LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnan kehittämis-suunnitelma

Allonen, Janne

2017 Laurea

Laurea-ammattikorkeakoulu

Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnan kehittämissuunnitelma

Janne Allonen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma

Janne Allonen

Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnan kehittämissuunnitelma

Vuosi 2017 Sivumäärä 53

Yhteiskuntamme digitalisoituu yhä nopeammin ja verkkoon kytkettyjä laitteita on ennustettu olevan kymmeniä miljardeja lähivuosina. Uusi teknologia, uudet innovaatiot ja palveluiden sähköistyminen luovat kybermarkkinoille uusia mahdollisuuksia. Samaan aikaan kyberrikollisuus on myös voimakkaassa nousussa ja asettaa yhteiskuntamme kriittisimmätkin toimijat alttiiksi erilaisille uhille ja häiriöille.

Yritysten osalta, niin julkisella- kuin yksityissektorillakin, Viestintävirastolla on suuri rooli yritysturvallisuuden parantamisessa. Viestintäviraston tehtävä on tarjota varmaa ja vaivatonta viestintää Suomessa. Viestintäviraston tehtävänä on myös ohjata ja valvoa tietoturvallisuuden arviointilaitoksia. Tietoturvallisuuden arviointilaitokset tarjoavat viranomaisille ja yrityksille luotettavaa ja puolueetonta tietoturvallisuuden arviointipalvelua. Tietojärjestelmätarkastukset ovat suuri osa tästä kokonaisuudesta.

Yhteistoiminta Viestintäviraston ja tietoturvallisuuden arviointilaitoksen välillä on varsin nuorta, eikä hyväksi todettuja menetelmiä ole muodostunut. Tämän kvalitatiivisen ja toiminnallisen opinnäytetyön tutkimuksen tuloksena syntyi kehittämissuunnitelma yhteistoiminnan parantamiseksi organisaatioiden välillä.

Opinnäytetyön tietoperusta pohjautuu pääsääntöisesti julkisiin asiakirjoihin, asia koskevaan lainsäädäntöön, Viestintäviraston laatimaan ohjeeseen tietoturvallisuuden arviointilaitoksille sekä Viestintäviraston määräyksiin ja muuhun ohjeistukseen. Opinnäytetyön tiedonkeruu suoritettiin sisällönanalyysin ja puolistrukturoidun teemahaastattelun avulla. Sisällönanalyysi kohdistui arviointilaitostoimintaan liittyvään dokumentaatioon eli raportteihin, todistuksiin ja lausuntoihin. Tutkimusta varten haastateltiin Viestintäviraston ja tietoturvallisuuden arviointilaitosten asiantuntijoita.

Opinnäytetyön tutkimuksen avulla voidaan todeta, että yhteistoiminta Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä ei ole vielä tällä hetkellä riittävän hyvällä tasolla. Yhteistoiminnan kehittäminen vaatii prosessien selkeyttämistä, koulutuksen lisäämistä, dokumentaation yhtenäistämistä, tapaamisten säännöllistämistä, valvonnan järkevöittämistä ja lisäresursoinnin tarpeellisuuden pohtimista. Tulosten analysointi suoritettiin itsenäisesti laatijan toimesta.

Opinnäytetyön pyrkimys oli lisätä laadukasta yhteistyötä Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä. Tämä tavoite myös saavutettiin. Tutkimus on tarpeellinen ja hyödyllinen kaikkien osapuolten näkökulmasta. Kehittämissuunnitelma esitellään yritysten johdolle ja jalkautetaan opinnäytetyöstä erillisenä prosessina Viestintävirastolle ja tietoturvallisuuden arviointilaitoksille opinnäytetyön valmistuttua.

Valtioneuvoston tuore selvitys Suomen kyberturvallisuuden nykytilasta kuvaa elintärkeiden toimintojen ja huoltovarmuuskriittisten yritysten kyberuhilta suojautumiskyvyn riittämättömänä ja häiriötilanteiden resilienssin heikkona. Tämä osoittaa tutkimuksen reliabiliteettia ja validiteettia sekä avaa myös mahdollisuuden jatkotutkimukselle näiden asioiden ympärillä.

Asiasanat: Kehittämissuunnitelma, Kyberturvallisuus, Tietoturvallisuuden arviointilaitos, Tietojärjestelmätarkastus, Viestintävirasto

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

Janne Allonen

Establishing a Development Plan for co-operation between the Finnish Communications Regulatory Authority and Information Security Inspection Bodies

Year 2017 Pages 53

The digitalisation of society is faster than ever and according to latest research there are predicted to be tens of billions of devices connected to the Internet in the upcoming years. New technology, new innovations and the electronic access to services create new possibilities on the cybermarket. At the same time we can see a strong increase in cybercrime, which makes even the most critical actors of society vulnerable to different kinds of threats and disturbances.

The Finnish Communications Regulatory Authority (FICORA) has an important role in improving corporation security, both in the public and private sectors. FICORA's mission is to offer reliable and easy communications means for everyone in Finland. FICORA also has duties in guiding and supervising the Information Security Inspection Bodies. The inspection bodies offer reliable and impartial evaluation of information security to authorities and corporations. The inspection of information security systems is a crucial part of this inspection task.

The activity of co-operation between FICORA and facilities has a short history. Solid methods for co-operation have not been developed. As a result of this qualitative and functional research a development plan for improving the co-operation between the organisations was established.

The framework of reference is based on public documents, legislation on the matter, FICORA's guidelines for inspection bodies and other regulations and guidelines. The research data was analysed by content and by combining structured and focused interview techniques. The content analysis focused on the documentation used in the activity of inspection bodies, more specifically reports, certificates and statements. Specialists of FICORA and Information Security Inspection Bodies were interviewed.

Based on the research, it can be concluded that the co-operation between FICORA and the inspection bodies is not operated sufficiently enough at the moment. The development of co-operation requires a clarification of processes, increase in training, standardising documents, regular meetings, reasoning the measures of controls and considering the necessity of additional resources. The results were analysed independently by the investigator.

The objective of the research was to improve the qualitative co-operation between FICORA and the Information Security Inspection Bodies. This objective was also met. The research is necessary and useful from the point of view of all parties. The research results will be presented to representatives of both organizations. They will also be implemented in practise.

Recent research on the Finnish government describes the protection of cyber threats and the resilience of disturbances for corporations and supply secure state administrators as insufficient and weak. This points out the reliability and validity of the research and offers also a possibility of a further investigation considering these matters.

Keywords: Cyber Security, Development Plan, Finnish Communications Regulatory Authority, Information Security System Inspection, Information Security Inspection Bodies

Sisällys

1 Johdanto

Kyberturvallisuus on toimialana uusi, eikä sen käsitteistö ole vielä vakiintunut. Aiheena kyberturvallisuus on ajankohtainen ja media kirjoittaa siitä runsaasti. Vielä muutamia vuosia sitten koko sanasta ei ollut tietoakaan. Nykyään kyberuhkia tai -haavoittuvuuksia välitetään kansalaisille tiedoksi jopa iltapäivälehtien etusivuilla. Gartner Research on arvioinut, että vuonna 2020 Internetiin on liitettynä yli 20 miljardia laitetta. Tutkimuksen mukaan villeimmät arvioit liikkuvat jopa yli 75 miljardin laitteen tienoilla (RCR Wireless News 2017). Uusi teknologia, uudet innovaatiot ja palveluiden sähköistyminen luovat kybermarkkinoille uusia mahdollisuuksia. Samaan aikaan kyberrikollisuus on voimakkaassa nousussa ja asettaa yhteiskuntamme kriittisimmätkin toimijat alttiiksi erilaisille uhille ja häiriöille.

Suomen valtion ensimmäinen kyberturvallisuusstrategia hyväksyttiin periaatepäätöksenä valtioneuvoston yleisistunnossa vasta 24. tammikuuta 2013. Tämän seurauksena muun muassa Viestintäviraston Kyberturvallisuuskeskus aloitti toimintansa 1. tammikuuta 2014 (Turvallisuuskomitea 2015). Voidaankin mielestäni ihan aiheellisesti kysyä, mitä olemme tehneet viimeiset kymmenen vuotta kyberturvallisuuden osa-alueella.

Internetin räjähdysmäinen kasvu niin käyttäjien kuin laitteiden saralla ja digitalisaation voimakas vyöry markkinoille sen kaikissa muodoissaan tuovat mukanaan valtavan potentiaalin hyötynäkökulmasta. Samat ilmiöt mahdollistavat myös suuren potentiaalin uusille riskeille ja haavoittuvuuksille (Valtiovarainministeriö 2016a).

Tämän päivän rikollisuus ilmenee yhä enemmän erilaisina huijausmenetelminä Internetin välityksellä. Sitä voidaan kohdistaa niin yksilöihin, yrityksiin kuin valtiollisiin toimijoihin monilla eri tavoilla. Suomessa viime aikoina kalastelu- ja huijausviestit ovat kohdistuneet yksityisiin henkilöihin. Haitta- tai kiristyshaittaohjelmat pyritään usein kohdistamaan yritysten tai organisaatioiden johtoon. Yhteinen tekijä näillä kaikilla on mahdollisimman suuren rikoshyödyn tavoittelu joko suoraan tai välillisesti. Verkkovakoilu ja informaatiovaikuttaminen ovat kehittyneet ja monipuolistuneet viime vuosina kohteinaan yleisesti julkishallinnon toimijoiden tai yritysten tietojärjestelmät sekä ulkoasian- ja puolustushallinnot. (Viestintävirasto 2017a.)

Globaalit trendit kuten esineiden Internet (IoT), automatisaatio, robotisaatio, 5G-teknologia ja jo mainittu digitalisaatio ovat jättäneet pysyvät jäljet kuluttajien, yritysten ja valtioiden jokapäiväiseen toimintaan. Yhä useampi henkilö tai organisaatio on nykyään riippuvainen näiden trendien mahdollistavista sähköisistä toiminnoista. Tämän myötä myös palveluiden tai toimintojen eheys, luotettavuus, oikeellisuus ja niiden jatkuvuudenhallinta on korostunut. Toiminnot on pystyttävä takaamaan niin normaali kuin poikkeusoloissakin. Näiden trendien mukanaan tuomien hyötyjen ja haittojen erittely varsinkin kansalaisille on yhä vaikeampaa.

1.1 Aiheen valinta

Opinnäytetyön aihe valikoitui luontaisesti omien työtehtävieni toimenkuvan perusteella. Kybertoimintaympäristö elää jatkuvan muutoksen aallonharjalla ja tulee tulevaisuudessa olemaan yksi tärkeimmistä turvallisuuden osa-alueista - niin kansallisesti kuin kansainvälisestikin. Tärkeyden korostuessa voidaan todeta, että myös viranomaisen työtehtävät tällä osa-alueella tulevat varmuudella lisääntymään. Viranomaisen näkökulmasta ongelma on suuri. Resurssit eivät tahdo riittää kasvavien tehtävämäärien hoitamiseen.

Opinnäytetyön ajankohtaisuus on myös merkittävä, koska uusia kyberilmiötä esiintyy yhä enemmän ja ne ovat globaaleja. Näistä viimeisimpinä esimerkkeinä ovat maailmanlaajuinen palvelunestohyökkäys ja yksi maailman yleisimmin käytetyn langattomien verkkojen salaukseen liittyvän salausmenetelmän murtaminen. Kyberturvallisuuden tason osoittaminen ja sen ylläpitämisen merkitys on korostunut yhteiskunnassamme. Viranomaisen resurssipulan avuksi on luotu tietoturvallisuuden arviointilaitoksia, joiden tehtävänä on auttaa Viestintävirastoa yritysturvallisuuden parantamisessa. Organisaatioiden yhteistoiminnan kehittäminen ja laadun parantaminen on kaikkien osapuolten yhteinen intressi. (Viestintävirasto 2017a.)

Nämä edellä mainitut seikat ovat muodostaneet Viestintävirastolle tarpeen kehittää omia ja tietoturvallisuuden arviointilaitosten välisiä toimintatapoja. Tämän lisäksi Viestintävirastolla on vastuu viranomaisen roolissa ohjata ja valvoa tietoturvallisuuden arviointilaitoksia.

1.2 Tutkimuskysymykset ja aiheen rajaus

Viestintävirastolla on merkittävä ja yhteiskunnallisesti vaikuttava tehtävä kyberturvallisuuden toimintaympäristössä. On erittäin mielenkiintoista päästä vaikuttamaan ja kehittämään toimintatapoja organisaatioiden välillä. Digitaalinen muutos on voimakasta seuraavien vuosien aikana ja tulee varmuudella aiheuttamaan muutoksia kybertoimintaympäristössä maailmanlaajuisesti.

Tutkimuksen kannalta keskeisiä kysymyksiä ovat:

1. Millaisilla ratkaisuilla toimintatapoja ja kulttuuria Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä voidaan yhtenäistää ja parantaa (nykytila vs. tulevaisuus)?
2. Millaisilla keinoilla toteutetaan viranomaisen valvontavastuu?

Opinnäytetyötä tarkastellaan vain kansallisen tietoturvaviranomaisen eli Viestintäviraston ja tietoturvallisuuden arviointilaitosten näkökulmasta. Pääpaino on Viestintäviraston ja tietoturvallisuuden arviointilaitosten suorittamissa tietojärjestelmien ja tietoliikennejärjestelyiden

vaatimuksienmukaisuuden tarkastuksissa. Kehittämissunnitelma jalkautetaan opinnäytetyöstä erillisenä prosessina arviointilaitoksille opinnäytetyön valmistuttua.

1.3 Tutkimustavoite ja -teoria

Tämän laadullisiin menetelmiin perustuvan toiminnallisen opinnäytetyön tavoitteena on laatia yhteistoiminnan kehittämissuunnitelma Viestintävirastolle ja tietoturvallisuuden arviointilaitoksille. Suunnitelmalla pyritään ensisijaisesti yhtenäistämään Viestintäviraston ja arviointilaitosten toimintatapoja, kirjallisia dokumentteja sekä toimintakulttuuria ja toissijaisesti parantamaan viranomaisen valvontavastuuta.

Opinnäytetyön toteutus jakautuu neljään vaiheeseen. Ensimmäisessä vaiheessa luodaan tutkittavalle aiheelle teoriapohja ja tutustutaan sisällönanalyysin avulla olemassa olevaan dokumentaatioon. Toisessa vaiheessa muodostetaan haastattelurungot ja kerätään tietoa asiantuntijahaastatteluilla. Opinnäytetyön kolmas vaihe koostuu sisällönanalyysin sekä haastatteluiden tuloksista ja niiden analysoinnista. Neljännessä vaiheessa laaditaan kehittämissuunnitelma. Opinnäytetyön tietoperustan ja tiedonkeruu- sekä analysointimenetelmien tarkempi kuvaus on käsitelty luvussa neljä. Kehittämissuunitelma kuvataan luvussa viisi.

1.4 Keskeiset käsitteet

Tietoturvallisuus
Tietoturvallisuus on järjestelyitä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Käytettävyys tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta. (Valtiovarainministeriö 2008.)

Tietojärjestelmätarkastus
Tietojärjestelmän määritelmä kuvaillaan yleensä yhden tai useamman ohjelmiston, tietovarastojen, laitteiden ja palveluiden muodostamaksi kokonaisuudeksi, jonka tarkoitus on helpottaa tai mahdollistaa jotakin toimintaa. Määritelmien mukaan tietojärjestelmä käsittää myös organisationaaliset, sosiaaliset ja inhimilliset ulottuvuudet, kuten ohjelmistoja käyttävät ihmiset. (Pohjonen 2002, 5-6.) Viestintäviraston Kyberturvallisuuskeskuksen yhtenä vastuualueena on viranomaisen turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja käsittelyyn liittyvät tietojärjestelmätarkastukset yrityksissä tai organisaatiossa, jotka käsittelevät tai säilyttävät viranomaisen turvaluokiteltua tietoa. Tietojärjestelmätarkastuksia kuvataan tarkemmin luvussa kolme.

Tietoturvallisuuden arviointilaitos

Tietoturvallisuuden arviointilaitokset ovat yksityisiä yrityksiä. Viestintävirasto ohjaa ja valvoo arviointilaitoksia, jotka tarjoavat viranomaisille ja yrityksille luotettavaa sekä puolueetonta tietoturvallisuuden arviointipalvelua. Kansallinen akkreditointielin FINAS (Finnish Accreditation Service) taas vastaa arviointilaitosten ja sen työntekijöiden riippumattomuuden ja pätevyyden arvioinnista ja seurannasta. Tietoturvallisuuden arviointilaitoksia käsitellään tarkemmin luvussa kolme. (Viestintävirasto 2017b.)

Kyberturvallisuus

Kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa kybertoimintaympäristössä voidaan luottaa ja jossa sen toiminta turvataan. Tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. Luottamus kybertoimintaympäristöön perustuu siihen, että sen toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenettelyjä. Menettelyjen avulla pystytään estämään tietoturvauhkien toteutuminen, ja niiden mahdollisesti toteutuessa estämään, lieventämään tai sietämään niiden vaikutuksia. (Turvallisuuskomitea 2015.)

2 Kybertoimintaympäristö

Kybertoimintaympäristöllä tarkoitetaan ihmisten luomaa digitaalista rinnakkaistodellisuutta, joka yhdistää maailmanlaajuisesti informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli. Jotta valtiot, yritykset ja yksityiset kansalaiset voivat hyödyntää kybertoimintaympäristön tuomat mahdollisuudet, on tärkeä varmistaa, että nämä verkot toimivat mahdollisimman luotettavasti ja turvallisesti. (Ulkoministeriö 2015.)

Kybertoimintaympäristöön kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmaksi yksittäisten ihmisten, yritysten sekä koko yhteiskunnan kannalta. Uhkia muodostavat toimijat ovat ammattimaisempia kuin ennen ja nykyään niihin voidaan laskea kuuluviksi myös valtiolliset toimijat. Tästä huolimatta kybertoimintaympäristö tulee nähdä sekä mahdollisuutena ja voimavarana. Turvallinen kybertoimintaympäristö helpottaa yksilöiden ja yritysten oman toiminnan suunnittelua, mikä lisää taloudellista aktiviteettia. (Turvallisuuskomitea 2015.)

Samaan näkemykseen on päädytty valtioneuvoston puolustusselonteon mukaan. Selonteossa todetaan, että kybertoimintaympäristön merkitys kasvaa. Yhteiskunnan digitalisaatio, teknisten järjestelmien riippuvuus rajat ylittävistä tietoverkoista sekä järjestelmien keskinäiset riippuvuussuhteet ja haavoittuvuudet altistavat yhteiskunnan elintärkeät toiminnot kybervaikuttamiselle. Kyber- ja informaatiovaikuttamista on kohdistettu lähialueillemme ja myös

Suomeen muun muassa kriittistä infrastruktuuria, teollisuuslaitoksia sekä poliittista päätöksentekojärjestelmää ja kansalaisia vastaan. (Valtioneuvoston kanslia 2017.)

2.1 Kyberturvallisuus

Sana kyber tulee kreikan kielestä sanasta kybereo, joka tarkoittaa ohjaamista, opastamista tai hallitsemista. Tässä yhteydessä kuitenkin kyber tarkoittaa digitaalista tai bittien maailmaa. Tähän maailmaan kuuluvat esimerkiksi käyttämäsi internet, sosiaalinen media, erilaiset tietoverkot ja -järjestelmät ja älypuhelimesi sovelluksineen. Kyber on yksittäisenä sanana harvinainen, koska yleensä sen käyttöön liittyy jonkinlainen loppuosa, kuten kyber-rikollisuus, kyber-uhka tai kyber-turvallisuus. (Limnéll ym. 2014, 29-31)

Suomen kyberturvallisuusstrategian mukaan yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä ja yhteiskuntamme elintärkeät toiminnot on pystyttävä turvaamaan kaikissa tilanteissa. Suomi on tietoyhteiskuntana riippuvainen tietoverkkojen- ja järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuville häiriöille. Yhteiskunnan lisääntynyt tietointensiivisyys, tieto- ja viestijärjestelmien keskinäinen integraatio, kaikille avointen tietoverkkojen käyttö sekä lisääntynyt riippuvuus sähköstä ovat asettaneet uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvallisuudelle. (Turvallisuuskomitea 2015.)

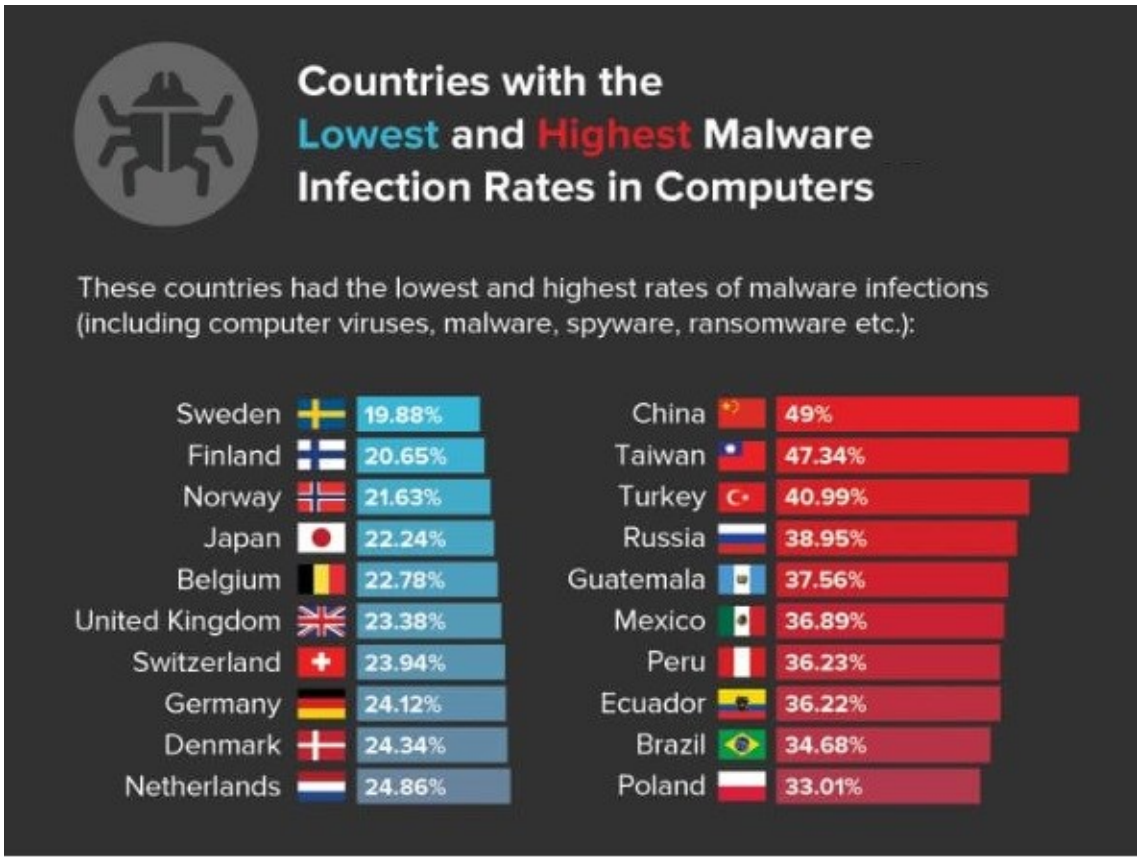
Valtioneuvoston puolustusselonteossa myös Aalto-yliopiston professori Jarno Limnéll kertoo, että Suomi on hyvin riippuvainen kybertoimintaympäristöstään. Kyberturvallisuus ei ole pelkästään uhkien ja riskien hallintaa. Kyber sanana viittaa sähköiseen tiedonkäsittelyyn, tiedonsiirtoon ja tietojärjestelmiin. Nykypäivän yhteiskuntien yhdeksi kilpailukykytekijäksi on noussut turvallisuus. Yhteiskunnan vakaus, sen turvallisuudesta huolehtiminen ja varautumiskeinojen kunnossa pitäminen ovat houkuttelevia tekijöitä, kun pohditaan investointikohteita. Suomen vahvaa kansainvälistä luottamuspääomaa ja kyberturvallisuusosaamista pitää pystyä hyödyntämään. Kyberturvallisuus tulee nähdä positiivisena kilpailukyvyn etuna vaikka kybervaikuttaminen informaatiovaikuttamisen, tietomurtojen, tietovuotojen tai poliittisen vaikuttamisen myötä ovatkin lisääntyneet viime vuosina. (Valtioneuvoston kanslia 2017a.)

Suomessa kyberturvallisuustyötä on tehty 1990-luvulta lähtien. Kyberturvallisuuden vastuuta on jaettu yksilöistä valtionhallintoon. Valtiolla on ollut erityisvastuu koko yhteiskunnan toimivuuden säilymisestä. Päävastuun toiminnasta ovat kantaneet keskeiset turvallisuusviranomaiset, joita käsitellään tarkemmin myöhemmin tässä opinnäytetyössä. (Valtioneuvoston kanslia 2017b) Viestintäviraston ja Kyberturvallisuuskeskuksen tehtävänä on ollut kehittää ja valvoa viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Kyberturvallisuuskeskus tuottaa tilannekuvaa tietoturvallisuuden ilmiöistä ja tiedottaa niistä sekä toimii tietotur-

vallisuusviranomaisena. Viestintäviraston tehtävät kuvataan tarkemmin seuraavassa pääluvussa. (Viestintävirasto 2017c.)

2.2 Kybertilastot

Comparitech Limited on brittiläinen yhtiö, jonka ensisijainen tehtävä on auttaa kuluttajia Iso-Britanniassa ja Yhdysvalloissa tekemään oikeita ratkaisuja kyberturvatuotteiden (VPN, antivirus, pilvipalvelut, salasanaohjelmat) suhteen. Ensisijaisen tehtävänsä ohessa Comparitech ylläpitää internetsivustoa comparitech.com, joka tarjoaa tietoa, työkaluja ja vertailuja erilaisista kybertilastoista. Tämän vuoden helmikuussa tehdyn tutkimuksen (Kuvio 1) mukaan maailman kyberturvallisimpien maiden joukossa kärjessä oli Ruotsi (19,88%), Suomi (20,65%) ja Norja (21,63%). Eniten haittaohjelmatartuntoja havaittiin Kiinassa (49%), Taiwanissa (47,34%) ja Turkissa (40,99%). Tilastojen kärkimaat tulivat pääsääntöisesti Euroopasta. Suomen kannalta merkittävien maiden kuten Venäjän haittaohjelmatartuntojen luku oli maailman neljänneksi korkein (38,95%) vuonna 2017. (Comparitech Limited 2017.)



Kuvio 1: Haittaohjelmatartuntojen tilasto (Comparitech Limited 2017)

Microsoftin asiakkailleen, yhteistyökumppaneilleen ja teollisuudelle tekemän 22:n Security Intelligence Report (SIR)-raportin mukaan vuoden 2017 ensimmäisen neljänneksen (3/2017) kyberturvallisimpia maita olivat Japani (1,1%), Ruotsi (1,8%) ja Suomi (2,0%). Heikoimmin pär-

jäsivät Bangladesh (26,6%), Pakistan (26,2%) ja Indonesia (25,6%). Venäjän luku Microsoftin tekemässä tutkimuksessa (12,0%) oli melko maltillinen. Prosenttiluku kuvaa haittaohjelmahavaintojen lukumäärää. Näitä tilastoja tarkastellessa on otettava huomioon, että tutkimuksen tilastojen lukuihin on laskettu vain Microsoftin turvallisuustuotteita käyttävät tietokoneet. Raportin tilastoja varten Microsoftin turvallisuustuotteet skannaavat yli 400 miljardia sähköpostia, 18 miljardia internetsivustoa sekä käsittelee yli 450 miljardia todennusta joka kuukausi. Otanta kattaa noin 600 miljoonaa tietokonetta maailmanlaajuisesti. (Microsoft 2017.)

2.3 Kybertulevaisuus

Uusia teknologioita kehitetään nyt radikaalimmin ja nopeammin kuin koskaan aikaisemmin. Teknologioiden avulla on tarkoitus auttaa ja tuoda helpotuksia kansalaisten arkeen. Hyötyjen ohella nämä uudet laitteet tai palvelut tuovat mukanaan haittoja. Erilaisia tutkimuksia asian suhteen on tehty jo useita vuosia. Alla on kuvattu kybertulevaisuuteen vaikuttavien ilmiöiden tutkimuksia kansallisella tasolla, EU-tasolla ja kansainvälisesti.

Valtioneuvoston kanslian tekemän tutkimuksen "Suomen kyberturvallisuuden nyky- ja tavoitetilasta" mukaan Suomi pyrkii vuoteen 2020 mennessä tilaan, missä kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus. Tutkimuksen perusteella Suomi ei tällä hetkellä ole edelläkävijä kyberuhkiin varautumisessa tai niiden aiheuttamissa häiriötilanteissa. Suurimmiksi kehittämiskohteiksi tutkimus tunnisti kyberturvallisuuden strategisen johtamisen Suomessa, kybertilannekuvan ja analysointikyvykkyyden kehittämisen ja kansallinen kyberresilienssin. Suomen kyberturvallisuuden edelläkävijyys ja kyvykkyys tulevaisuudessa on kuitenkin omissa käsissämme. (Valtioneuvoston kanslia 2017b.)

Tutkimus osoittaa myös, että viime vuosina olemme tasaisesti saaneet tietoa erilaisista kiristyshaittaohjelmista, haavoittuvuuksista ja palvelunestohyökkäyksistä. Näistä kuuluisimpina ovat Mirai-bottiverkon, ennätyksellisen suuren kohdistetetun palvelunestohyökkäyksen, leviäminen maailmanlaajuisesti vuonna 2016 ja yksi maailman yleisimmin WIFI-verkkojen salaukseen käytetty WPA2-protokolla, josta löydettiin vakava haavoittuvuus vuonna 2017. Nopeasti kasvava äly- ja IoT-laitteiden määrä antaa houkuttelevan kohteen kyberrikollisille. Motivaationa heillä on useasti raha, maine, vaikuttaminen (liiketoiminnallinen, taloudellinen tai poliittinen) tai toimeksianto. Kuka tahansa pystyy esimerkiksi nykypäivänä ostamaan palvelunestohyökkäyksiä ja kohdistamaan niitä haluamaansa kohteeseen. Puhumattakaan jos tekijä on valtio, jolla on tahtotila, rahaa ja resursseja. Tutkimuksen mukaan tulevaisuudessa kyberturvallisuutta eniten muokkaavat laaja-alaiset kyberhyökkäykset ja hakkeroinnin teollistuminen sekä tietoturvamarkkinoiden monimutkaisuus ja hajautuneisuus. Tietovuotojen kustannusten on myös ennustettu kasvavan ja yhteensopivien tietoturvateknologioiden ja tietoturvaammattilaisten puute on ilmeinen. Tulevina vuosina kyberturvarikollisten suurimpina uusien ja vaarallisten mahdollisuuksien alueina nähdään esineiden Internet, pilvipalvelut, big data

(erittäin suuri, järjestelemätön ja jatkuvasti lisääntyvä tietomassa) ja mobiliteetti. (Valtioneuvoston kanslia 2017b.)

European Union Agency for Network and Information Security (ENISA) on ilmaissut huolensa nopeasti kasvavien ilmiöiden, kuten esineiden Internet ja tekoäly, joilla on potentiaalinen vaikutus arkeemme tulevaisuudessa muuttamalla ihmisten ja koneiden käyttäytymistä. Kehittyvät teknologiat avaavat hyvinvointia edistäviä sosioekonomisia mahdollisuuksia mutta tuovat mukanaan sääntelyyn, etiikkaan ja vastuuseen liittyviä haasteita. (Enisa 2017.)

Samalla tavalla Yhdysvaltojen tiedustelupalveluiden vuotuisessa uhkaraportissa nousevat teknologiat saavat paljon huomiota. Uhkaraportin mukaan esineiden Internetin ja tekoälyn lisäksi esille nousevat geenimuokkausteknologiat, joilla voidaan kehittää uusia lähetysmistapoja lääketieteeseen tai ihmisten terveyteen. Tietotekniikka ja sen johdannaisten kehittyminen mainitaan raportissa myös yhtenä tulevaisuutta häiritsevänä teknologiana. Raportin mukaan tietokoneiden teho tuplaantuu joka toinen vuosi ja vuoteen 2020 mennessä perinteiset informaatioteknologian turvallisuustekijät eivät ole enää hyödyllisiä. (DNI 2017.)

Puolustusvoimien tutkimuslaitos on tehnyt tutkimuskatsauksen kvanttiteknologiasta ja kyberturvallisuudesta. Aalto-yliopiston tutkija Mikko Möttösen mukaan kvanttiteknologia perustuu fysiikkaan ja nopeaan laskentaan, jolla kyetään tulevaisuudessa ratkaisemaan monimutkaisia ongelmia äärimmäisen nopeasti (Teknologiateollisuus 2017.). Kehittyvän kvanttiteknologian on jo vuosia puhuttu tulevaisuudessa mullistavan kyberturvallisuusympäristön aiheuttamalla uusia uhkia mutta myös parantamalla tiedonvälityksen turvallisuutta. Kvanttilaskennan käyttö tulevaisuuden supertietokoneissa on aiheuttanut huolia ja kerännyt julkisuutta, sillä monet nykyisistä salausmenetelmistä voidaan murtaa, kun tarpeeksi suuren laskentatehon omaava kvanttitietokone on saatu kehitettyä. Tämä uhka koskee esimerkiksi RSA-salausta, DSA-allekirjoitusta ja Diffien-Hellman avaintenvaihtoa. Tällaista kvanttitietokonetta ei vielä ole olemassa mutta tutkimuskatsauksen mukaan tämä voisi olla melko optimistisesti käytettävissä viiden vuoden päästä, kymmenen vuoden päästä jo hyvinkin mahdollista ja kahdenkymmenen vuoden päästä kvanttitietokoneen saatavuus on lähes varmaa. (Puolustusvoimien tutkimuslaitos 2017.)

Kyberturvallisuus on tunnistettu tulevaisuuden suureksi voimavaraksi niin hyvässä kuin pahassakin. Etenkin valtiolliset toimijat ja teollisuuden suuryritykset ovat hyvinkin tietoisia ja kiinnostuneita kybertulevaisuuden tuomista tulevaisuuden mahdollisuuksista ja uhista. Kvantti-, lohkoketju- ja IoT-teknologia sekä tekoäly ja robotiikka ovat tulevaisuutta varmuudella muokkaavia tekijöitä. Valtioille ja pk-yrityksille on yhä tärkeämpää saavuttaa ja ylläpitää tietty tietoturvallisuuden taso. Ihmiskunnan on monelta eri taholta todettu kuitenkin muuttuvan seuraavan 30 vuoden aikana enemmän kuin viimeiseen 300 vuoteen. Hyvä esimerkki varautu-

misesta tulevaisuuteen on Jyväskylässä jo vuodesta 2013 alkaen järjestetty valtionhallinnon viranomaisten yhteinen kyberharjoitus. Harjoituksella on pyritty luomaan mahdollisimman realistinen ympäristö internetin palveluineen ja pahoine tyyppeineen. Harjoituksen tarkoitus on mitata organisaatioiden omaa suorituskykyä ja yhteistyötä viranomaisten kesken. (Ruotuväki 2017.)

3 Viestintäviraston toimintaympäristö

Viestintävirasto on perustettu (Kuvio 2) vuonna 1988, jolloin se toimi vielä Telehallintokeskuksen nimellä. Telehallintokeskuksen perustaminen katsottiin tarpeelliseksi, koska telealan kilpailun käynnistäessä oli tarpeellista erottaa viranomais- ja liiketoiminta toisistaan. Vuonna 2001 otettiin käyttöön uusi nimi Viestintävirasto, sillä toimialan nopean kehittymisen vuoksi sähköisen viestinnän ja tietoyhteiskuntapalvelujen yleinen hallintoviranomainen, eikä entinen nimi enää vastannut viraston tehtäväkuvaa ja jatkuvasti laajenevaa toimialaa.

Viestintämarkkinat ovat koko viraston toimiajan eläneet voimakkaassa murroksessa, jossa keskeisinä muutostekijöinä ovat olleet Internetin ja viestintäpalveluiden vahva kasvu, globalisaatio sekä sähköisen asioinnin ja kaupankäynnin mukanaan tuomat haasteet. Viestintäviraston historian suurimpana muutoksena voidaan pitää nyt käsillä olevaa televiestinnän, informaatioteknologia ja mediaviestinnän konvergenssiä. Sen toteutumista ja yleistymistä edesauttavat jatkuva Internetin käytön vahva kasvu ja digitalisaatio. (Viestintävirasto 2017d.)

Jatkuvasti laajenevan toimialan, Internetin käytön voimakkaan kasvun ja digitalisaation myötä myös Viestintävirasto on joutunut vastaamaan uusiin haasteisiin kyberilmiöiden kansainvälistymisen ja runsauden myötä. Uusia toimintoja, kuten Computer Emergency Response Team (CERT), National Communications Security Authority (NCSA) ja Public Regulated Service (PRS) on perustettu. Kyberturvallisuuskeskus, joihin edellä mainitut toiminnot nykyään kuuluvat, aloitti toimintansa virallisesti vuonna 2014.

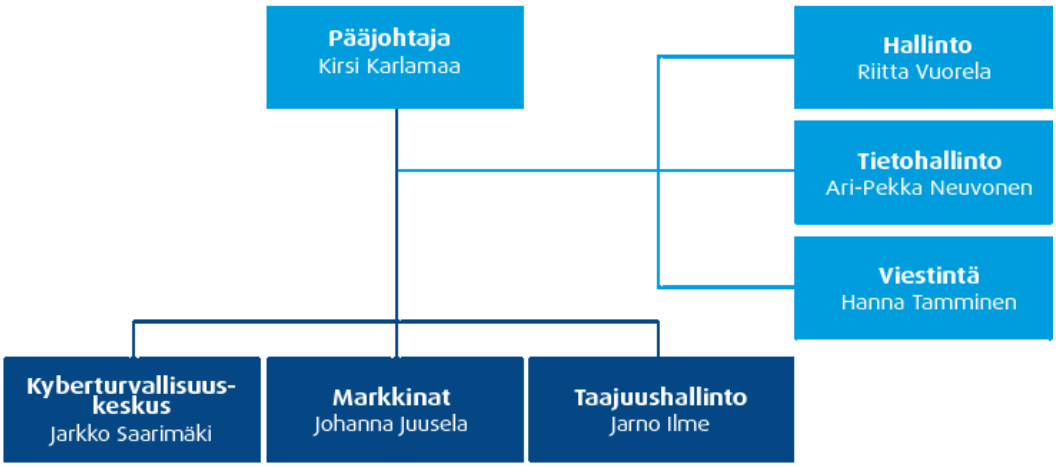
Kuvio 2: Viestintäviraston virstanpylväät (Viestintävirasto 2017)

3.1 Viestintävirasto

Nykyään Viestintävirasto on liikenne- ja viestintäministeriön alaisuudessa toimiva asiantuntijavirasto, jonka tehtävänä on huolehtia siitä, että Suomessa on monipuoliset, toimivat ja turvalliset viestintäyhteydet. Viestintävirasto rakentaa toiminnallaan luotettavaa tietoyhteiskuntaa sekä turvaa viestintäpalveluiden käyttäjien aseman ja oikeudet takaamalla yhteiskunnan, elinkeinoelämän ja kansalaisten käyttöön muun muassa:

- Nopeat ja turvalliset tietoliikenneyhteydet
- Toimivat ja tehokkaat viestintämarkkinat
- Tehokkaassa käytössä olevat taajuudet ja tunnukset
- Laadukkaat ja kohtuuhintaiset viestintäpalvelut
- Monipuoliset sähköiset mediapalvelut
- Objektiivista tietoa viestintämarkkinoiden ja -palveluiden kehityksestä, hinnoittelusta ja palvelutasosta

Helsingissä sijaitseva Viestintävirasto työllistää noin 240 juridiikan, talouden ja tekniikan asiantuntijaa kuudella eri toimialalla (Kuvio 3). Viestintäviraston sisäiset toimialat Hallinto, Tietohallinto ja Viestintä huolehtivat tehtäviensä mukaisesti viraston sisäisen toiminnan takaamisesta. Viestinnällä on sisäisten tehtävien lisäksi myös luontainen rooli viraston ulkoisessa viestinnässä. Kyberturvallisuuskeskus, Markkinat ja Taajuushallinto taas ovat Viestintäviraston ulkoisia toimialoja, jotka toimivat viraston asiakasrajapinnassa huolehtien alla kuvatuista toimialakohtaisista tehtävistä. (Viestintävirasto 2017e.)



Kuvio 3: Viestintäviraston organisaatio (Viestintävirasto 2017)

Kyberturvallisuuskeskuksen tehtävänä on kehittää viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta, lisätä yhteiskunnan luottamusta sähköisten palveluiden käyttöön vahvistamalla kansallista tietoturvaa ja terävöittää yleisten viestintäverkkojen ja -palveluiden tietoturvallisuuden sekä varautumisen teknistä ohjausta ja valvontaa. Kybertur-

vallisuuskeskuksen operatiivinen toiminta muodostuu kansallisesti ja kansainvälisesti havaittujen tietoturvapoikkeamien ja -uhkien selvittämisestä (CERT), tietojärjestelmien ja tietoliikennejärjestelyiden vaatimuksenmukaisuuden tarkastuksista (NCSA), yleisten viestintäverkkojen ja -palveluiden tietoturvallisuuden sekä varautumisen ohjauksesta ja valvonnasta sekä kansallisen kyberturvallisuuden tilannekuvan ylläpitämisestä ja Galileo-satelliittipaikannusjärjestelmän (PRS) julkisesti säännellyn palvelun hallinnoinnista. (Viestintävirasto 2016b.)

Markkinat toimiala pyrkii takaaman jokaiselle suomalaiselle oikeuden viestinnän peruspalveluihin. Toimialan tehtävänä on muun muassa käsitellä viestintäverkkojen ja -palveluiden toimivuutta, seurata viestintätoimialan ja sen toimintaympäristön yleistä markkinaseurantaa sekä valvoa huomattavan markkinavoiman käyttöä. Taloudellisella valvonnalla varmistutaan siitä, että kilpailu markkinoilla on tasapuolista, toimivaa sekä hinnoittelu- ja toimintavelvoitteita noudattavaa. Varmistamalla laadukkaat ja toimivat tietoliikenneyhteydet, edistämällä palveluntarjoajien välistä kilpailua, mahdollistamalla uusien verkkojen rakentamista voidaan ihmisille tarjota yhä kehittyneempiä palveluita, joista jokainen voi valita itselleen sopivimman. (Viestintävirasto 2017f.)

Taajuushallinto toimialan tehtävänä on varmistaa langattoman viestinnän sujuvuus arjessa ja auttaa uusien taajuuksia käyttävien innovaatioiden kehittämisessä ja käyttöönotossa. Kansainvälisesti toimialan tehtävänä on varmistaa Suomen etu kansainvälisessä päätöksenteossa. Riittävien, tasapuolisten ja häiriöttömien radiotaajuuksien varmistaminen on kaikkien etu nopeasti digitalisoituvassa yhteiskunnassamme. (Viestintävirasto 2017f.)

3.2 Tietojärjestelmien ja tietoliikennejärjestelyiden tarkastukset

Ruotsi ja Suomi ovat molemmat sitoutuneet omissa kansallisissa kyberturvallisuusstrategioissaan kehittämään ja vahvistamaan kyberturvallisuuttaan. Kyberturvallisuus koskettaa koko yhteiskuntaa ja jokaisen on otettava siitä vastuuta. Molemmat maat mainitsevat strategioissaan yhdeksi painopisteeksi verkko-, järjestelmä- ja tuoteturvallisuuden parantamisen niin kansalaisten, teollisuuden kuin valtionhallinnonkin piirissä. Kyberturvallisuuden tarve on tiedostettu ja valtiot ovat priorisoineet strategian jalkauttamisen. Strategiaa noudatetaan tarkkojen suunnitelmien mukaisesti ja toimintaympäristön kehitystä seurataan. (Ministry of Justice of Sweden 2017.)

Suomessa Viestintäviraston sisällä tietojärjestelmien ja tietoliikennejärjestelyiden tarkastustehtävät on annettu Kyberturvallisuuskeskuksen NCSA-toiminnolle, jonka tehtävänä on vastata turvaluokitellun aineiston sähköisen tiedonsiirron ja -käsittelyn liittyvistä turvallisuusasioista. Viestintäviraston NCSA-toiminto on osa Suomen turvallisuusviranomaisorganisaatiota. Viestintävirasto toimii määrättynä turvallisuusviranomaisena (Designated Security Authority, DSA) ja

kansallisena tietoturvaviranomaisena. Kansainvälisten tietoturvavelvoitteiden kokonaisvastuu on ulkoministeriön National Security Authority-yksiköllä (NSA), joka toimii kansallisena turvallisuusviranomaisena. NSA:n tehtävänä on ohjata kansallista toimintaa, vastata kansainvälisten turvallisuussopimusten valmistelusta sekä ohjata ja valvoa, että kansainvälisesti erityissuojattavat (EU, NATO ym.) tietoaineistot suojataan ja niitä käsitellään asianmukaisesti. Muita määrättyjä turvallisuusviranomaisia (DSA) ovat puolustusministeriö, suojelupoliisi ja pääesikunta. (Viestintävirasto 2017g.)

Alla olevassa kuviossa (Kuvio 4) on kuvattu Viestintäviraston tehtävämääriä vuonna 2016. Viestintäviraston suorittamia tietojärjestelmätarkastuksi tehtiin yhteensä 88 kappaletta. Tehtävämäärä on valtava suhteutettuna NCSA-toiminnon henkilöresurssiin.

Kuvio 4: Viestintäviraston tilastot vuonna 2016 (Viestintävirasto 2017)

Viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit perustuvat lakiin kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), turvallisuusselvityslakiin (726/2014) ja lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinnista (1406/2011). Arviointi- ja hyväksyntäprosessit edellyttävät tilaajaorganisaatiolta tiettyjä toimenpiteitä ennen tarkastusta ja perusteltua tarvetta käsitellä kansallista tai kansainvälistä salassa pidettävää tietoa. Tilaajaorganisaation näkökulmasta arviointiprosessi on hieman erilainen kuin hyväksyntäprosessi. Prosessien paremmin havainnollistamiseksi prosessit on kuvattu erillisillä kaaviolla alapuolella.

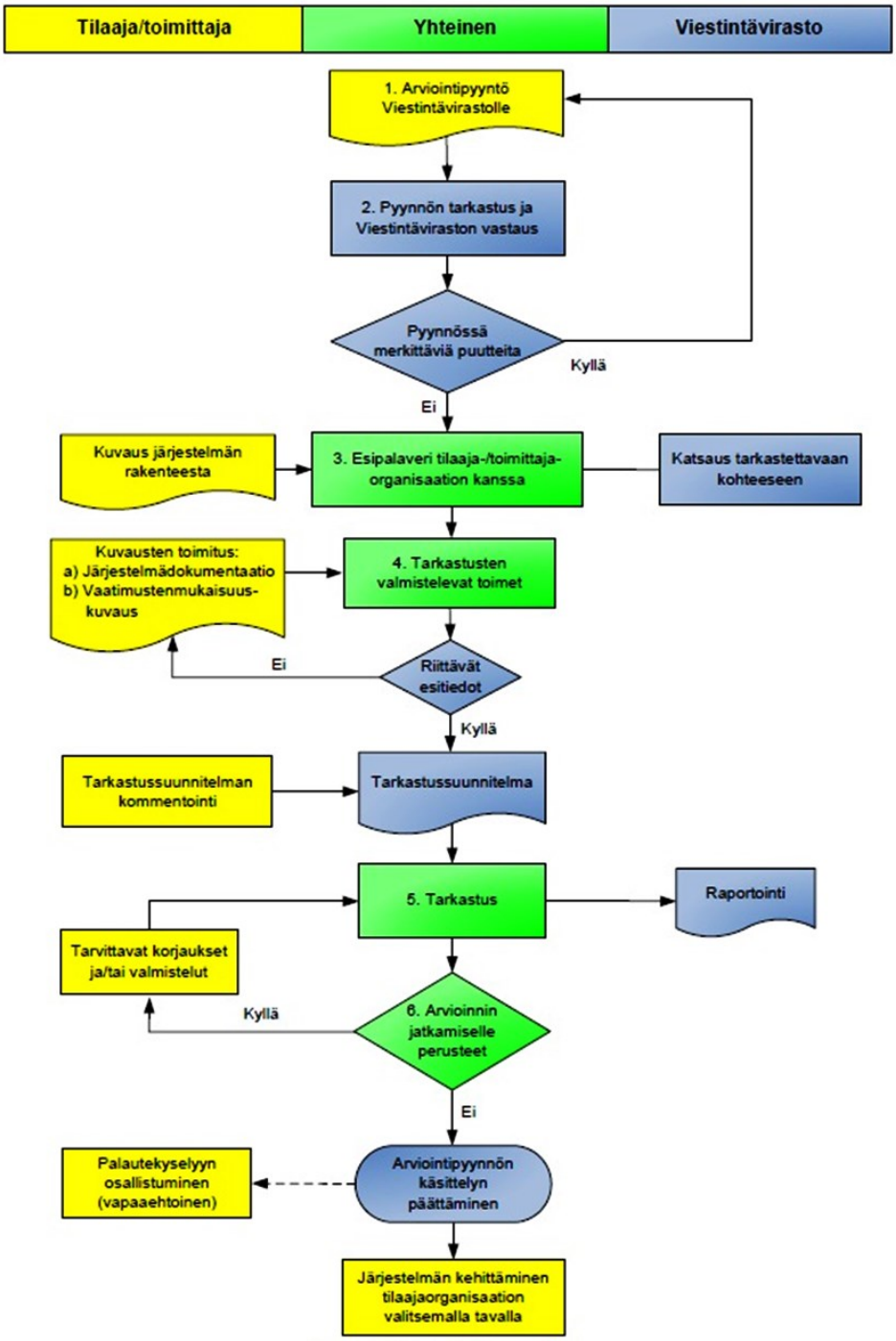
Tarkastuksella tarkoitetaan riippumattoman tahon suorittaman kohteen, sen toiminnan ja toiminnan tulosten yleensä määräajoin tapahtuvaa tutkimista sen selvittämiseksi, vastaako järjestelmä tai sen osa siihen kohdistuvia vaatimuksia. (Viestintävirasto 2017h.)

Arvioinnilla tai arviointiprosessilla (Kuvio 5) tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, miltä osin järjestelmä täyttää siihen kohdistuvat vaatimukset. Arviointiprosessi on usein hyväksyntäprosessin osaprosessi. (Viestintävirasto 2017h.)

Arviointipyynnöllä ja siitä saatavalla lausunnolla tilaajaorganisaatio saa realistisen ja puolueettoman kuvan oman tietoturvallisuutensa tasosta. Tämän jälkeen tilaajaorganisaatio voi

kehittää omaa turvallisuuttaan valitsemallaan tavalla. Arviointipyyntö ei velvoita tilaajaorganisaatiota mihinkään, toisin kuin hyväksyntäprosessi.

Tietoturvallisuuden arviointilaitokset tarjoavat tietoturvallisuuden arviointipalveluita perustuen lakiin tietoturvallisuuden arviointilaitoksista (1405/2011). Tämän myötä toiminta mahdollistaa vain arviointiprosessinmukaisia arviointeja. Viestintävirasto voi tietoturvallisuuden arviointilaitoksien suorittamien arviointien perusteella hyödyntää tehtyjä arviointeja omassa hyväksyntäprosessissaan.



Kuvio 5: NCSA-toiminnon arviointiprosessikuvaus (Viestintävirasto 2017)

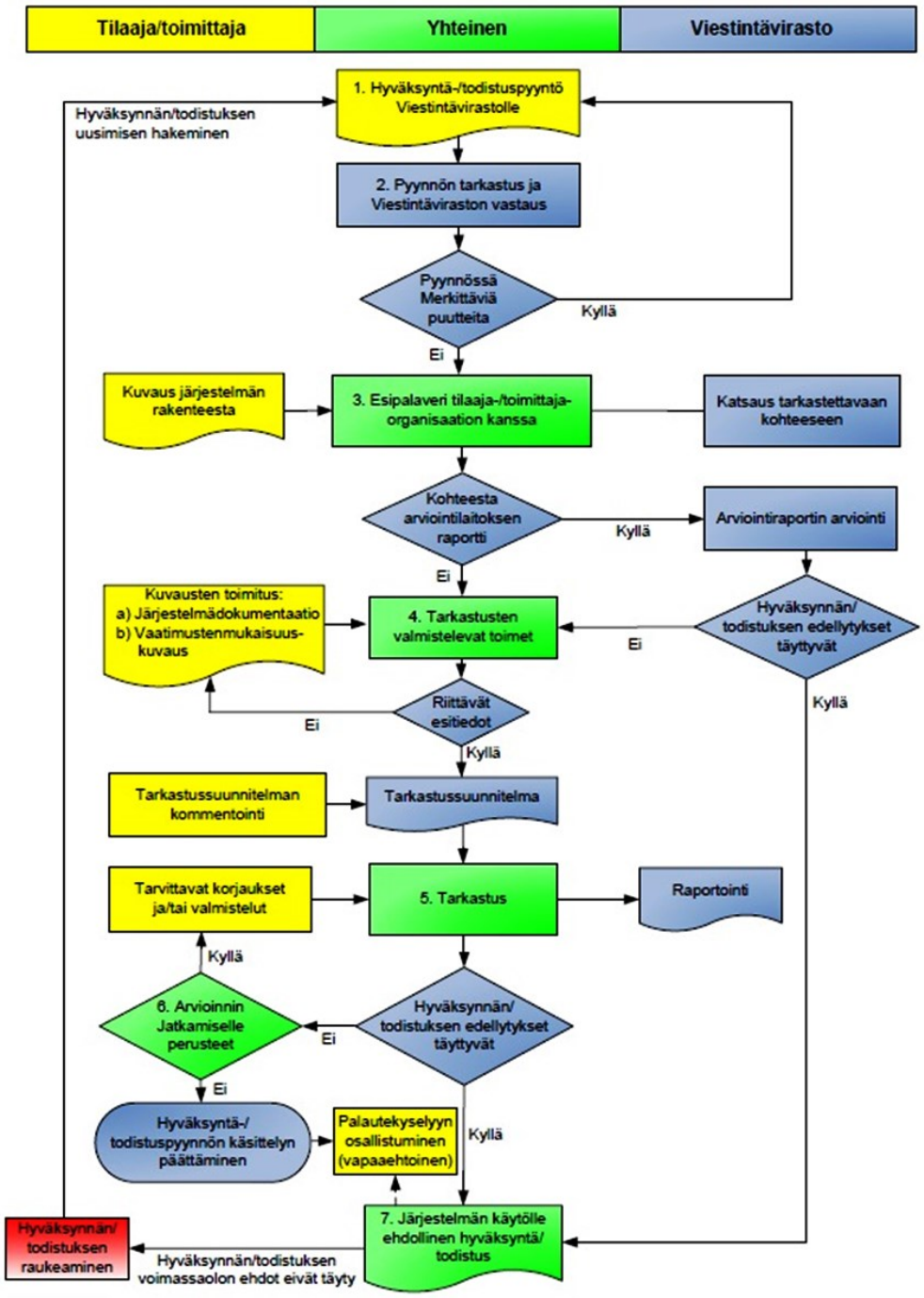
Hyväksynnällä tai hyväksyntäprosessilla (Kuvio 6) tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, että järjestelmä on hyväksytty käytettäväksi määritellyssä turvallisuusluokassa. Prosessi määrittelee myös, että tiettyä turvallisuuden takaavaa toimintatapaa noudatetaan käyttöympäristössään ja hyväksyttävällä riskitasolla. Tämä edellyttää, että hyväksytyt hallinnolliset, fyysiset ja tekniset menettelyyn liittyvät turvatoimet on toteutettu. (Viestintävirasto 2017h.)

Hyväksyntäprosessissa on valtaosin yhteneväiset suoritteet kuin arviointiprosessissa mutta se sisältää niiden lisäksi seitsemännen suoritteen. Arviointi- ja hyväksyntäprosessin vaiheet on kuvattu seuraavasti Viestintäviraston ohjeessa:

1. Arviointi-, todistus- tai hyväksyntäpyyntö Viestintävirastolle
2. Viestintäviraston vastaus
3. Esipalaveri tilaajaorganisaation kanssa
4. Tarkastusten valmistelevat toimet
5. Tarkastus
6. Arvioinnin jatkamisen perusteet
7. Järjestelmän käytölle ehdollinen hyväksyntä tai todistus (vain hyväksyntäprosessissa)

Jos tilaajaorganisaatio hakee hyväksyntäprosessissa järjestelmälleen ehdollista hyväksyntää tai todistusta tarkoittaa se sitä, että tilaajaorganisaatio sitoutuu ylläpitämään hyväksytyn tietoturvallisuuden tason. Viestintäviraston myöntämä ehdollinen hyväksyntä tai todistus on voimassa lähtökohtaisesti kolme vuotta. Mikäli tarkastetussa kohteessa tai organisaatiossa tapahtuu merkittäviä turvallisuuteen vaikuttavia muutoksia, hyväksyntä tai todistus raukeaa. Merkittävinä muutoksina voidaan pitää esimerkiksi verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tilaajaorganisaatio on velvollinen ilmoittamaan merkittävistä muutoksista Viestintävirastolle. (Viestintävirasto 2017h.)

Arviointiprosessi voidaan toteuttaa myös vain osittain, kuten esimerkiksi rajaamalla arviointi koskemaan vain hallinnollisen, fyysisen tai teknisen tietoturvallisuuden osuutta kohteesta. Vaihtoehtoisesti voidaan myös määritellä tietty ympäristö, sovellus tai alue, jota arviointi koskee. Hyväksyntäprosessi taas suoritetaan kokonaisuudessaan ympäristössä, jota hyväksyntä koskee. Tällöin prosessi ottaa huomioon hallinnollisen, fyysisen ja teknisen tietoturvallisuuden ja mahdollisesti kansainvälisistä vaatimuksista tulevat erityistarpeet. Tietoturvallisuuden arviointilaitokset voivat tehdä arviointeja myös "ei arviointilaitoksena", jolloin heitä ei velvoita Viestintäviraston ohjeen määrittelemät soveltamisohjeet, arviointimenetelmät tai muut vaatimukset. Tällöin tilaajaorganisaatio ei kuitenkaan voi hakea Viestintävirastolta hyväksyntää tai todistusta järjestelmälleen. Tämä toiminta on mahdollistettu terveen liiketoiminnan ja kilpailukyvyn ylläpitämiseksi. (Viestintävirasto 2016a.)



Kuvio 6: NCSA-toiminnon hyväksyntäprosessikuvaus (Viestintävirasto 2017)

3.3 Tietoturvallisuuden arviointilaitokset

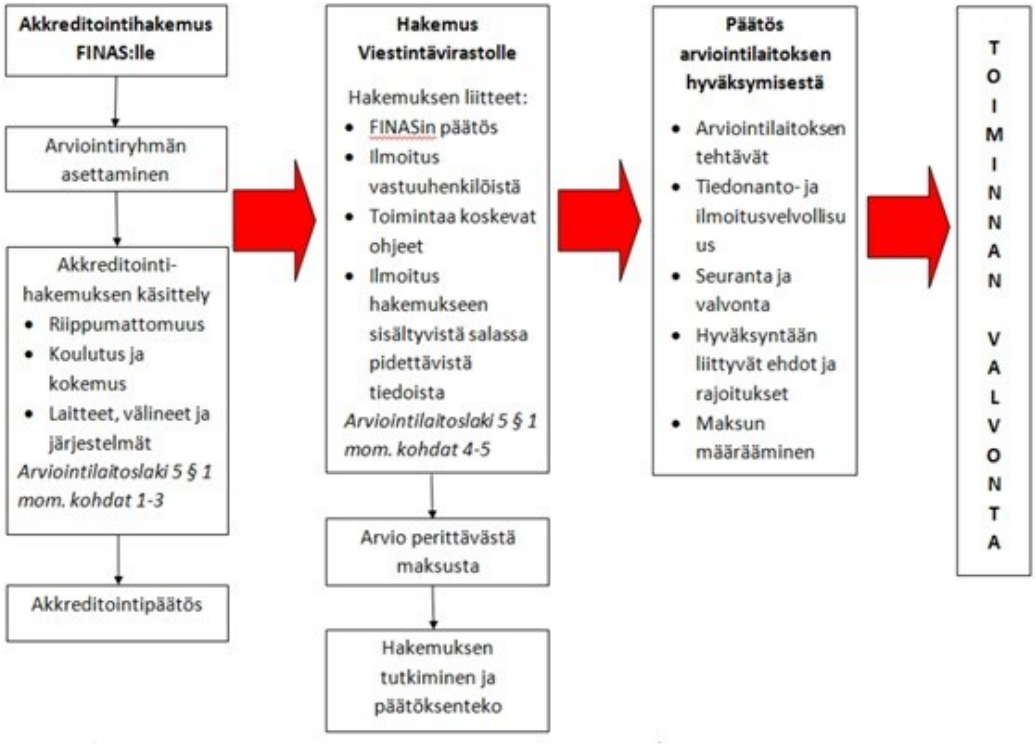
Tietoturvallisuuden arviointilaitokset ovat Viestintäviraston hyväksymiä, valvonnan ja ohjauksen alla olevia yksityisiä yrityksiä, jotka tarjoavat viranomaisille ja yrityksille luotettavaa ja puolueetonta tietoturvallisuuden arviointipalvelua. Tietoturvallisuuden arviointilaitosten suorittaman arvioinnin avulla yritykset voivat todistaa, että yrityksen toiminta täyttää tietotur-

vallisuusvaatimukset tai osoittaa kansalliselle viranomaiselle, että sen toiminnassa on toteutettu määrätty tietoturvallisuuden taso. Todistus tai sertifikaatti, jota monesti nykyään jopa vaaditaan, voi edesauttaa yritysten vientiä sekä kansallisilla kuin kansainvälisillä markkinoilla. (Viestintävirasto 2017b.)

Tieturvallisuuden arviointilaitosten ohjaus ja valvonta on jaettu kahden viranomaisen kesken. Viestintävirasto hyväksyy ja ohjaa sekä valvoo arviointilaitosten toimintaa. Kansallinen akkreditointielin FINAS arvioi tietoturvallisuuden arviointilaitosten riippumattomuuden ja arviointilaitosten työntekijöiden pätevyyden. FINAS vastaa myös omalta osaltaan arviointilaitosten pätevyyden seurannasta. Myös pätevyysalueiden valvonta on jaettu. Viestintävirasto valvoo Katakri- sekä Vahti-pätevyysalueiden arviointien toteutumista ja FINAS puolestaan ISO-standardin mukaisia arviointeja. (Viestintävirasto 2017b.)

Viestintäviraston Kyberturvallisuuskeskukseen on sijoitettu erityisasiantuntijan virka. Erityisasiantuntijan toimenkuvauksessa yhtenä tehtävänä on kuvattu tietoturvallisuuden arviointilaitosten ja Viestintäviraston yhteistoiminnan kehittäminen, koordinointi ja valvonta. Tehtävästä on käytetty myös arviointilaitoskoordinaattori nimikettä. Tässä opinnäytetyössä arviointilaitoskoordinaattori nimikkeellä tarkoitetaan yllä mainittua tehtävää.

Hyväksytyksi arviointilaitokseksi hakeutuminen (Kuvio 7) on yrityksille vapaaehtoista. Kiinnostusta lisännee kuitenkin se, että yhä useammassa laissa, asetuksessa tai erityissäännöksessä edellytetään viranomaisen tai hyväksytyn arviointilaitoksen suorittamaa tietoturvallisuuden tarkastusta. Arviointilaitosten pitää aluksi tehdä akkreditointihakemus FINAS:lta toiminnalleen, jonka vaatimusten (mm. ISO 27001) täyttäminen on edellytys hyväksytyn päätöksen saamiseksi. Samanaikaisesti on hyvä tehdä myös arviointilaitoshakemus Viestintävirastolle, joka suorittaa arviointilaitokseksi hakeutuvan yrityksen hallinnollisen ja teknisen tietoturvaosaamisen tason arvioinnin. Prosessit ovat raskaita ja saattavat viedä yllättävän paljon aikaa. Saatuaan tiedon arviointilaitoksen hakemuksesta, Viestintävirasto pyytää Suojelupoliisia antamaan yrityksen tilaturvallisuudesta ja yrityksen johdosta lausunnot. Edellyttäen, että arviointilaitokseksi hakeutuva yritys täyttää akkreditointihakemuksessa olevat osaamisalueet, Suojelupoliisin tilaturvallisuustarkastuksen ja yritysjohtoa koskevat vaatimukset sekä Viestintäviraston vaatimukset voidaan aloittaa hyväksyntäpäätöksen tekeminen. Hyväksyntäpäätös itsessään on nopeahko hallinnollinen toimenpide mutta mikäli viranomaisten vaatimusten täyttymisten suhteen tulee ongelmia, voi matka hyväksytyksi arviointilaitokseksi olla todella pitkä. Aluksi hyväksytty arviointilaitos saa pätevyysalueekseen ISO 27001-standardin mukaisesti suoritettavat tarkastukset mutta arviointilaitos voi hakea tietoturvallisuuden osaamistasonsa mukaan lisäpätevyysalueita (VAHTI, Katakri), jotka myöntää Viestintävirasto. Pätevyysalueiden lisääminen vaatii aina oman erillisen hakemuksensa ja vastaavanlaiset tarkastukset kuin arviointilaitokseksi hakeutumisessa.



Kuvio 7: Arviointilaitoksen hyväksymismenettely (Viestintävirasto 2017)

Pätevyysalueet luokitellaan suojaustasoittain. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa määrittelee suojaustasojen perusteet. Asetus määrittelee suojaustasot korkeimmasta, suojaustaso I, matalimpaan, suojaustaso IV. Tietoturvallisuuden arviointilaitokset saavat pätevyysalueillensa (ISO 27001) aluksi hyväksynnän suojaustasolle IV. Asetus määrittelee suojaustaso IV:n seuraavasti: Suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 2010.). Käytännössä tämä tarkoittaa siis sitä, että aluksi hyväksytty tietoturvallisuuden arviointilaitos voi tehdä arviointeja vain kohteisiin, joissa käsitellään tai säilytetään viranomaisen salassa pidettävää tietoa korkeintaan suojaustasolla IV.

Asetuksen 3. luvun 9§:n mukaan salassa pidettävien asiakirjojen luokittelussa käytetyt muut suojaustasot ja määritykset luokitellaan seuraavasti:

- Suojaustaso I, mikäli tiedon oikeudeton paljastuminen voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
- Suojaustaso II, mikäli tiedon oikeudeton paljastuminen voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle edulle
- Suojaustaso III, mikäli tiedon oikeudeton paljastuminen voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitetulle yleiselle tai yksityiselle edulle

Alla olevassa taulukossa (Taulukko 1) on esitetty Viestintäviraston hyväksymät tietoturvallisuuden arviointilaitokset 1.11.2017 mennessä.

Tietoturvallisuuden arviointilaitos	Pätevyysalue ja suojaustaso	Alkuperäinen hyväksyntä
KPMG IT Sertifiointi Oy	ISO 27001, suojaustaso IV Katakri II, suojaustaso IV Katakri 2015, suojaustaso III VAHTI, suojaustaso IV	6.10.2014
Nixu Certification Oy	ISO 27001, suojaustaso IV Katakri II, suojaustaso IV Katakri 2015, suojaustaso IV VAHTI, suojaustaso IV	2.9.2016
Inspecta Sertifiointi Oy	ISO 27001, suojaustaso IV	10.3.2017

Taulukko 1: Viestintäviraston hyväksymät tietoturvallisuuden arviointilaitokset (Viestintävirasto 2017)

KPMG IT Sertifiointi Oy on Suomen ensimmäinen Viestintäviraston hyväksymä tietoturvallisuuden arviointilaitos. Yritys on myös toistaiseksi ainoa tietoturvallisuuden arviointilaitos, jolla on pätevyysalueenaan suojaustason III pätevyys (Katakri 2015). KPMG IT Sertifiointi Oy toimitusjohtaja Mika Laaksosen mukaan tilojen, tarkastusmenetelmien, sisäisten prosessien ja työvälineiden saattamisessa viranomaisten vaatimusten edellyttämälle tasolle ja niiden osoittamisessa viranomaisille oli erittäin suuri työ ja vaati merkittäviä investointeja. Kokonaisuudessaan hakeutuminen tietoturvallisuuden arviointilaitokseksi vei KPMG:ltä noin neljä vuotta. (KPMG 2014.)

Nixu Certification Oy on hyväksytty Viestintäviraston toiseksi tietoturvallisuuden arviointilaitokseksi vuonna 2016. Nixun pätevyysalueet (ISO 27001, VAHTI, Katakri 2015) kattavat tällä hetkellä toistaiseksi suojaustaso IV mukaiset viralliset arvioinnit. (Nixu 2016.)

Inspecta Sertifiointi Oy on Viestintäviraston tuorein hyväksymä tietoturvallisuuden arviointilaitos. Inspecta on perinteikäs tarkastustoimintaan perehtynyt yritys. Se hakeutui tietoturvallisuuden arviointilaitokseksi vuonna 2017 pätevyysalueenaan toistaiseksi ISO 27001. Samana vuonna emoyhtiö Inspecta toteutti uudistuksen, jonka myötä sen nimi vaihtui Kiwa Inspecta Suomeksi. Tämä ei vaikuta tietoturvallisuuden arviointilaitoksena toimivan Inspecta Sertifiointi Oy:n operatiiviseen toimintaan. (Inspecta 2017.)

3.4 Arviointilaitostoiminta

Suomessa arviointilaitostoimintaa on olemassa myös muilla valtionhallinnon toimialoilla, ei pelkästään kyberturvallisuuden muodossa. Näiden toimintaa on kuitenkin hankala vertailla, sillä lainsäädäntö ja standardien vaatimukset eivät ole keskenään vertailtavissa. Euroopassa on myös tunnistettu vastaavanlaista toimintaa mutta se on luonteeltaan kuitenkin hieman erilaista, eikä perustu vastaavanlaisiin vaatimuksiin kuin Suomessa.

FINAS voi myöntää testaus-, tarkastus-, sertifiointi- tai kalibrointitoimintaa harjoittavalle organisaatiolle hakemuksen ja yritykseen suorittamansa tarkastuksen jälkeen hyväksytyn akkreditointipäätöksen, mikäli yritys täyttää kaikki akkreditointialueen ISO-standardin määrittelemät vaatimukset. Tietoturvallisuuden arviointilaitosten tapauksessa esimerkiksi ISO 27006 standardi täytyy täyttää ISO 27001 standardin perusteella. Hyväksytyn päätöksen jälkeen organisaatiot voivat hoitaa eri direktiivien mukaisia vaatimustenmukaisuuden arviointitehtäviä riippuen heille myönnetyistä pätevyysalueista. Monet näistä ovat viranomaisen alaisuudessa suoritettavia tehtäviä. Pätevyysalueen mukaan määritellään kuitenkin, minkälaisia palveluita voidaan tarjota akkreditoituna. Pätevyysalueita voi hakea esimerkiksi laboratorioissa tapahtuviin kalibrointimittauksiin tai testauksiin, järjestelmä- tai henkilösertifiointeihin tai erilaisiin todentajaorganisaatioihin. FINAS pitää verkkosivuillaan listaa kaikista akkreditoiduista toimijoista. Pätevyysalueet pidetään ajan tasalla ja niitä päivitetään päivittäin. (FINAS 2017.)

4 Opinnäytetyön toteutus

Vahvasti lainsäädäntöön ja muuhun kirjallisen dokumentaation pohjautuvan tietoperustan suuren määrän vuoksi sisällönanalyysi koettiin hyväksi vaihtoehdoksi todentaa yhteistoiminnan nykytilaa. Sen avulla pystyttiin keräämään tietoa lainsäädännöstä, viranomaisen ohjeesta ja muusta organisaatioiden välisestä dokumentaatiosta. Puolistrukturoidut teemahaastattelut valittiin opinnäytetyöhön soveltuvaksi, koska tuloksia nykytilasta ja kehitettävistä asioista saatiin niiden avulla kerättyä vielä laajemmin. Haastatteluiden avulla pystyttiin kohdentamaan vastaukset haluttuihin aihealueisiin. Teemoittelu valittiin, koska se todettiin kehittämissuunnitelman kannalta sopivaksi analysointimenetelmäksi. Sisällönanalyysin ja puolistrukturoitujen teemahaastatteluiden tulokset koottiin teemoittelun avulla tärkeysjärjestykseen. Teemoittelun priorisoinnin koettiin tukevan kehittämissuunnitelman laatimista.

Opinnäytetyön tavoitteena oli ensisijaisesti parantaa Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoimintaa. Toissijaisesti haluttiin parantaa viranomaisen valvontavastuuta. Opinnäytetyön tuloksena syntyy yhteistoiminnan kehittämissuunnitelma. Työhön käytettäviä tutkimusmenetelmiä kartoitettiin kirjallisia lähteitä ja aikaisempia opinnäytetöitä hyödyntäen. Menetelmien soveltuvuutta peilattiin samalla suunniteltuun tietoperustaan. Pää-

tös käytettävistä menetelmistä tehtiin huolellisesti ja harkiten. Tutkimusmenetelmien valinnan tarkoituksena oli saada tehtyä laadukas pohjatyö hyvien tulosten takaamiseksi.

Opinnäytetyön aihe ja tavoite määrittelevät työn toiminnalliseksi opinnäytetyöksi, joka perustuu laadulliseen tutkimukseen. Hirsjärven, Remeksen ja Sajavaaran (2007, 218-219) laadulliselle tutkimukselle on tavanomaista, että tietoa on kerätty vaiheittain eri menetelmien avulla. Tästä syystä analysointia voidaan tehdä koko työn aikana yhdessä tiedonkeruun kanssa samanaikaisesti. Laadullinen tutkimus pyrkii Hirsjärven ym. mukaan kuvamaan todellista elämää mahdollisimman kokonaisvaltaisesti. Laadullinen tutkimus on luonteeltaan kokonaisvaltaista tiedonhankintaa ja tutkimuksen aineisto kootaan yleensä todellisissa tilanteissa. Tiedonkeruun instrumenttina käytetään ihmistä, jota havainnoidaan esimerkiksi kuuntelemalla ja seuraamalla. Osallistuvan havainnoinnin lisäksi aineistonkeruumetodina käytetään teema- ja ryhmähaastattelua sekä dokumenttien ja tekstien diskursiivista analysointia. Laadulliselle tutkimukselle on myös tavanomaista sen toteuttamisen joustavuus: tutkimussuunnitelma muotoutuu tutkimuksen edetessä ja sitä muutetaan olosuhteiden mukaisesti. Tutkittavat tapaukset ovat ainutlaatuisia ja aineistoa tulkitaan sen mukaisesti. (Hirsjärvi ym. 2007, 164.)

Opinnäytetyö toteutettiin neljässä vaiheessa. Ensimmäisessä vaiheessa luotiin tietoperusta opinnäytetyölle ja tutustuttiin organisaatioiden dokumentaatioon sisällönanalyysin avulla. Toisessa vaiheessa muodostettiin haastattelurungot ja kerättiin tietoa asiantuntijahaastatteluiden avulla. Kolmas vaihe koostui käytettyjen tiedonkeruumenetelmien tulosten analysoinnista, joiden myötä luotiin kehittämissuunnitelma. Neljännessä vaiheessa luotiin kehittämissuunnitelma. Alla olevissa alaluvuissa on käsitelty tarkemmin opinnäytetyön tietoperusta sekä tiedonkeruu- ja analysointimenetelmät.

4.1 Tietoperusta

Opinnäytetyön tietoperusta pohjautuu pääsääntöisesti julkisiin asiakirjoihin, lakiin kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), turvallisuusselvityslakiin (726/2014) ja lakiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinnista (1406/2011), lakiin tietoturvallisuuden arviointilaitoksista (1405/2011) sekä tietoturvallisuuden arviointilaitoksille annetun ohjeen (Viestintävirasto 2016a.) ympärille.

Tiedonkeruumenetelmät kohdistettiin kirjallisiin ja sähköisiin lähteisiin. Niiden tarkoituksena oli kerätä opinnäytetyöhön liittyvää tietoa uskottavista lähteistä sekä samalla syventää opinnäytetyön laatijan tietämystä ja ymmärrystä käsiteltävästä aiheesta. Lähteet tukevat työssä käytettyä tietoperustaa. Kirjalliset lähteet koostuvat pöytäkirjoista, raporteista, lausunnoista ja muusta dokumentaatiosta. Sähköisten lähteiden avulla kuvataan esimerkkejä toimintaympäristöstä, nykytilasta ja tulevaisuudesta. Lainsäädännön tarkastelun osalta hyödynnettiin FINLEX-tietokantaa.

Aikaisempaa teoreettista tutkimusta opinnäytetyöhön liittyen ei pystytty hyödyntämään, koska tutkimuksia ei ole tehty. Osa dokumenttiaineistosta saattaa sisältää salassa pidettävää tai luottamuksellista tietoa. Salassa pidettävää tai luottamuksellista tietoa ei käsitellä opinnäytetyössä.

4.2 Sisällönanalyysi

Ensimmäisenä menetelmänä opinnäytetyöhön valittiin sisällönanalyysi, koska suuri osa tietoperustasta oli dokumenttipohjaista joko kirjallisessa tai sähköisessä muodossa. Sisällönanalyysissä aineistoa tarkastellaan eritellen, yhtäläisyyksiä ja eroja etsien ja tiivistäen. Tutkimuksessa on tarkoitus perehtyä sisällönanalyysin avulla lainsäädäntöön, Viestintäviraston tietoturvallisuuden arviointilaitoksille antamaan ohjeeseen, arviointilaitostapaamisten pöytäkirjoihin, arviointi- ja lausuntoraportteihin sekä muuhun dokumentaatioon. Sisällönanalyysin avulla on tarkoitus kuvata tiivistetysti tutkittava ilmiö ja kytkeä sen tulokset laajempaan asiayhteyteen sekä muihin tutkimustuloksiin. Dokumenttiaineistoa on tarkoitus analysoida tutkijan toimesta järjestelmällisesti ja yleispätevästi (Tuomi & Sarajärvi 2002, 105.)

Tuomen ja Sarajärven (2002, 98-99) mukaan aineiston pelkistäminen ja ryhmittely kuuluvat sisällönanalyysiin. Tässä opinnäytetyössä dokumentaatio ryhmiteltiin Viestintäviraston ja tietoturvallisuuden arviointilaitosten väliseen toimintaan liittyvään lainsäädäntöön ja dokumentaatioon. Sisällönanalyysi oli jatkuvaa ja sitä toteutettiin laatijan toimesta itsenäisesti koko opinnäytetyön ajan.

4.2.1 Lainsäädäntö

Viestintäviraston ja tietoturvallisuuden arviointilaitosten toimintaa määrittelee ja ohjaa ensisijaisesti laki, toissijaisesti määräykset ja ohjeet. Alla on kuvattu toimintaan liittyvät lait ja niiden tehtävät.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinnista (1406/2011) määrittelee viranomaisten tietojärjestelmien arvioinnista sekä niiden käytöstä. Laissa määritellään myös Viestintäviraston tehtävät, oikeudet ja tietoturvallisuuden tasosta myönnetyn todistuksen antamisesta ja velvoitteista.

Laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi. Laki määrittelee kansallisen turvallisuusviranomaisen ja määrätyt turvallisuusviranomaiset sekä niiden välisestä yhteistyöstä. Laki määrittelee myös tietoturvallisuustoimenpiteistä. Tällaisia ovat esimerkiksi

salassapitovelvollisuus, vaitiolovelvollisuus, turvallisuusluokituksien merkitseminen ja käsittely sekä turvallisuusselvityksien arviointi.

Turvallisuusselvityslain (726/2014) tarkoituksena on parantaa mahdollisuuksia ennalta ehkäistä toimintaa, joka voi vahingoittaa Suomen valtion turvallisuutta tai siihen verrattavaa yleistä etua. Laki määrittelee selvityksen kohteena olevan henkilön tai yrityksen aseman ja oikeudet sekä turvallisuusselvitysprosessin. Prosessi on määritelty turvallisuusselvityksen hakemisesta, tietojen käsittelystä sen aikana aina rekisterimerkintään ja voimassaoloon asti.

Laki tietoturvallisuuden arviointilaitoksista (1405/2011) tarkoituksena on osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso. Lakia sovelletaan elinkeinoharjoittajiin ja julkishallinnolle palveluita tarjoaviin yksiköihin. Laki määrittelee arviointilaitokseksi hakeutumisesta, velvollisuuksista ja tehtävistä sekä erinäisistä määräyksistä, joita tietoturvallisuuden arviointilaitosten tulee noudattaa kaikessa toiminnassaan.

Lainsäädäntöön tehdyn sisällönanalyysin avulla voidaan todeta, että lainsäädäntö Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä on tuoretta sääntelyä, pois lukien laki kansainvälisistä tietoturvallisuusvelvoitteista, joka on säädetty vuonna 2004. Lainsäädäntö tarvitsee tietyiltä osin tarkennuksia. Tietoturvallisuuden arviointilaitosten toimintaa ei hyväksyttynä arviointilaitoksena ei esimerkiksi käsitellä millään tavalla lainsäädännössä. Käytännössä toiminta kuitenkin on mahdollista. Yhtenä puutteena havaittiin myös selkeä arviointilaitosten valvonnan määrittelyn puute Viestintäviraston ja FINAS:n osalta. Hyvänä puolena nähtiin vuonna 2014 säädetyn turvallisuusselvityslain hyvä prosessikuvaus turvallisuusselvitysten osalta.

4.2.2 Ohje tietoturvallisuuden arviointilaitoksille

Viestintäviraston Kyberturvallisuuskeskuksen NCSA-toiminnon lakimiehen tehtävänä on ollut luoda tietoturvallisuuden arviointilaitoksille ohje. Ohje on valmistettu vuonna 2013. Ohje kuitenkin elää kokoajan ja tarvitsee päivittämistä tasaisin väliajoin. Ohjetta on päivitetty neljä kertaa sen valmistumisen jälkeen. Tämä johtuu lainsäädännön muutoksista, toimintatapojen elämisestä, teknologian kehittymisestä ja Viestintäviraston sisäisistä muutoksista. Ohjetta on viimeksi päivitetty 19.5.2017. (Viestintävirasto 2016b.)

Ohjeessa tietoturvallisuuden arviointilaitoksille kuvataan näiden pohjalta arviointilaitosten toimintaa koskevat vaatimukset ja tietoturvallisuuden arviointeja koskeva menettely. Ohje on luotu tietoturvallisuuden arviointilaitoksille asioiden selkeyttämiseksi, mahdollisten avoimeksi jäävien kysymysten vastauksen saavuttamiseksi ja yleisten raamien sekä kehysten asettamiseksi arviointilaitostoiminnalle. Ohje on yleensä tietoturvallisuuden arviointilaitoksilta tulevi-

en kysymysten asettelun perusta. Arviointilaitokset ovat omaksuneet ohjeen käytön ja soveltavat sitä luontevasti. Ohjeen jalkauttaminen arviointilaitoksille on onnistunut hyvin, eikä se ole aiheuttanut epäjohdonmukaisuuksia arviointilaitosten ohjauksessa tai arviointilaitosten keskuudessa. Ohje on julkinen asiakirja, mikä omalta osaltaan helpottaa sen käsittelyä ja jalkauttamista. (Viestintävirasto 2016b.)

Ohjetta tarkasteltiin ja voidaan todeta, että ohje on erittäin kattavasti tehty ja määrittelee arviointilaitoksien toimintaympäristöä ja laitoksille asetettuja vaatimuksia hyvin. Yhtenä kehitettävänä asiana todettiin ohjeen laajuus. Ohje on tällä hetkellä 48 sivun pituinen dokumentti. Sitä on vaikea enää mieltää ohjeeksi. Toisena kehitettävän asiana todettiin tulkinnan ja prosessien selkeyttäminen. Tämä koskee haku-, arviointi- ja valvontavaihetta arviointilaitostoiminnassa. Vaikka lakien ja ohjeen vaatimukset, raamit ja kehykset ovat valmiiksi asetettu toimintaympäristön ympärille, tulee eteen tilanteita, joissa joudutaan pohtimaan miten ohjetta ja lainsäädäntöä sovelletaan terminologiaan tai tiettyyn tilanteeseen arviointilaitostoiminnassa.

4.2.3 Muu dokumentaatio

Viestintäviraston ja tietoturvallisuuden arviointilaitosten välistä muuta dokumentaatiota syntyy erilaisten tapaamisten, suoritettujen arviointien, jaettujen lausuntojen tai todistusten ja yhteisten keskustelujen pohjalta. Alla on kuvattu organisaatioiden välisen muun dokumentaation muodostumistapoja.

Arviointilaitostapaaminen on perinteeksi muodostunut Viestintäviraston järjestämä yhden päivän pituinen kokous, johon kutsutaan kaikki hyväksytyt tietoturvallisuuden arviointilaitokset ja käsitellään ajankohtaisia asioita, koulutettavia asioita sekä mahdollisia ongelmia. Tapahtuma järjestetään yleensä kaksi kertaa vuodessa. Tapahtumaa on pidetty yleisesti hyvänä mutta toiveena on ollut ehkä hieman yksityiskohtaisempi koulutustarjonta, lyhyempikestoiset tietoiskut ja useammat tapaamiset joko koulutus- tai tiedonjakotarkoituksessa. Tapaamisista on tehty erillinen pöytäkirja käsiteltyjen asioiden osalta. Näiden pöytäkirjojen tarkastelun osalta voitiin todeta, että koulutuksien ja tapaamisten lisääminen sekä täsmällisempi ajankäyttö tunnistettiin yhdeksi kehittämiskohteeksi.

Arviointiraportit, todistukset ja lausunnot ovat yksi tärkeimpiä viranomaisen työkaluja, kun puhutaan tietoturvallisuuden arviointilaitosten viranomaisen hyväksyntään tähtäävästä arvioinnista. Viestintävirasto voi hyödyntää hyväksytyn tietoturvallisuuden arviointilaitoksen tekemän arvioinnin tuloksia kohtuullisen suoraviivaisesti arvioidessaan palvelujen tai järjestelmien soveltuvuutta viranomaisten salassa pidettävien tietojen käsittelyyn (Viestintävirasto 2017b.) Raporttien ja lausuntojen muodostamisessa on niin Viestintävirastolla kuin tietoturvallisuuden arviointilaitoksilla käytössä useampaa mallia. Raporttien ja lausuntojen taso on

ollut vaihtelevaa, mutta pääsääntöisesti kuitenkin hyvällä tasolla. Tarkasteltaessa näitä dokumentteja todettiin kehittämistarpeena yhtenäiset dokumentit. Tähän kehittämistarpeeseen ratkaisuna on pohdittu yhteisen kaikkien organisaatioiden käytössä olevan raportti- ja lausuntopohjan käyttämistä tulevaisuudessa.

Sähköposti on osoittautunut yhdeksi tehokkaimmista tiedonvälitystavoista Viestintäviraston ja tietoturvallisuuden arviointilaitosten välisessä yhteydenpidossa. Erityisesti arviointilaitosten alkutaipaleella tiedonvälitys ja viranomaisten ohjaaminen on ollut päivittäistä. Hyväksyttyjen VAHTI- ja Katakri-pätevyysalueiden saavuttamisen jälkeen yhteydenpito on kuitenkin satunnaistunut. Sähköpostien sisältö vaihtelee kysymyksistä ja tulkinnoista hyväksyttyjen menetelmien ja tuotteiden käyttöön liittyviin politiikkoihin. Monesti kysymyksien ja tulkintojen lisäksi on esitetty esimerkki tukemaan ymmärrystä mahdollisessa ongelmatilanteessa. Sähköposti on helppo ja nopea tapa tiedonvälitykseen . Sen kääntöpuolena voidaan pitää tiedon jäämistä rajatun piirin sisälle, unohtamista muuhun massaan tai päätymistä vääriin käsiin. Hyvänä esimerkkinä voidaan pitää viime kesän Venäjän presidentti Vladimir Putinin valtiovierailun tietojen päätymistä ulkopuolisen sähköpostiin (Iltalehti 2017.) Sähköposti tiedonvälityskanavana on myös varsin henkilösidonnainen. Tiedon päätyminen henkilöille, joille se alun perin on tarkoitettu ei ole ongelmatonta.

Ongelmaa on pyritty ratkaisemaan ohjaamalla kysymyksiä ja keskusteluja NCSA-toiminnon yhteiseen sähköpostilaatikkoon. Yhteinen sähköpostilaatikko on kuitenkin valitettavan ruuhkainen ja täyttyy nopeaan tahtiin kansallisten ja kansainvälisten yhteystyökumppaneiden yhteydenottojen ja kysymysten osalta. Sen seurantaa ei ole täysipäiväisesti vastuutettu kenellekään, vaan jokaisen on annettava oma panoksensa asialle. Käytännössä tämä johtaa siihen, että laatikossa olevia, sähköpostilla tulleita kysymyksiä tai tietoa ei välttämättä lueta. Ryhmäsähköpostilaatikko vastaanottajana ei sido henkilökohtaisesti ryhmän jäseniä, jolloin kysymys on helppo väistää tai olla välittämättä. Sisällönanalyysin avulla todettiin, että sähköpostin henkilösidonnaisuus ja vastuuttamattomuus todettiin kehitettäväksi asiaksi. Ongelma pyritään ratkaisemaan luomalla arviointilaitoksille täysin erillinen ryhmäsähköpostilaatikko, jonka seuraaminen olisi vastuutettu tietyille henkilöille. Tällainen henkilö voisi olla esimerkiksi Viestintäviraston arviointilaitoskoordinaattori.

Tietoturvallisuuden arviointilaitoksille on Viestintäviraston toimesta luotu oma extranet-tila. Tähän tilaan on koottu tulkintoja, menetelmiä, arviointilaitostoiminnassa käytettäviä dokumentteja ja yleisiä ohjeita. Tilaan on rajattu pääsy vain aktiivisesti arviointilaitoksien tarkastustoimintaan osallistuville henkilöille. Extranet-tilaan on myös ohjeistettu laittamaan yleistietoja arviointilaitosten mahdollisista arvioinneista, kuitenkin niin ettei mitään turvaluokiteltua tietoa laiteta tilaan. Extranet-tilan käyttö on ollut vähäistä ja esimerkiksi arviointien tietojen syöttäminen ei ole pysynyt ajan tasalla. Tila on liian sekava. Tulkintoja ja menetelmiä

on kuvattu tilassa runsaasti, mikä aiheuttaa sen käytettävyydelle ongelmia, koska niitä on vaikea löytää isosta massasta. Tila tarjoaa kuitenkin hyvää potentiaalia ja voisi olla aktiivisemmin käytettynä ja selkeämmin järjesteltynä hyvä lisä arviointilaitosten toimintaan. Lisäkoulutus tilan käytön parantamiseksi todettiin yhtenä kehitettävänä asiana.

4.2.4 Sisällönanalyysin yhteenveto

Lainsäädäntöön ja dokumentaatioon suoritetun sisällönanalyysin avulla saatiin hyviä kehittämisideoita yhteistoiminnan parantamiseksi. Tämän yhteenvedon tarkoituksena on koota sisällönanalyysin tulokset yhteen, jotta ne pystytään hahmottamaan helpommin analyysimenetelmää varten. Alla on lueteltu sisällönanalyysin myötä havaittuja ideoita:

- lainsäädännöllinen valvonnan määrittely Viestintäviraston ja FINAS:n osalta
- arviointilaitoksille suunnatun ohjeen tiivistäminen (tällä hetkellä 48 sivuinen ohje)
- prosessikuvaus arviointilaitostoiminnasta (hakuvaihe, arvioinnit, valvonta)
- tapaamisten lisääminen ja täsmällisempi ajankäyttö
- yhteiset raportti- ja lausuntopohjat
- arviointilaitoskohtainen sähköposti ja sen vastuuttaminen
- extranet-tilan järjestely ja lisäkoulutus.

4.3 Henkilöhaastattelut

Haastattelu on Hirsjärven, Remeksen ja Sajavaaran (2007, 204) mukaan yksi laadullisen tutkimuksen pääaineistonkeruumenetelmä. Hirsjärvi ym. pitävät yhtenä hyötynä haastattelun kautta saatujen tuloksien mahdollisuutta yhdistää niitä suurempiin asiayhteyksiin. Haastattelun onnistumiseen vaikuttaa myös haastateltavien motivaatio ja ajankäyttö. Aikaa on syytä varata riittävästi, ettei haastateltavan keskittyminen häiriinny.

Hirsjärven ja Hurmeen (2009, 34) mukaan haastattelun yksi tärkeimmistä tavoitteista on saada käsitys siitä, mitä haastateltava ajattelee ja saada tietoa hänen mielipiteistään tutkimuskysymysten ratkaisemiseksi. Yhtenä haastattelun vahvuutena pidetään tutkijan mahdollisuutta tarkentaa kysymyksiä tai esittää lisäkysymyksiä varmistuakseen siitä, että haastateltava on ymmärtänyt kysymysten tarkoitusperän.

Hirsjärven ym. mukaan (2007, 206, 211) haastattelun suurin haaste on se, että sen toteuttaminen vie paljon aikaa. Haastattelutilanteen tulisi kestää 1-2 tuntia. Ojasalo, Moilanen ja Ritalahti (2009, 110.) mukaan haastattelun kesto voi olla kymmenistä minuuteista tunteihin. Haastattelun kesto on riippuvainen sen haastatteluluokasta, avoimuudesta ja siitä kuinka paljon tietoa tarvitaan.

Tutkimusmenetelmänä käytettiin strukuroidun- ja teemahaastattelun yhdistelmää. Menetelmä antaa haastateltaville vapautta vastauksiin, vaikka tietoa haetaankin etukäteen laaditun haastattelulomakkeen pohjalta (Aaltola & Valli 2001, 24-25, 100-101.)

Haastattelurunko (Liite 1) muodostettiin etukäteen valituilla, sisällönanalyysin tuloksien sekä tutkimuskysymyksiin pohjautuvien, aihealueiden perusteella. Rungon kysymykset on luotu opinnäytetyön laatijan toimesta vastaamaan haluttuihin aihealueisiin. Haastattelurunko teemoiteltiin etukäteen ja teemoja valittiin yhteensä kuusi kappaletta. Teemat luokiteltiin seuraavasti: nykytila, toiminnan kehittäminen, yhdenmukaisuus, koulutus, viranomaisvalvonta ja tulevaisuus. Teemojen alla esitettiin vähintään kaksi avointa kysymystä. Kysymykset ja aihealueet olivat samoja kaikille haastateltaville. Tällä varmistuttiin halutuista käsiteltävistä aiheista mutta samalla oli tarkoitus antaa haastateltaville vapautta liikkua ilman tiukkaa etenemisreittiä.

Haastattelurunkoa testattiin etukäteen kolmella eri henkilöllä. Jokainen testi suoritettiin erikseen. Haastattelurunkoa muokattiin jokaisen testauksen jälkeen sopivimmaksi tukemaan tutkimuskysymyksiä ja valittuja teemoja. Lopuksi haastattelurunko koostettiin viralliseen muotoonsa ja todettiin sen olevan valmis käytettäväksi.

Haastateltaviksi valittiin yksi esimies ja yksi asiantuntija Viestintävirastosta, KPMG IT Sertifiointi Oy:stä ja Nixu Certification Oy:stä. Haastattelujen tarkoituksena oli tuoda lisäarvoa ja kehitettäviä asioita lainsäädäntöön ja dokumentaatioon suoritetun sisällönanalyysin tueksi. Inspecta Sertifionti Oy rajattiin ulos haastateltavien osalta, koska heidän arviointilaitoshyväksyntä oli vasta saavutettu, eikä heidän haastattelusta koettu saatavan lisäarvoa tutkittavalle asialle.

Haastateltavien suostumusta tiedusteltiin ja haastattelukutsut lähetettiin haastateltaville kesäkuun lopulla. Kaikki haastateltaviksi suunnitellut henkilöt suostuivat pyyntöön ja olivat erittäin myötämielisiä vaikuttamaan yhteiseen asiaan. Haastateltavien kiinnostus ja motivaatio oli erittäin hyvällä tasolla alusta alkaen. Haastattelurunko lähetettiin haastateltaville noin kaksi viikkoa ennen varsinaista haastattelua heinäkuun lopussa. Haastattelut toteutettiin ennalta laaditun ja testatun rungon mukaisesti. Jokainen haastattelu oli sovittu suoritettavaksi erikseen haastateltavan organisaation tiloissa.

Yhteensä haastatteluja tehtiin kuusi kappaletta. Haastattelujen kestot vaihtelivat haastateltavien kesken 26 minuutista yhteen tuntiin ja 19 minuuttiin. Haastattelut nauhoitettiin mahdollisten tarkennusten saamiseksi laatijalle. Kaikki haastattelut suoritettiin alkuperäisen suunnitelman mukaisesti aikataulussa elokuussa. Haastattelut suoritettiin haastateltavien anonymiteettiä kunnioittaen. Anonymiteetti koettiin tarpeelliseksi, koska laatija halusi mah-

dollisimman suoria ja rehellisiä mielipiteitä haastateltavilta. Haastateltavia pyydettiin myös arvioimaan jokaista etukäteen teemoiteltua asiakokonaisuutta asteikolla 1-5 tukemaan haastattelusta saatavia tietoja.

4.3.1 Nykytila

Haastateltavien antama yleisarvosana Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistyöstä oli 2,33. Kaikki haastateltavat olivat yhtä mieltä siitä, että Viestintäviraston ja arviointilaitosten yhteistyö ei ole riittävällä tasolla ja kehitettäviä asioita riittää. Kolme haastateltavista kokee, että tämänhetkisessä tilanteessa kyse ei ole niinkään yhteistyöstä vaan ennemminkin asetelmasta, jossa arviointilaitokset ovat Viestintäviraston arvioitavana.

Neljä haastateltavaa kokee, että Viestintäviraston ohjaus on riittävää tällä hetkellä, tämä on osittain johdannaista siitä, että arviointilaitokset ovat olleet pitkään hyväksyntäprosessissa mukana, jolloin yhteydenpito on ollut aktiivisempaa Viestintäviraston kanssa.

Kolme haastateltavaa myös toivoi Viestintävirastolta selkeämpää prosessimaista kaaviota arviointilaitostoimintaan, josta kukin tietäisi mitä tietyissä vaiheissa aina tapahtuu, nyt tällaista ei ole olemassa ja vaiheet saattavat tulla arviointilaitoksille hieman yllätyksenä tai vähällä reagointiajalla.

Kolmen haastateltavan mukaan säännölliset tapaamiset niin omistaja kuin asiantuntijataholla olisivat omiaan parantamaan nykytilaa. Tällä tavalla pysyttäisiin kartalla missä kukin menisi. Kahden haastateltavan mukaan resursointia arviointilaitostoimintaan pitäisi lisätä viranomaisen puolelta. Yksi haastateltavista ehdotti arviointilaitoskohtaista koordinaattoria toiminnan parantamiseksi jos toiminta laajenee tulevaisuudessa. Pääsääntöisesti haastateltavien toimesta toivottiin ylipäänsä yhteistyön lisääntymistä ohjauksen, yhdessä tekemisen, kouluttamisen tai työkalujen vaihtojen muodossa.

4.3.2 Toiminnan kehittäminen

Haastateltavien antama yleisarvosana oman organisaation osaamisen tasosta arviointilaitostoiminnassa oli 3,33. Haastateltavat olivat pääsääntöisesti tyytyväisiä omaan osaamiseensa mutta neljä haastateltavaa totesi, että yksityiskohtainen osaaminen tai kyvykkyys on henkilösidonnaista ja vaatii organisaatiolta ponnisteluja. Viiden haastateltavan mukaan tähän parhaana ratkaisuna nähtiin niin sanottu best practice-oppiminen, jossa Viestintävirasto tai arviointilaitokset ottaisivat mukaansa henkilöitä muista organisaatioista arvioinneilleen, jolloin olisi mahdollisuus oppia.

Viisi haastateltavaa totesi myös, että tekemällä oppii ja arviointilaitoksena suoritettavia arviointeja toivottiin mutta toistaiseksi arviointien vähäinen määrä on rajoittanut oppimista. Kaikilla haastateltavilla oli omat sisäiset prosessit oman toiminnan kehittämiseensä mutta käytännön työ tehtyjen arviointien muodossa koettiin erityisen tärkeänä.

Oman toiminnan kehittämisen kannalta koettiin seuraavia asioita: kolmen haastateltavan mukaan resursointia arviointilaitostoimintaan niin viranomaisen kuin arviointilaitosten taholta tulee vääjäämättä lisätä tulevaisuudessa jos arviointilaitosten tekemät arvioinnit lisääntyvät. Arvioinneilla pyritään pitämään aina useampia henkilöitä mukana kaikkien haastateltavien osalta, tämä tietotaidon siirtymisen ja toiminnan jatkuvuuden mahdollistamiseksi. Organisaatioiden oman toiminnan kehittäminen on toteutettu sisäisillä prosesseilla, perehdyttämällä uusia henkilöitä toimintaan ja kouluttamalla arviointilaitosasioita.

Yhtenä ongelmana nähdään myös, että Viestintävirastossa arviointilaitostoiminnassa ei ole henkilöä, jonka toimenkuva muodostuisi täyspäiväisesti tästä toiminnasta. Viestintäviraston arviointilaitostoimintaan on tällä hetkellä nimetty neljä henkilöä Viestintävirastosta. Kaikki arviointilaitostoiminnassa mukana olevat virkamiehet tekevät näitä asioita päätoimensa ohella.

4.3.3 Yhdenmukaisuus

Haastateltavien antama yleisarvosana Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhdenmukaisuudesta oli 2,33. Organisaatioiden välisissä arviointien toimintatavoissa, prosesseissa, arvioinneissa ja niiden lopputuloksissa nähtiin eroavaisuuksia ja epätasaisuutta. Kaikkien haastateltavien mukaan prossien, menetelmien ja lopputulosten tulisi olla mahdollisimman samankaltaisia. Jokaisella organisaatiolla on omat dokumenttipohjat käytössään.

Yhdenmukaisuuden saavuttamiseksi kaikkien haastateltavien mukaan parhaita keinoja olisivat yhdessä arviointien tekeminen ja yhteisten työkalujen käyttäminen. Arviointeja voitaisiin olla mahdollisesti puolin ja toisin seuraamassa tai vaihtoehtoisesti siten, että Viestintävirasto ottaisi arviointilaitoshenkilökuntaa mukaan suorittamiinsa arviointeihin. Yhdenmukaiset dokumenttipohjat nähtiin haastateltavien toimesta myös hyvänä ja mahdollisena voimavarana yhdenmukaisuuden kannalta, kunhan säilytetään keskusteluyhteys sen sisällöstä ja yksityiskohtien tekemisestä dokumentteihin. Kolme haastateltavaa myös totesi, että rakentavan palautteen saaminen suoritetusta työstä on myös erityisen tärkeä osa oppimisen kannalta.

Extranet-tilan käytettävyyden parantaminen ja sen mahdollinen lisäkouluttaminen sekä ohjeistaminen tunnistettiin myös yhtenä mahdollisena kehittämiskohteena. Sen avulla laitosten ohjeistaminen ja arviointien valvonta helpottuisi nykytilanteessa. Tämä edesauttaisi myös arviointilaitoksia pitämään yllä kokonaisuutta suoritettavista arvioinneista.

4.3.4 Koulutus

Haastateltavien antama yleisarvosana Viestintäviraston tietoturvallisuuden arviointilaitoksille tarjoamasta koulutuksen tasosta oli 2,83. Viestintäviraston antaman koulutuksen taso jakoi haastateltavien mielipiteitä. Tiettyjen yksityiskohtaisten koulutusten, kuten esimerkiksi fyysisen turvallisuuden koulutus, sai hyvää palautetta mutta yleisesti pidettyjen koulutusten taso ja koulutusten kesto eivät olleet haastateltavien mieleen.

Viiden haastateltavan mukaan Viestintäviraston tarjoamaa koulutusta on liian vähän. Hyödyllisimmäksi koulutukseksi katsottiin koulutukset, joissa käsiteltiin arvioinneissa esiintyvien vaatimusten tulkintoja tai todennusmenetelmiä. Kaksi haastateltavaa ehdotti ulkopuolisen yhteiskoulutuksen järjestämistä, jossa saataisiin laadukas ja mahdollisesti kallis koulutus kolmannelta osapuolelta (esimerkiksi SANS, Microsoft, Santa Monica Networks tai F-Secure) kustannettua yhteisesti. Yleisesti koulutusta toivottiin määrällisesti olevan enemmän. Lukumäärät vaihtelivat vähintään neljästä kerrasta vuodessa, tarpeen mukaan tai aina toiminnan uudistusten tullessa. Kehitettävänä asiana nähtiin myös esimerkkien kautta tulkitseminen ja enemmän hands-on tyyppisen koulutuksen tarjonta. Kolmen haastateltavan mukaan erityisesti teknisen tietoturvallisuuden koulutuksen tarjoaminen hallinnollisen ja fyysiseen turvallisuuden lisäksi Viestintäviraston toimesta olisi toivottavaa.

4.3.5 Viranomaisvalvonta

Haastateltavien antama yleisarvosana viranomaisen valvontavastuun toteutumisesta Viestintäviraston osalta oli 3,20. Kaikkien haastateltavien mukaan viranomaisen valvontavastuu on enemmän tai vähemmän ollut osa arviointilaitosten hyväksyntäprosessia. Valvonnan riittävän tason määrittely todettiin vaikeaksi. Yhteneväisiä oltiin myös siitä, että valvontaa tulisi suorittaa dokumentaatioperusteisesti. Kolmen haastateltavan mielestä valvontaa tulisi Viestintäviraston osalta suorittaa myös olemalla arvioinneissa mukana joko etukäteen ilmoittamalla tai pistokoemaisesti.

Yhtenä ongelmana kaksi haastateltavaa näki viranomaisten valvonnan tekemisen. Viestintäviraston ja FINAS:n roolituksen selkeyttämistä toivottiin päällekkäisen työn välttämiseksi. Nyt asia ei ole täysin selvä. Kaksi muutakin haastateltavaa toivat esille asian eri teeman alaisuudessa. Yhden haastateltavan mukaan yhtenä vaihtoehtona valvonnalle voitaisiin pitää asiakastyytyväisyyspalautetta.

4.3.6 Tulevaisuus

Haastateltavien antama yleisarvosana Viestintäviraston ja tietoturvallisuuden arviointilaitosten toiminnan tarpeellisuudesta tulevaisuudessa oli 4,66. Kaikkien organisaatioiden haastateltavat olivat yhtä mieltä siitä, että arviointilaitoksien tarve on ilmeinen tulevaisuudessa. Kol-

men henkilön mielestä arviointilaitostoiminnan suurimpana uhkana voidaan pitää henkilöstön vaihtuvuutta, kahden haastateltavan mielestä muuttuva kriteeristö ja lainsäädännön muutokset ovat suurin huolenaihe. Kaksi haastateltavaa piti uhkana myös arviontien myymistä liian halvalla, tarkoittaen työnlaadun heikentymistä.

Keskeisimpinä kehittämistarpeina tulevaisuuden arviointilaitostoiminnassa nähtiin kolmen haastateltavan osalta prosessien selventäminen sekä suunnitelmallisuus ja kaksi haastateltavaa mainitsi myös laadukkaan kokonaisturvallisuuden tavoittelun. Tällä tarkoitettiin sitä, että tuntuma nyt vaikuttaa siltä, että keskitytään liialti yksittäisiin prosesseihin. Viestintäviraston ja arviointilaitosten ristiin työskentely nähtiin vain yhden haastateltavan mielestä mahdollisuutena.

4.3.7 Haastattelujen yhteenveto

Haastatteluista voidaan todeta, että Viestintäviraston ja tietoturvallisuuden arviointilaitosten henkilöt, jotka ovat sitoutuneet arviointilaitostoimintaan, ovat motivoituneita ja kiinnostuneita kehittämään toimintaa hyvässä yhteistyössä. Esimiehiin ja asiantuntijoihin kohdistuneen strukturoidun teemahaastattelun avulla saatiin hyviä kehittämisideoita yhteistoiminnan parantamiseksi. Tämän yhteenvedon tarkoituksena on koota haastattelun tulokset yhteen, jotta ne pystytään hahmottamaan helpommin analyysimenetelmää varten. Alla on lueteltu haastattelun myötä havaittuja ideoita luokiteltuna teemojen mukaisesti:

Nykytila:

- selkeämpi prosessimainen kaavio arviointilaitostoiminnasta
- säännölliset tapaamiset
- arviointilaitoskohtainen koordinaattori.

Toiminnan kehittäminen:

- best practice-oppiminen
- arviointilaitoshenkilöstön lisääminen (Viestintävirasto ja arviointilaitokset)
- koulutuksen lisääminen
- viestintäviraston henkilöstö päätoimisesti arviointilaitostoimintaan.

Yhdenmukaisuus:

- yhteiset arviointikeikat
- yhteiset työkalut
- seuranta ja koulutusmahdollisuus arvioinneilla
- yhdenmukaiset dokumentit
- rakentavan palautteen antaminen
- extranet-tilan käytettävyyden parantaminen ja lisäkoulutus.

Koulutus:

- viestintäviraston koulutusten kesto täsmällisemmäksi ja määrällisesti enemmän
- tulkinnat ja todennusmenetelmät hyödyllisimpiä koulutuksia
- kolmannen osapuolen tarjoama kallis ja laadukas koulutus
- hands-on tyyppisen koulutuksen mahdollistaminen.

Viranomaisvalvonta:

- suoritettava dokumenttiperusteisesti
- paikanpäällä mukana arvioinneissa
- etukäteen ilmoittamalla tai pistokoemaisesti
- päällekkäinen valvonta Viestintäviraston ja FINAS:n osalta
- asiakastyytyväisyyspalaute.

Tulevaisuus:

- prossien ja suunnitelmallisuuden parantaminen arviointilaitostoiminnassa
- lainsäädännön ja ohjeistuksen muutoksista tiedottaminen ajoissa.

4.4 Analysointimenetelmät

Opinnäytetyön analysointimenetelmäksi valittiin teemoittelu, jonka avulla pyrittiin saamaan vastauksia tutkimuskysymyksiin. Teemoittelun todettiin soveltuvan opinnäytetyöhön hyvin siinä käytettyjen tiedonkeruumenetelmien ja teorian vuoksi. Muita yleisesti käytettyjä laadullisen aineiston analysointimenetelmiä ovat tyypittely, sisällönerittely, diskurssi ja keskusteluanalyysi. (2007, 218-219.)

Teemoittelun perusperiaatteena on, että aineisto on pilkottu pienempiin osiin eri teemojen alle, jotka rakentuvat tiedonkeruumenetelmien sekä teorian avulla. Osiin pilkottu aineisto rakentuu uudenlaiseksi kokonaisuudeksi tiedonkeruumenetelmien ja teorian avulla. Teemoittelu voidaan suorittaa esimerkiksi poimimalla haastatteluista kyseiseen teemaan liittyvät asiakohdat. Teemoittelun yhteydessä materiaali lajitellaan teemojen alle kokonaisuuksiksi, joilla pyritään ratkaisemaan myös tutkimuskysymyksiin vastauksia. (Tuomi & Sarajärvi 2009, 93-95.)

Tässä opinnäytetyössä tiedonkeruumenetelmien tulokset teemoiteltiin eri teemojen alle priorisointijärjestyksessä seuraavanlaisesti:

- välittömästi kehittämistä vaativat asiat
- seuraavan vuoden aikana kehittämistä vaativat asiat
- lähitulevaisuudessa (1 - 3 vuotta) kehittämistä vaativat asiat.

Tiedonkeruumenetelmien avulla saatuja samankaltaisia tuloksia on yhdistetty päällekkäisyyksien välttämiseksi. Analysointi on opinnäytetyön laatijan omakohtaista tulkintaa. Analysoinnin tulokset on lueteltu alla:

Välittömästi kehittämistä vaativat asiat:

- prosessikuvaus arviointilaitostoiminnasta (hakuvaihe, arvioinnit, valvonta)
- säännölliset tapaamiset ja täsmällisempi ajankäyttö
- yhdenmukaiset raportti- ja lausuntopohjat
- arviointilaitoskohtainen sähköposti ja sen vastuuttaminen
- extranet-tilan käytettävyyden parantaminen ja lisäkoulutus
- rakentavan palautteen antaminen.

Seuraavan vuoden aikana kehittämistä vaativat asiat:

- päällekkäisen valvonnan poistaminen Viestintäviraston ja FINAS:n osalta
- koulutuksen lisääminen
- best practice-oppiminen
- yhteiset arviointikeikat / seuranta ja koulutusmahdollisuus arvioinneilla
- viestintäviraston koulutusten kesto täsmällisemmäksi ja määrällisesti enemmän
- yhteiset työkalut
- suoritettava dokumenttiperusteisesti (viranomaisvalvonta)
- paikanpäällä mukana arvioinneissa (viranomaisvalvonta)
- etukäteen ilmoittamalla tai pistokoemaisesti (viranomaisvalvonta)
- tulkinnat ja todennusmenetelmät hyödyllisimpiä koulutuksia
- hands-on tyyppisen koulutuksen mahdollistaminen
- tulkinta ja todennusmenetelmäkoulutuksen lisääminen
- arviointilaitoksille suunnatun ohjeen tiivistäminen (tällä hetkellä 48 sivuinen ohje).

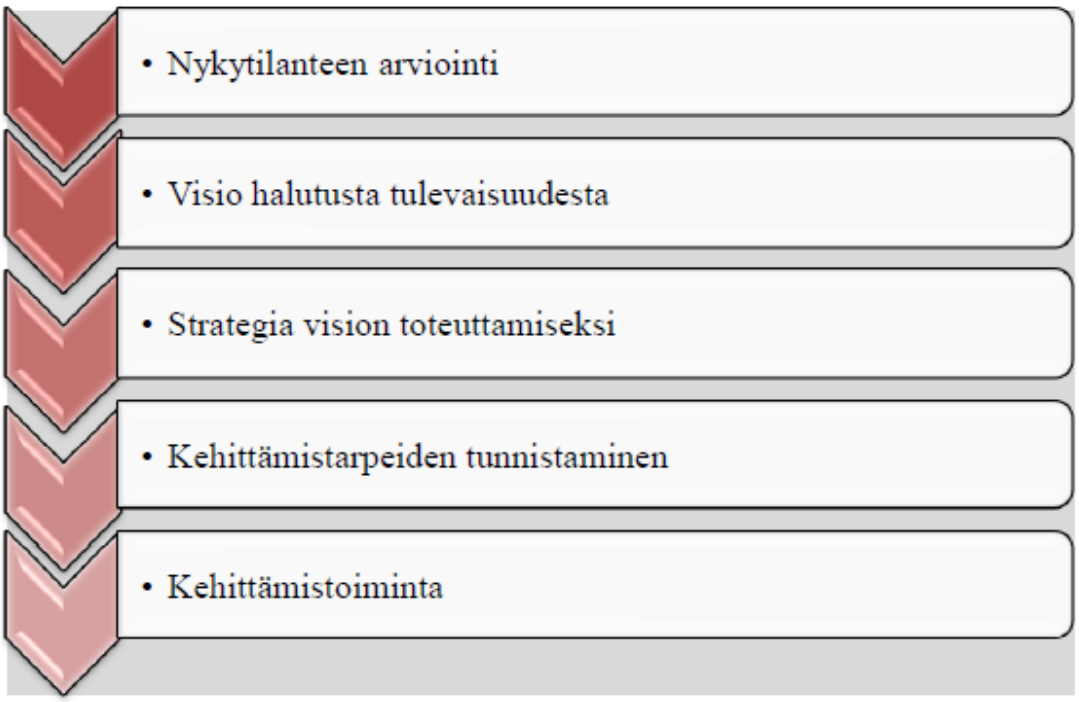
Lähitulevaisuudessa (1 - 3 vuotta) kehittämistä vaativat asiat:

- arviointilaitoskohtainen koordinaattori
- arviointilaitoshenkilöstön lisääminen (Viestintävirasto ja arviointilaitokset)
- viestintäviraston henkilöstö päätoimisesti arviointilaitostoimintaan
- lainsäädännöllinen valvonnan määrittely Viestintäviraston ja FINAS:n osalta
- kolmannen osapuolen tarjoama kallis ja laadukas koulutus
- asiakastyytyväisyyspalaute viranomaisvalvonnan näkökulmasta
- prossien ja suunnitelmallisuuden parantaminen arviointilaitostoiminnassa tulevaisuudessa
- lainsäädännön ja ohjeistuksen muutoksista tiedottaminen ajoissa tulevaisuudessa.

5 Kehittämissuunnitelma

Kehittämissuunnitelman laatimisessa hyödynnettiin Viestintäviraston ja tietoturvallisuuden arviointilaitosten välisen lainsäädäntöön ja dokumentaatioon suoritetun sisällönanalyysin sekä henkilöhaastatteluiden tuloksia. Tulokset analysoitiin ja niiden perusteella tuotiin esiin kehittämistarpeita. Kehittämistarpeet teemoiteltiin valmiiksi laadittujen teemojen alle yllä olevan analysointimenetelmän mukaisesti. Analysoinnin avulla laadittiin kehittämissuunnitelma Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnalle.

Kehittämissuunnitelma luomisessa otettiin mallia Tuomi & Samkin mukaisesta henkilöstön kehittämissuunnitelmasta (Kuvio 8), joka perustuu nykytilanteen tunnistamiseen ja visioon tulevaisuudesta. Kehittämistarpeita verrataan käytössä oleviin resursseihin ja mahdollisuuksiin. Havainnot kehitettävistä kohteista dokumentoidaan, jotta ne voitaisiin muuttaa toiminnaksi. (Tuomi & Sumkin 2012, 58-59.)



Kuvio 8: Henkilöstön kehittämissuunnitelma (Tuomi & Samkin 2012)

Opinnäytetyön avulla saatiin selville kaikki Tuomen ja Samkinin mallin vaiheet. Tiedonkeruumenetelmien avulla saatiin muodostettua Viestintäviraston ja tietoturvallisuuden arviointilaitosten nykytila. Kehittämissuunnitelman visio on yhteistoiminnan parantaminen organisaatioiden välillä. Kehittämistarpeet kerättiin tiedonkeruumenetelmien avulla ja ne dokumentoitiin. Analysoinnin avulla teemoiteltiin kehitettävät kohteet kolmen eri teeman alle prioriteettijärjestyksessä.

Kehittämistä tullaan ohjaamaan 70-20-10-säännön mukaan, jonka mukaan 10% osaamisen kehittämisestä tapahtuu ulkoa ostetun koulutuksen avulla, 20% sisäisen koulutuksen ja osaamisen jakamisen avulla ja 70% työssä oppimalla. (Eosmo 2017.)

Kehittämissuunnitelma esitellään organisaatioiden johdolle heti opinnäytetyön valmistuttua. Kehittämistoiminta aloitetaan täysimittaisesti ensi vuoden alusta suunnitellun mukaisesti. Vuoden 2018 loppuun mennessä tulisi suunnitelman kaksi ensimmäistä teemaa olla käsiteltynä eli välittömästi kehittämistä vaativat asiat ja seuraavan vuoden aikana kehittämistä vaativat asiat.

Kehittämissuunnitelman toteuttamiseksi hyödynnetään Kyberturvallisuuskeskuksen asiantuntijoita osaamista. Tämä edellyttää Kyberturvallisuuskeskuksen hyvää sisäistä yhteistyötä ryhmien välillä. Kehittämissuunnitelman toimenpiteet välittömästi kehittämistä ja seuraavan vuoden aikana vaativista tarpeista on kuvattu alla olevassa taulukossa. (Taulukko 2) Lähitulevaisuudessa kehitettävien tarpeiden toimenpiteet voidaan toteuttaa vastaavalla tavalla. Vastuu niiden toteuttamisesta siirretään kehittämissuunnitelman jalkautuksesta vastaavalle arviointilaitoskoordinaattorille.

Taulukossa kuvataan kehittämistä vaativa toimenpide, miten se toteutetaan, missä aikamääreessä (kk / vuosi) ja kuka vastaa sen toteuttamisesta. Vastuut toteuttamisesta jaetaan neljään kategoriaan:

- A = Arviointilaitoskoordinaattori
- B = NCSA-toiminnon lakimies
- C = NCSA-toiminto
- D = Kyberturvallisuuskeskuksen asiantuntijat

Kategoriat luodaan mahdollisten Kyberturvallisuuskeskuksen henkilövaihdosten vuoksi. Vastuut sidotaan tehtävään tai ryhmään, ei henkilöön. Tällä pyritään varmistamaan suunnitelman jatkuminen mahdollisten henkilöriskien toteutuessa.

Toimenpide	**Toteutus**	**Aika**	**Vastuu**
Prossikuvaus	Prosessikaavion tekeminen	1/2018 mennessä	A
Tapaamiset	Tarvekartoitus ja vuosikellon luonti	1/2018 mennessä	A
Yhdenmukaiset pohjat	Mallipohjien laatiminen	1/2018 mennessä	C

Sähköpostilaatikko	Ryhmäpostilaatikon luominen arviointilaitoksille	1/2018 mennessä	D
Extranet-tila	Tilan järjestely ja koulutus seuraavassa arviointilaitostapaamisessa	1/2018 mennessä	A
Rakentava palaute	Dokumentoidaan omaan toimintaan jatkuvaksi prosessiksi	1/2018 mennessä	A
Valvonta	Raporttitarkastukset, arvioinneilla mukana, valvontasuunnitelma, valvonnan prosessikuvaus, vuosikellon luonti	12/2018 mennessä	C
Koulutus	Koulutuskartoitus, koulutussuunnitelma, tyytyväisyyskysely, ostettu koulutus, vuosikellon luonti	6/2018 mennessä	A +C + D
Työkalut	Tarvekartoitus ja lisenssiehtojen sekä jakomahdollisuuden selvittäminen	6/2018 mennessä	C
Arviointilaitosohje	Tiivistäminen, detaljien poistaminen	12/2018 mennessä	B

Taulukko 2: Kehittämissuunnitelman välittömästi ja seuraavan vuoden aikana toteutettavat toimenpiteet (Viestintävirasto 2017)

Kehittämissuunnitelman jalkauttaminen, arviointi ja seuranta Viestintävirastossa ja tietoturvallisuuden arviointilaitoksissa vastuutetaan Viestintäviraston arviointilaitoskoordinaattorille. Jalkautus tehdään opinnäytetyöstä erillisenä prosessina. Kehittämissuunnitelman seurantaa ja arviointia suoritetaan kvartaaleittain kyselyn avulla.

6 Johtopäätökset

Viestintävirastossa on pyritty kehittämään tietoturvallisuuden arviointilaitosten yhteistoimintaa viraston kanssa aikaisemminkin. Tämä työ on valitettavasti kuitenkin jäänyt kesken johtuen henkilövaihdoksista työtehtävissä. Kehittämistyö vastuutettiin uudelleen opinnäytetyön laatijalle.

Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnan toimintaympäristö on edelleen nuori ja siihen liittyvä lainsäädäntö myös melko tuoretta. Tämä johtaa monesti tilanteisiin, jossa viranomainenkin joutuu tulkintaa määritellessään kysymään lain pykälän perimmäistä tarkoitusta aina lain laatijalta saakka. Viestintäviraston omien prosessien selkeyttäminen, annettava ohjeistus, tuotettava tieto ja yhteistoiminta tietoturvallisuuden arviointilaitosten kanssa tulisi olla mahdollisimman laadukasta ja vaikuttavaa.

Opinnäytetyö on ensimmäinen Viestintävirastossa tehty tutkimus tietoturvallisuuden arviointilaitosten yhteistoiminnan parantamisesta ja kehittämisestä. Toimintatapojen ja -kulttuurin yhtenäistämistä tarkasteltiin huolellisesti valittujen tiedonkeruu- ja analysointimenetelmien avulla. Tutkimusmenetelmiä kartoitettiin kirjallisten lähteiden ja aikaisempien opinnäytetöiden avulla. Näiden avulla pystyttiin valitsemaan tietyt hyväksi todetut menetelmät. Menetelmiksi valittiin sisällönanalyysi, puolistrukturoitu teemahaastattelu ja teemoittelu. Yhteistoiminnan dokumentaatioon perustuvan sisällönanalyysin avulla kerättiin tietoa toiminnan nykytilasta. Puolistrukturoiduilla teemahaastatteluilla tuettiin sisällönanalyysin avulla tehtyjä havaintoja. Sisällönanalyysin tuloksia täsmennettiin haastattelujen avoimilla kysymyksillä. Lopulta vastaukset analysoitiin teemoittelun avulla isompien asiakokonaisuuksien alle kehittämissuunnitelmaa paremmin tukevaksi. Hyvien tiedonkeruu- ja analysointitulosten perusteella voidaan todeta, että opinnäytetyössä käytettyjen tutkimusmenetelmien valinnat olivat tehty hyvin.

Viestintäviraston ja tietoturvallisuuden arviointilaitosten toimintatapojen ja -kulttuurin kehittämistarpeet olivat alustavasti jo tiedostettu ennen opinnäytetyön aloittamista. Tehdyn opinnäytetyön avulla kyettiin osoittamaan myös uusia toiminnassa olevia epäkohtia ja käytännön työhön vaikuttavia kehittämistarpeita. Opinnäytetyö myös tuki näkemystä siitä, että Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnan kehittäminen on tärkeä ja kriittinen tekijä tulevaisuudessa. Opinnäytetyö toteutettiin objektiivisesti ja relevantteja lähteitä hyödyntäen. Käytettyjen tutkimusmenetelmien avulla kyettiin nostamaan toistuvia kehittämisideoita esille, joita oli jo työn suunnitteluvaiheessa otettu esille. Nämä asiat lisäävät opinnäytetyön uskottavuutta.

Opinnäytetyössä asetettiin kaksi tutkimuskysymystä toimintatapojen ja -kulttuurin yhtenäistämisestä ja parantamisesta sekä viranomaisen valvontavastuun parantamisesta.

Opinnäytetyön kannalta keskeisiä tutkimuskysymyksiä olivat:

1. Millaisilla ratkaisuilla toimintatapoja ja kulttuuria Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä voidaan yhtenäistää ja parantaa (nykytila vs. tulevaisuus)?
2. Millaisilla keinoilla toteutetaan viranomaisen valvontavastuu?

Opinnäytetyön tutkimuskysymyksiin saatiin selkeitä vastauksia. Opinnäytetyön tuloksista voidaan vetää johtopäätös, että toimintatavat ja -kulttuuri eivät nykymuodossaan ole riittävän yhdenmukaisia organisaatioiden välillä. Säännöllisten tapaamisten lisäämisellä, koulutusta kohdentamalla, työkaluja vaihtamalla, arviointeja tekemällä, yhdenmukaistamalla dokumentaatiota, prosesseja selventämällä ja tiedonkulkua lisäämällä yhteistyö olisi hedelmällisempää organisaatioiden välillä ja loisi paremman toimintaympäristön yritysturvallisuuden kokonaisvaltaiselle parantamiselle. Näiden toimenpiteiden avulla toimintatapoja ja -kulttuuria pystytään yhtenäistämään ja parantamaan. Viranomaisen valvontaprosessi tulisi olla selkeä ja ennakoitava, niin että arviointilaitostoiminnan kaikki vaiheet olisivat etukäteen suunniteltuja ja kaikille tiedossa. Viranomaisvalvonnan tulisi olla dokumentaatioon perustuvaa ja etukäteen ilmoitettua. Arviointien seuranta pistokoemaisesti nähtiin myös yhtenä viranomaisvalvonnan toteutuskeinona.

Tutkimuskysymyksien valintaa voidaan pitää onnistuneena. Kysymyksiin saatujen vastausten ja opinnäytetyön tuloksena valmistuneen kehittämissuunnitelman avulla Viestintäviraston ja tietoturvallisuuden yhteistoiminnalle annetaan hyviä ja konkreettisia kehittämisideoita toiminnan kehittämisestä.

Kehittämissuunnitelma antaa myös selkeän aikataulun ja toimenpiteet tavoitteen eli yhteistoiminnan parantamiseksi. Suunnitelman toteuttaminen ja seuranta on vastuutettu Viestintäviraston arviointilaitoskoordinaattorin vastuulle. Kehittämissuunnitelma viedään tuotantoon ensi vuoden alussa yhtenä osana Viestintäviraston ohjaus- ja valvontavelvoitetta.

Opinnäytetyöprosessi on ollut omaa ammatillista osaamista rakentava ja erittäin positiivinen kokemus. Työssä on hyödynnetty hyvässä yhteistyössä Viestintäviraston ja tietoturvallisuuden arviointilaitosten näkemyksiä kehitettävistä asioista. Opinnäytetyötä pystytään hyödyntämään myös tulevien arviointilaitosten yhteistoiminnassa.

7 Arviointi

Luotettavuus on keskeinen osa opinnäytetyön tutkimuksen lopputuloksen arviointia. Luotettavuuden arvioinnin keskeisimpiä käsitteitä ovat reliabiliteetti (luotettavuus) ja validiteetti (pätevyys). (Saaranen-Kauppinen, Puusniekka, Kuula, Rissanen & Karvinen 2009, 24-27.) Laadullisen tutkimuksen osalta luotettavuuden arvioinnin suhteen pitää pohtia tutkimuksen johdonmukaisuutta, haastattelukysymyksien vastauksien samankaltaisuutta ja tutkittavien käsitteiden selkeyttä sekä tutkijalle että haastateltaville. Opinnäytetyön asetettuihin tavoitteisiin on vastattu toiminnallisella ja laadullisella tutkimuksella.

Pätevyyden osalta tarkastellaan opinnäytetyön perusteellisuutta ja johtopäätöksien "oikeellisuutta". (Saaranen-Kauppinen ym. 2009, 25-27.) Tavoiteltaessa kehittämistä ei tyypillisesti ole yhtä oikeata totuutta tai täydellisyyttä. Kehittämistavoitteissa haetaan menettelytapoja ja ohjeistuksia, jotka pystyvät elämään muuttuvassa toimintaympäristössä.

Tahtotila arviointilaitostoiminnan kehittämiselle oli nähtävissä jo opinnäytetyötä suunniteltaessa. Viestintävirastossa oli havaittu, että yhteistoiminta Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä ei ollut riittävällä tasolla. Samalla oli halu kohdentaa viranomaisen valvontaa oikeisiin asioihin. Opinnäytetyön tavoite oli tyydyttää tämä havainto ja halu työstä syntyvällä kehittämissuunnitelmalla.
Opinnäytetyötä kirjoitettaessa havainto yhteistoiminnan tason riittämättömyydestä vain vahvistui. Riittämättömyyttä todennettiin puolistrukturoitujen teemahaastatteluiden, sisällönanalyysin ja teemoittelun avulla. Opinnäytetyön toteuttaminen aiheutti aluksi huolta työn tekijällä mutta alun epävarmuus karisi nopeasti pois. Tiedonkeruu- ja analysointimenetelmät soveltuivat työhön erittäin hyvin. Menetelmien avulla saatiin konkreettisia kehittämisideoita, joita voidaan hyödyntää yhteistoiminnan kehittämisessä. Työn edetessä laatijan oma motivaatio ja halu kehittää yhteistoimintaa nousivat uudelle tasolle.

Opinnäytetyön luotettavuutta ja pätevyyttä pyrittiin varmistamaan eri menetelmillä. Haastattelurunkoa testattiin kolmeen kertaan, kolmella eri henkilöllä. Runkoa muokattiin jokaisen kerran jälkeen. Tällä haluttiin varmistua siitä, että haastattelukysymykset ymmärretään. Haastattelut myös nauhoitettiin haastateltavien suostumuksella. Nauhoitusten ja työn laatijan omien muistiinpanojen avulla varmistuttiin vastauksien oikeellisuudesta. Niiden avulla voitiin myös tarvittaessa palata annettuihin vastauksiin. Sisällönanalyysi toteutettiin järjestelmällisesti dokumentaatioon aihealue kerrallaan. Analyysin tulosten avulla saatiin epäkohdat yhdenmukaisesta raportoinnista esille. Tätä näkemystä vahvistivat myös haastattelusta saadut tulokset. Opinnäytetyön tuloksena syntynyt kehittämissuunnitelmaan on laadittu toimenpiteet, aikataulut ja vastuut. Kehittämissuunnitelma on helppo toteuttaa niiden avulla.

Aikaisempia tutkimuksia ei pystytty hyödyntämään, koska aikaisempia tutkimuksia ei ole tehty. Vertailua vastaavaan toimintaan ei myöskään alan yksityiskohtaisuuden ja vahvan reguloinnin vuoksi ollut mahdollista tehdä. Opinnäytetyön tietoperusta on vahvasti lainsäädäntöön, määräyksiin ja dokumentaatioon perustuvaa. Opinnäytetyön tulosten analysointi ja kehittämissuunnitelman laatiminen perustuu työn laatijan omaan tulkintaan.

Opinnäytetyö on johdonmukainen ja etenee suunnitellun mukaisesti. Työ syvensi tekijän tietämystä organisaatioiden yhteistoiminnasta ja vallitsevasta lainsäädännöstä. Työllä on myös suora vaikutus suomalaisen yritysturvallisuuden laadun parantumiseen ja Viestintäviraston maineeseen. Opinnäytetyö vastaa asetettuihin tutkimuskysymyksiin. Yhtä lailla opinnäytetyön tavoite täyttyy kehittämissuunnitelmalla. Opinnäytetyötä on toteutettu Viestintäviraston asiantuntijoiden ja tietoturvallisuuden arviointilaitosten henkilöstön kanssa hyvässä yhteistyössä.

Valtioneuvoston kanslian tuore selvitys Suomen kyberturvallisuuden nykytilasta antaa huolestuttavan kuvan:

> "Suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä riittävällä tavalla suojattu erilaisia kyberuhkia vastaan ja myös häiriötilanteiden sietokyky on edelleen osassa suojattavia kohteita heikolla tasolla"

Selvityksen mukaan tavoitetilassa vuonna 2020 Suomessa kyberturvallisuus on digitaalisen yhteiskunnan sisäänrakennettu ominaisuus, mikä mahdollistaisi kaikkien toimijoiden luotettavasti hyödyntää yhteiskunnan kaikkia digitaalisia ratkaisuja turvallisesti. Opinnäytetyön laatijan näkemyksen mukaan viranomaisten salassa pidettävän tiedon sähköinen käsittely ja säilyttäminen tulevat tämän tavoitetilan myötä kasvamaan räjähdysmäisesti. Digitaalisten ratkaisujen luotettava ja turvallinen hyödyntäminen tarkoittaa ratkaisujen tietoturvallisuuden tason arviointia tai hyväksyntää. Viestintäviraston ja tietoturvallisuuden arviointilaitosten tehtävämäärät lisääntyvät, mikäli tavoitetila täyttyy. Tämä avaa jatkotutkimusmahdollisuuden Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhteistoiminnalle. Näkökulmana voisi olla yhteistoiminnan järkevä laajentaminen ja resursointi.

Opinnäytetyön pienestä viivästyksestä huolimatta työn laatija pitää opinnäytetyötä onnistuneena tuotoksena. Laatijan näkemyksen mukaan tehty työ on myös hyödyllinen. Opinnäytetyön tekijä sai työn toteuttamisen myötä uuden kipinän jatko-opiskelulle. Toimeksiantajan palaute on myös ollut positiivista koko toteutuksen ajan. Toimeksiantaja on todennut esitetyt kehittämisideat realistisiksi ja yhteistoimintaa aidosti hyödyttäviksi.

Lähteet

Kirjalliset lähteet

Aaltola, J. & Valli, R. 2001. Ikkunoita tutkimusmetodeihin I: metodin valinta ja aineistonkeruuvirikkeitä aloittelevalle tutkijalle. Jyväskylä: PS-kustannus.

Hirsjärvi, S. & Hurme, H. 2009. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13.-14., osin uudistettu painos. Helsinki: Tammi.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Pohjonen, R. 2002. Tietojärjestelmien kehittäminen. Jyväskylä: Docendo Finland.

Saaranen-Kauppinen, A., Puusniekka, A., Kuula, A., Rissanen, R. & Karvinen, I. 2009. Toinen vedos. Menetelmäopetuksen tietovaranto. Tampere: Tampereen yliopisto.

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. 6. Uudistettu laitos. Helsinki: Tammi.

Tuomi, L & Sumkin, T. 2012. Osaamisen ja työn johtaminen. Helsinki: Sanoma Pro.

Sähköiset lähteet

Comparitech Limited. 2017. Cyber security and internet statistics by country. Viitattu 30.10.2017. https://www.comparitech.com/blog/information-security/cyber-security-statistics/

eOSMO. 2017. Kehittämissuunnitelmien laatimiseen hyviä käytäntöjä. Viitattu 15.11.2017. http://www.eosmo.fi/tyokirja/extrat/extra4-2.html

European Union Agency for Network and Information Security. Cyber Security in the Age of IoT and AI. Viitattu 14.11.2017. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-age-of-iot-and-ai

Finnish Accreditation Service. 2017. Akkreditointiprosessi. Viitattu 30.10.2017. https://www.finas.fi/akkreditointi/Akkreditointiprosessi/Sivut/default.aspx

Iltalehti. 2017. Poliisin vakava virhe: Viestejä Putinin Suomen-vierailusta vuoti ulkopuolisen sähköpostiin. Viitattu 3.11.2017. http://www.iltalehti.fi/kotimaa/201708072200309013_u0.shtml

Inspecta Sertifiointi Oy. 2017. Inspecta on Viestintäviraston hyväksymä tietoturvallisuuden arviointilaitos. Viitattu 24.10.2017. https://www.inspecta.fi/Tiedotus/Uutishuone/uutiset/2017/inspecta-on-viestintaviraston-hyvaksyma-tietoturvallisuuden-arviointilaitos/

KPMG IT Sertifiointi Oy. 2014. KPMG:stä Suomen ensimmäinen virallinen tietoturvallisuuden arviointilaitos. Viitattu 24.10.2017.
https://home.kpmg.com/fi/fi/home/media/lehdistotiedotteet/2014/10/kpmg-suomen-tietoturvallisuuden-arviointilaitos.html

Microsoft. 2017. Microsoft Security Intelligence Report. Viitattu 30.10.2017.
https://www.microsoft.com/en-us/security/intelligence-report

Nixu Certification Oy. 2016. Tietoturvallisuuden arviointilaitos. Viitattu 24.10.2017.
https://www.nixu.com/fi/palvelualueet/tietoturvallisuuden-arviointilaitos

Ministry of Justice of Sweden. 2017. A national cyber security strategy. Viitattu 30.10.2017.
http://www.government.se/49edf4/contentassets/b5f956be6c50412188fb4e1d72a5e501/fact-sheet-a-national-cyber-security-strategy.pdf

Office of the Director of National Intelligence. Worldwide threat assessment of the US intelligence community. Viitattu 14.11.2017.
https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf

Puolustusvoimien tutkimuslaitos. 2017. Kvanttilaskenta ja kyberturvallisuus. Viitattu 31.10.2017.
http://puolustusvoimat.fi/documents/1948673/2104503/PVTUTKL+Tutkimuskatsaus+1-2017.pdf/fc2dd702-919f-4395-a385-0fc391525ff8

RCR Wireless News. Reality check: 50B IoT devices connected by 2020. Viitattu 5.6.2017.
http://www.rcrwireless.com/20160628/opinion/reality-check-50b-iot-devices-connected-2020-beyond-hype-reality-tag10

Ruotuväki. 2017. Kyha17-kyberharjoitus haastaa valtiohallinnon. Viitattu 1.11.2017.
http://ruotuvaki.fi/-/kyha17-kyberharjoitus-haastaa-valtiohallinnon

Sisäministeriö. 2017. Kyberrikollisuus ylittää rajat tietoverkoissa. Viitattu 6.11.2017.
http://intermin.fi/poliisiasiat/kyberrikollisuus

Teknologiateollisuus. Kvanttitietokone mullistaa tulevaisuuden tietojenkäsittelyn. Viitattu 14.11.2017. http://teknologiateollisuus.fi/fi/ajankohtaista/uutiset/kvanttitietokone-mullistaa-tulevaisuuden-tietojenkasittelyn

Turvallisuuskomitea. 2015. Suomen kyberturvallisuusstrategia. Viitattu 19.4.2017.
http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia

Ulkoministeriö. 2015. Kyberturvallisuus ja kybertoimintaympäristö. Viitattu 17.10.2017.
http://formin.finland.fi/public/default.aspx?nodeid=49571&contentlan=1&culture=en

Valtioneuvoston kanslia. 2017a. Valtioneuvoston puolustusselonteko. Viitattu 17.10.2017.
http://www.defmin.fi/files/3683/J05_2017_VN_puolustusselonteko_Su_PLM.pdf

Valtioneuvoston kanslia. 2017b. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Viitattu 31.10.2017.
http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Valtiovarainministeriö. 2008. Valtionhallinnon tietoturvasanasto. Viitattu 20.11.2017.
https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

Valtiovarainministeriö. 2016a. Pilkahduksia tulevaisuuteen. Viitattu 5.6.2017. http://vm.fi/documents/10623/3507992/Pilkahduksia+tulevaisuuteen+%E2%80%93+digitalisaation+ja+robotisaation+mahdollisuudet+-raportti/e7154bd3-910a-4f99-89ee-4f9299043d3c

Valtiovarainministeriö. 2016b. Lakiuudistus parantaa tietosuojaa EU:ssa. Viitattu 3.2.2017. http://vm.fi/artikkeli/-/asset_publisher/lakiuudistus-parantaa-tietosuojaa-eu-ssa-tuore-raportti-uudistuksesta-antaa-suosituksia-muutosvaiheeseen

Viestintävirasto. 2016a. Ohje tietoturvallisuuden arviointilaitoksille 210/2016 O. Viitattu 19.4.2017.

Viestintävirasto. 2016b. Toimintasuunnitelma 2014-2016. Viitattu 23.10.2017. https://www.viestintavirasto.fi/attachments/Kyberturvallisuuskeskus_toimintasuunnitelma_2014-2016.pdf

Viestintävirasto. 2017a. 10 tietoturvanäkymää vuodelle 2017. Viitattu 23.10.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/01/ttn201701171301.html

Viestintävirasto. 2017b. Tietoturvallisuuden arviointilaitokset. Viitattu 19.4.2017. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvallisuudenarviointilaitokset.html

Viestintävirasto. 2017c. Kyberturvallisuus. Viitattu 20.11.2017. https://www.viestintavirasto.fi/kyberturvallisuus.html

Viestintävirasto. 2017d. Historia. Viitattu 12.10.2017. https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/historia.html

Viestintävirasto. 2017e. Viraston esittely ja tehtävät. Viitattu 19.4.2017. https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat.html

Viestintävirasto. 2017f. Viestintäviraston toimialat. Viitattu 23.10.2017. https://www.viestintavirasto.fi/viestintavirasto/virastonesittelyjatehtavat/toimialat.html

Viestintävirasto. 2017g. Tietoturvasta vastaavat viranomaiset. Viitattu 23.10.2017. https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/muidenviranomaistentietoturvapalvelut.html

Viestintävirrasto. 2017h. Viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Viitattu 25.10.2017. https://www.viestintavirasto.fi/attachments/Viestintaviraston_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

Julkaisemattomat lähteet

Haastattelu A. 2017. Haastattelu 10.8.2017. Viitattu 5.11.2017.

Haastattelu B. 2017. Haastattelu 10.8.2017. Viitattu 5.11.2017.

Haastattelu C. 2017. Haastattelu 11.8.2017. Viitattu 5.11.2017.

Haastattelu D. 2017. Haastattelu 11.8.2017. Viitattu 5.11.2017.

Haastattelu E. 2017. Haastattelu 15.8.2017. Viitattu 5.11.2017.

Haastattelu F. 2017. Haastattelu 15.8.2017. Viitattu 5.11.2017.

Virallislähteet

ISO/IEC 27001:2013

Laki kansainvälisistä tietoturvallisuusvelvotteista (588/2004)

Laki tietoturvallisuuden arviointilaitoksista (1045/2011)

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)

Turvallisuusselvityslaki (726/2014)

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)

Kuviot

Taulukot

Liitteet

Liite 1: Tutkimuksen henkilöhaastattelukysymykset

1. Nykytila

- Miten yhteistyö Viestintäviraston ja tietoturvallisuuden arviointilaitosten välillä on toteutunut? Arvioikaa yhteistyön toteutuminen asteikolla 1 - 5 (1=huono ja 5=erinomainen).
- Minkälaisia kehitettäviä asioita näette yhteistyössä?
- Viestintävirasto valvoo ja ohjaa tietoturvallisuuden arviointilaitoksia. Miten Viestintäviraston tehtävä on toteutunut? Arvioikaa ohjaamisen toteutuminen asteikolla 1 - 5 (1=huono ja 5=erinomainen).
- Oletteko kokeneet että Viestintävirasto ohjaa arviointilaitoksia liian vähän, riittävästi, liian paljon?

2. Toiminnan kehittäminen

- Miten arvioitte oman organisaationne osaamisen tasoa arviointilaitostoiminnassa asteikolla 1 - 5 (1=huono ja 5=erinomainen)?
- Millaisilla keinoilla osaamista voitaisiin kehittää?
- Miten organisaationne on toteuttanut arviointilaitostoiminnassa henkilöstön vaihtuvuuden / toiminnan jatkuvuuden / tietotaidon siirtymisen? Arvioikaa toimintojen toteutuminen asteikolla 1 - 5 (1=huono ja 5=erinomainen).
- Millaisilla keinoilla toteutatte nämä toiminnot organisaatiossanne?

3. Yhdenmukaisuus

- Arvioikaa asiakasnäkökulmasta Viestintäviraston ja tietoturvallisuuden arviointilaitosten yhdenmukaisuutta (toimintatavat, prosessit, arvioinnit, lopputulos jne.) asteikolla 1 - 5 (1=huono ja 5=erinomainen).
- Minkälaisia lomakkeita organisaatiossanne käytetään arvioinneissa (suunnitelma, raportti, todistus)? Ovatko ne arvioijien kesken samanlaisia vai kaikilla omia?
- Näettekö mahdollisesti samankaltaiset (organisaatioiden omilla yksityiskohdilla) suunnitelmat, raportit tai todistukset Viestintävirastolla ja tietoturvallisuuden arviointilaitoksilla positiivisena vai negatiivisena asiana?
- Millaisilla keinoilla Viestintäviraston ja tietoturvallisuuden arviointilaitosten suorittamia arviointeja voitaisiin yhtenäistää?

4. Koulutus

- Millainen on Viestintäviraston tarjoama koulutuksen taso? Arvioikaa koulutuksen taso asteikolla 1 - 5 (1=huono ja 5=erinomainen).
- Kuinka usein mielestänne koulutus olisi vähintään tarpeellista?
- Minkälainen koulutus olisi mielestänne hyödyllisintä?
- Mitä kehitettävää tai mahdollisia ongelmakohtia näette Viestintäviraston koulutuksessa?

5. Viranomaisvalvonta

- Miten viranomaisen valvontavastuu toteutuu Viestintäviraston osalta? Arvioikaa valvonnan toteutuminen asteikolla 1 - 5 (1=huono ja 5=erinomainen).
- Millaisilla keinoilla viranomaisen valvontavastuu tulisi mielestänne toteuttaa jatkossa?

6. Tulevaisuus

- Arvioikaa tarve Viestintäviraston ja tietoturvallisuuden arviointilaitosten toiminnalle seuraavina lähivuosina asteikolla 1 - 5 (1=vähäinen ja 5=suuri).
- Mitkä ovat mielestänne lähivuosien suurimmat uhat arviointilaitostoiminnalle?
- Antakaa vapaa sananne arviointilaitostoiminnan kehittämisestä?