voi toimia.

Toimenpidesuunnitelmassa on kahdeksan ylätason vaihetta. Se alkaa luokittelupäätöksestä, ja päättyy toimenpiteiden ylläpitoon. Vaiheisiin on pyritty luomaan työkalut, joilla ne saataisiin tehokkaasti toteutettua ja lisättyä osaksi organisaation riskienhallintaa. Työkalut löytyvät liitteistä, ja niiden alkua on täytetty esimerkin vuoksi. Organisaatio täyttää ne kuitenkin itse omilla tiedoillaan.

2 Luokittelupäätös

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa edellyttää, että valtionhallinnon organisaatiot ovat saavuttaneet tietoturvallisuuden perustason 1.10.2013. Jos organisaatio käsittelee korotetun tason tietoa, tulee sen tehdä luokittelupäätös, jonka mukaan korkeamman tason asiakirjoja käsitellään vahvemmin suojausperiaattein. Korotetulle tasolle tulee päästä viisi vuotta sen jälkeen, kun luokittelupäätös on tehty. Lisäksi organisaation toimitilojen tulee olla asetuksen vaatimalla tasolla viisi vuotta asetuksen voimaantulon jälkeen, eli 1.10.2015. (L681/2010, 23§)

Organisaatioissa, joissa luokittelupäätös on tehty, on toimitilaprojekteille jo asetettu takaraja. Toimitilaprojektille tulee saada hyväksyntä johdolta, ja tämä lain määräämä takaraja toimii hyvänä perusteluna, miksi toimitilaprojekti tulisi aloittaa. Organisaatioissa, joissa päätöstä ei ole tehty, toimii lain vaatimus luokittelupäätökselle vastaavasti hyvänä perusteena toimitilaprojektille.

3 Sidosryhmien tunnistaminen ja sitouttaminen

Kun toimitilojen tietoturvallisuus pyritään nostamaan perustasolta korotetulle tasolle, tulee projektin avainhenkilöt tunnistaa ja kiinnittää projektiin jo alkuvaiheessa. Liitteessä 1 kuvattu taulukko avainhenkilöistä ja sidosryhmistä on jaettu karkeasti kolmeen ryhmään: suunnittelu-, toteutus- ja ylläpitovaiheeseen. Kun projektia vasta suunnitellaan, ei henkilöille tarvita vielä tarkkaa aikataulua tai tehtävänkuvia.

Avainhenkilöt ja sidosryhmät -taulukkoon (liite 1) täytetään projektissa olennaisten henkilöiden nimet. Taulukossa on lueteltu, millaisia tahoja sieltä tulisi ainakin löytyä, mutta organisaatio voi lisätä siihen lisäksi omalle toiminnalleen keskeisiä henkilöitä.

4 Nykytilan kartoitus

Ennen kuin tavoitellaan tietoturvallisuuden korotettua tasoa, tulee olla selvillä siitä, millä tasolla ollaan tällä hetkellä. Liitteestä 2 löytyy VAHTI 2/2013 toimitilojen tietoturvaohjeen kriteeristöistä muokattu taulukko, jossa on otettu huomioon rakenteet, valvontajärjestelyt sekä henkilöstön toimintatavat. Taulukko on täytetty esimerkin vuoksi, mutta organisaatio täydentää sen itse omilla tiedoillaan.

Organisaation koko vaikuttaa siihen, kuinka paljon kartoituksia tulee tehdä. Jos toimitiloja on vähän, kannattaa kaikki kartoittaa parhaimman käsityksen saamiseksi. Jos niitä on kuitenkin useita kymmeniä, tulisi niistä kartoittaa otanta, jossa olisi mahdollisimman monipuolisesti edustettuna erilaiset toimitilat. Valinnoissa tulee kiinnittää huomiota tilojen kokoon, henkilöstön määrään sekä niissä harjoitettavan toiminnan luonteeseen. Liitteestä 3 löytyy taulukko, johon merkitään toimitilojen ominaisuudet, sekä kartoitusten tulokset.

5 Riskiarvio

Kun nykytilan kartoituksessa on saatu selville organisaation riskitaso rakenteiden, valvontajärjestelyiden sekä henkilöstön toimintatapojen osalta, sekä kirjattua suurimmat puutteet, on riskiarvion aika. Suurimmille puutteille mietitään seuraukset. Jos puute on esimerkiksi äänieristyksen puuttuminen, on seurauksena salassa pidettävän tiedon kantautuminen ulkopuolisten korviin. Seurauksille lasketaan niiden riskiluvut kertomalla niiden vaikuttavuuden ja todennäköisyyden arvot keskenään. Tähän tarkoitettu kaavio löytyy liitteestä 4.

Kun mietitään seurausten todennäköisyyttä, on huomioitava seuraavat asiat:

1. Toimitilan ympäristö; millaista toimintaa ympärillä on ja kuinka lähellä on muita ihmisiä
2. Toimitilassa harjoitettavan toiminnan luonne; onko tiloissa paljon rahallisesti arvokasta tavaraa, mitä muuta rikollisia kiinnostavaa siellä on
3. Tilannekuva; millainen on vallitseva tilanne henkilöstössä tai jopa ympäröivässä yhteiskunnassa esimerkiksi talouden ja turvallisuuden suhteen, ja miten se vaikuttaa organisaatioon

Kun mietitään seurausten vakavuutta, on huomioitava seuraavat asiat:

1. Rahalliset vaikutukset; kuinka suuria tappioita seurauksesta syntyy

2. Vaikutukset henkilöstön turvallisuuteen ja hyvinvointiin; kuinka vahvoja negatiivisia vaikutuksia seurauksella on henkilöstön turvallisuuteen ja hyvinvointiin
3. Vaikutukset yhteiskunnan turvallisuuteen ja hyvinvointiin; kuinka vahvoja negatiivisia vaikutuksia seurauksella on yhteiskunnan turvallisuuden ja hyvinvoinnin kannalta
4. Vaikutus toiminnan jatkamiseen; vaikuttaako seuraus toiminnan jatkamiseen ja kuinka pitkäksi aikaa

Kun riskien seurausten vakavuus on laskettu taulukon avulla, laitetaan ne tärkeysjärjestykseen, päätetään mihin niistä puututaan ja määritellään suojaustoimenpiteet. Kriittisimpiin poikkeamiin tulisi ainakin puuttua, ja muiden kohdalla niitä tulee peilata organisaation toimintaan ja tilannekuvaan, ja päättää hyväksytäänkö riskit vai laaditaanko niille toimenpiteet. Toimenpiteet määritellään yleisellä tasolla sen perusteella, mitä toimitilakartoituksissa havaittiin puutteiksi. Toimenpiteille lasketaan kustannusarviot.

6 Kustannusarvio

Liitteestä 5 löytyy taulukko, johon merkitään toimipisteittäin riskiarvion perusteella päätetyt puutteet, toimenpiteet niiden korjaamiseksi, sekä kustannusarviot toimenpiteille. Ennen kuin voidaan siirtyä toimenpiteiden toteuttamiseen, kyseinen arvio tulee hyväksyttää johtoryhmällä.

Kustannukset vaihtelevat suuresti sen perusteella, mitä puutteita halutaan korjata, ja millaisia sopimuksia organisaatiolla on jo valmiiksi eri alihankkijoiden kanssa. Suuntaa antavana apuna kustannusarviossa voi käyttää kuitenkin seuraavia periaatteita:

Rakenteet: 3 prosenttia koko hankkeen kokonaiskustannuksista, kun halutaan nostaa toimitilat tietoturvallisuuden perustasolta korotetulle tasolle. Tähän lasketaan siis vain tiedon salassa pidettävyyteen liittyvät toimenpiteet, ei esimerkiksi paloturvallisuuteen liittyviä asioita.

Valvontajärjestelyt: 10 euroa neliötä kohden kertainvestointina. Lisäksi elinkaarikustannuksiin kuuluu huoltokulut sekä palvelumaksut.

Henkilöstön toimintatavat: Yksi ihminen 800 työntekijää kohden. Tällä tarkoitetaan kokopäiväistä henkilöä, jonka vastuulla on henkilöstön kouluttamiseen ja tietoisuuden ylläpitoon liittyvät asiat. Syntyvät kustannukset tarkoittavat siis tällaisen henkilön palkkakustannuksia. Joillakin organisaatioilla tällainen henkilö on jo valmiiksi, jos kyseiset asiat kuuluvat esimerkiksi riskienhallintapäällikön tehtäviin. Kustannuksiin vaikuttaa tämän lisäksi myös se, paljonko koulutuksiin osallistumalla menetetään työaikaa. Tämä vaihtelee organisaatioittain paljon.

7 Toteutus

Kun toimenpiteet ja niiden kustannukset on hyväksytetty organisaation johdolla, voidaan niitä alkaa toteuttaa. Liitteessä 6 on taulukko, johon merkitään päätetyt toimenpiteet, toimenpiteiden vaiheet sekä niiden vastuuhenkilöt ja aikataulu.

Taulukossa toimenpiteet avataan niin, että niiden eri toteutusvaiheet kirjataan ylös ja niille määritellään aikataulu ja vastuuhenkilö. Toteutusvaiheet määrittämällä varmistutaan siitä, että kaikki asiat otetaan alusta saakka huomioon, ja toimenpiteille on vastuuhenkilöt koko prosessin ajan. Aikataulua laadittaessa tulee ottaa huomioon, mitkä riskiarvioissa havaituista puutteista olivat kriittisimpiä.

Toteutus-vaiheen aluksi määritellään myös säännölliset ajankohdat palavereille, joissa käydään hankkeen etenemistä läpi. Palavereissa tulisi olla mukana organisaation sisäiset vastuuhenkilöt, sekä ulkoisten alihankkijoiden vastuuhenkilöt. Tarvittavat tahot voi tarkistaa liitteestä 1 löytyvästä vastuuhenkilöiden luettelosta, ja sieltä nimenomaan toteutusvaiheesta.

8 Auditointi

Kun toimenpiteet on suoritettu, tiloissa tehdään jälkitarkastus eli toisin sanoen auditointi. Tällä varmistetaan, että haluttuihin tuloksiin on päästy. Tähän kannattaa hankkia ulkopuolinen auditoija, joka näkee tilat uusin silmin.

Jos auditoinnin tulos osoittaa, että kaikkia tavoitteita ei ole saavutettu, asetetaan ajankohta seuraavalle auditoinnille, johon mennessä asia tulee korjata. Auditoinnin tuloksia tulee verrata riskiarvioon, eli kaikkia muutoksia ei välttämättä kannata sokeasti toteuttaa.

Auditoinnissa on vaikea huomioida henkilöstön toimintatapoja. Organisaation täytyy testata niitä toisin keinoin. Tähän soveltuu esimerkiksi verkkotentit organisaation oppimisympäristössä.

9 Ylläpito

Kun toimitiloissa ollaan päästy tietoturvallisuuden korotetulle tasolle, tarkoituksena olisi myös pysyä siellä. Sen takia on tärkeää määrittää myös turvallisuuden ylläpitokeinoja organisaatiossa. Seuraavassa on listattu yleiset periaatteet ylläpidolle, joita voi toki organisaation toiminnan luonteesta riippuen muovata:

1. Ylläpidolle on määriteltävä vastuuhenkilö, yleensä sama joka on ollut prosessin omistaja projektissa, esimerkiksi riskienhallintapäällikkö.
2. Rakenteellinen turvallisuus tarkistetaan yhdessä kiinteistön omistajan kanssa joka toinen vuosi.
3. Valvontajärjestelmien toimivuus ja ajankohtaisuus tarkistetaan vuosittain.
4. Henkilöstön perehdytyksen yhteydessä järjestetään turvallisuuskoulutus, jossa käydään läpi toimitilaturvallisuuteen liittyviä asioita.
5. Pakollinen turvallisuuskoulutus henkilöstölle vuosittain, jossa käsitellään myös toimitilaturvallisuuteen liittyviä asioita.
6. Turvallisuusohjeet ja dokumentit tarkistettava tai päivitettävä vuosittain.
7. Tarkistuksia ja koulutuksia tulee järjestää useammin, jos organisaation toiminnassa tai tilannekuvassa tapahtuu merkittäviä muutoksia.

Lähteet

L681/2010. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa.

Liitteet

Liite 3: Avainhenkilöt ja sidosryhmät

SUUNNITTELUVAIHE		
Henkilö	**Rooli**	**Ajankohta**
Riskienhallintapäällikkö	Prosessin omistaja	Koko prosessi
Tietoturvan substanssin osaaja	Asiantuntija-apu	Koko prosessi
Johto	Informoitava, antaa hyväksynnän	Lopussa
Henkilöstön edustaja	Asiantuntija-apu	Riskiarvion aikana
Kiinteistön omistajan edustaja	Toteuttaja	Koko prosessi
Organisaation kiinteistövastaava	Toteuttaja	Koko prosessi
TOTEUTUSVAIHE		
Henkilö	**Rooli**	**Ajankohta**
Riskienhallintapäällikkö	Prosessin omistaja	Koko prosessi
Kiinteistön omistajan edustaja	Toteuttaja	Koko prosessi
Organisaation kiinteistövastaava	Toteuttaja	Koko prosessi
Alihankkijat - rakennuspuoli	Toteuttaja	Koko prosessi
Alihankkijat - valvontapuoli	Toteuttaja	Koko prosessi
Johto	Informoitava, antaa hyväksynnän	Säännöllisin väliajoin
Ulkoinen auditoija	Asiantuntija-apu	Lopussa
YLLÄPITOVAIHE		
Henkilö	**Rooli**	**Ajankohta**

Riskienhallintapäällikkö	Prosessin omistaja	Koko prosessi
Johto	Informoitava, antaa hyväksynnän	Säännöllisin väliajoin
Organisaation kiinteistövastaava	Toteuttaa	Vuosittain

Liite 4: Kriteeristö toimitilojen kartoitukseen (Mukautettu VAHTI 2/2013, 37-39, 41)

ARVIOITAVA OSA-ALUE: RAKENTEET

VAATIMUS	PISTEET	HUOMIOITAVAA
Ulkoseinät lujaa betonia tai muuta vastaavan lujuuden omaavaa rakennetta	2	
Väliseinät (kun turvallisuusvyöhyke rajoittuu niihin) normaalia toimistokäyttöön hyväksyttyä harkkoseinää tai vahvistettua levyseinää	2	
Seinärakenteita ei voi irrottaa tilan ulkopuolelta	2	
Äänieristys estää asiattomia kuulemasta tiloissa käytyjä keskusteluja	2	
Alle 4 metriä maatasosta olevissa ikkunoissa suojalasitus	1	Ikkunat ovat yläkerroksissa, mutta joihinkin ikkunoihin pääsee alakatolta
Alle 4 metriä maatasosta olevia ikkunoita ei pysty avaamaan	1	Ikkunat ovat yläkerroksissa, mutta joihinkin ikkunoihin pääsee alakatolta
Ikkunoissa on sälekaihtimet	0	
Vyöhykkeen rajalla on turvaovi tai viranomaisten erillisvaatimusten mukaisesti vahvistettu vastaavan murtosuojan antava palo-ovi	1	2. kerroksessa vaatimukset täyttäviä, 3. kerroksessa ei
Aukot on suljettu kaltereilla tai vahvoilla terässäleiköillä	0	

Pisteytys:
2 pistettä = vaatimus täytetty
1 piste = lievä poikkeama vaatimuksesta
0 pistettä = vaatimusta ei ole täytetty

Alempien turvallisuusvyöhykkeiden hätäpoistumistiet eivät kulje vyöhykkeen kautta	2	
Salassa pidettävät asiakirjat säilytetään kassakaapissa	0	
Kassakaapin murtosuoja EURO II (EN 1143-1)	2	
Kassakaapin paloturva 60 P tai 60 DIS (VDMA 24491) tai yhdistelmäkaappi 60P + 60 diskette	2	
Vyöhykkeen rajalla oleva lukitus: käyttölukko heloineen ja vastalevyineen sekä hakatelljellä varustettu varmuuslukko vastalevyineen/muu saman murto- ja tiirikointilujuuden antava rakenne ja riittävät valvontajärjestelyt.	2	
Vyöhykkeen sisällä käyttölukot	0	Ovia pidetään auki
YHTEENSÄ	1,266667	

ARVIOITAVA OSA-ALUE: VALVONTAJÄRJESTELYT

VAATIMUS	PISTEET	HUOMIOITAVAA
Vyöhykkeen rajalla käytetään sähköistä kulunvalvontaa.	2	
Kulkuoikeuksien hallinnointi on viranomaisten hallinnassa, tai jos se on ulkoistettu, siitä on solmittu turvallisuussopimus	2	
Ovet on valvottu tunkeutumisenilmaisinjärjestelmällä	2	
Aukot on valvottu tunkeutumisenilmaisinjärjestelmällä	1	
Ikkunat on valvottu tunkeutumisenilmaisinjärjestelmällä	2	
Turvallisuusvyöhykettä valvotaan tallentavalla kameravalvonnalla	2	

Palvelintilaa valvotaan tallentavalla kameravalvonnalla	2	
Vartioinnin vasteaika on sellainen, että kiinnijäämisriski on merkittävä	2	ei tietoa
Vasteaika on testattu	0	
YHTEENSÄ	1,666667	

ARVIOITAVA OSA-ALUE: TURVALLISUUSTIETOISUUS JA TOIMINTATAVAT

VAATIMUS	PIS-TEET	HUOMIOITAVAA
Tunkeutumisenilmaisinjärjestelmän testauksesta ja hallinnoinnista on turvallisuusdokumentaatio	0	Rikosilmoitinjärjestelmää uu-sitaan
Vartioinnin vasteajan testauksen tulokset on dokumentoitu	0	
Henkilöstölle on koulutettu, että julkisissa tiloissa ei saa keskustella salassa pidettävistä asioista	2	
Huoneen ovet ja ikkunat pidetään kiinni keskusteltaessa salassa pidet-tävistä asioista	1	Ovia pidetään paljon auki
Monimuotoisessa työympäristössä keskustelut salassa pidettävistä asi-oista käydään riittävästi äänieriste-tyssä tilassa	2	
YHTEENSÄ	1	

	KOROTETUN TASON PISTEET
RAKENTEET	1,266666667
VALVONTAJÄRJESTELYT	1,666666667
TURVALLISUUSTIETOISUUS JA TOI-MINTATAVAT	1
YHTEENSÄ	1,311111111

Matala riskitaso: 1,5-2 pistettä
Keskimääräinen riskitaso: 1-1,5 pistettä
Korkea riskitaso: 0-1 pistettä

Liite 5: Toimipisteiden yhteenveto

Kartoitettu toimipiste	Henkilöstön määrä	Toimitilan koko (m2)	Tarkastuspäivä määrä	Rakenteet	Valvontajärjestelyt	Toimintatavat	Yhteensä	Suurimmat puutteet
Helsinki	50	300	1.6.2016	1,5	1	1,2	1,23	Tunkeutumisenilmaisinjärjestelmä puuttuu, ikkunat katukerroksessa ilman näköesteitä

Liite 6: Vaikuttavuuden arviointi

Seuraus	Todennäköisyys	Vaikutus	Riskin suuruus
	1=epätodennäköinen	1 =pieni	1-2 pieni
	2 =mahdollinen	2 =keskisuuri	3-4 kohtalainen, 5 merkittävä
	3 =todennäköinen	3 =suuri	6-9 sietämätön
Salassa pidettävät asiat kantautuvat ulkopuolisen korviin	2	1	2
Ulkopuoliset näkevät salassa pidettäviä asioita ikkunasta	3	2	6

Liite 7: Kustannusarvio

Toimitila	Puutteet	Toimenpiteet	Kustannusarvio (kertainvestointi + elinkaarikustannukset)
Helsinki	Äänieristys puuttuu	Väliseinien vahvistus huoneissa, joiden toisella puolella on eri organisaatioiden tiloja	Kertainvestointi: 4000 e, elinkaarikustannukset: 0 e
	Toimitiloissa ei ole kameravalvontajärjestelmää	Kameravalvonnan hankkiminen	Kertainvestointi: 2000 e, elinkaarikustannukset:
Tampere	Henkilöstö ei lukitse ovia perässään ja keskustelee salassa pidettävistä asioista ovet auki	Tunnin mittainen turvallisuuskoulutus henkilöstölle	Kertainvestointi: 300 e (menetetystä työajasta), elinkaarikustannukset: 0 e

Liite 8: Toimenpideluettelo toteutusvaiheeseen

Toimenpide	Vaiheet	Aikataulu	Vastuuhenkilö
Kameravalvontajärjestelmän hankkiminen Helsingin, Espoon ja Tampereen toimipisteisiin	Kameravavontajärjestelmien kilpailutus	10/2016	Turvallisuuspäällikkö
	Sopimusten ja rekisteriselosteiden laadinta	11/2016	Turvallisuuspäällikkö
	Suunnitelma sijoittelusta	11/2016	Turvallisuus- ja kiinteistöpäällikkö
	Yt-menettely	12/2016	Turvallisuuspäällikkö
	Järjestelmien asennus	1-2/2017	Kiinteistöpäällikkö ja alihankkija
Turvallisuuskoulutuksen järjestäminen Helsingin ja Tampereen henkilöstölle	Koulutusten suunnittelu ja hyväksyttäminen johdolla	1/2017	Riskienhallintapäällikkö
	Kolutuksista tiedottaminen	1/2017	Riskienhallintapäällikkö
	Koulutukset	2/2017	Riskienhallintapäällikkö
	Palautteen kerääminen	2-3/2017	Riskienhallintapäällikkö

Liite 9: Kohdeorganisaation turvallisuuspäällikön arvio opinnäytetyöstä

OPINNÄYTETYÖN ARVIOINTI

AIHE: Toimitilat tietoturvallisuuden korotetulle tasolle valtionhallinnossa

Maija Ronkainen teki opinnäytetyönsä yhteydessä organisaatiollemme toimenpidesuunnitelman toimitilojen tietoturvallisuuden korottamisesta. Tarve luoda organisaatiollemme keinot toimitilaturvallisuuden korottamiseksi syntyi alkuvuodesta 2015, kun toimitiloissamme tehtiin turvallisuuskartoituksia. Opinnäytetyöprosessi aloitettiin joulukuussa 2015.

Opinnäytetyössä on kuvattu selkeästi prosessi, jonka tuloksena toimenpidesuunnitelma syntyi. Toimenpidesuunnitelman vaiheiden valinnat on perusteltu hyvin ja ne ovat loogisessa järjestyksessä. Sen sisällössä on otettu kattavasti huomioon organisaatiomme tarpeet. Maijan kanssa yhteistyö kävi mutkattomasti ja meillä on ollut säännöllisiä palavereja koko prosessin ajan aiheeseen liittyen.

Toimenpidesuunnitelmaa ei olla esitelty vielä organisaatiossa niille tahoille, jotka sen käynnistämisestä päättävät. Maija olisi voinut laatia sen tiiviimmässä aikataulussa, jotta tulosten pätevyyttä olisi voinut arvioida useampi taho ja tarvittavat toimenpiteet olisi saatu nopeammin budjetoitua tuleville vuosille. Olisin myös toivonut, että kehitystarpeista olisi esitetty tarkemmat kustannuslaskelmat.

Opinnäytetyössä onnistuttiin luomaan pääosin toimivat ratkaisut toimitilaturvallisuuden korottamiseksi ja tulemme hyödyntämään opinnäytetyöstä saatuja työkaluja soveltuvin osin.

Helsingissä 1.8.2016

Nimi [redacted]

Allekirjoitus [redacted]