Elias Laine

TIETOTURVALLISUUDEN HALLINTA KUNNISSA – PROSESSI JA SEN VAIHEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Laine, Elias
Tietoturvallisuuden hallinta kunnissa – Prosessi ja sen vaiheet
Jyväskylä: Jyväskylän yliopisto, 2023, 49 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Tutkimuksessa tarkastellaan pienten ja keskisuurten kuntien tietoturvallisuuden hallintaprosessia sekä tiedonhallintalain vaatimuksia. Tutkimuksen tavoitteena oli selvittää pienten ja keskisuurten kuntien tietoturvallisuuden hallinnan taso ja siihen vaikuttavat tekijät. Tämän pohjalta tutkimuksessa rakennettiin ISO27001:n pohjautuva malli tietoturvallisuuden hallintaprosessista kunnille. Esiteltävä malli on yhdenmukaistava ja kokoava, joka toimii pohjana organisaatiokohtaisen mallin kehittämiselle.

Tutkimus toteutettiin kirjallisuuskatsauksena ja teemahaastatteluna. Tutkimuksen viitekehyksenä toimi ISO27001- standardi. Kirjallisuuskatsauksessa pureuduttiin tietoturvallisuuden hallintaprosessiin ja sen vaiheisiin. Kirjallisuuskatsauksen aineistoa kerättiin tutkimukseen kansallisesta lainsäädännöstä ja ohjeista sekä kansainvälisistä ohjeista ja standardeista. Teemahaastattelut toteutettiin kolmen eri kunnan tietoturvaan perehtyneen henkilön haastatteluna. Haastatteluilla pyrittiin saamaan kattava kuvaus tietoturvallisuuden hallinnasta ja tiedonhallintalain toteutumisesta pienissä ja keskisuurissa kunnissa.

Tutkimuksen perusteella tietoturvallisuuden hallinta ja siihen vaikuttavat tekijät vaihtelivat kunnittain. Tietoturvallisuuden hallintaa ei kaikilta osin ollut toteutettu kunnissa kokonaisuutena vaan yksittäisinä toimenpiteinä. Tutkimuksen perusteella kuntien tietoturvallisuuden hallintaan vaikuttivat osaltaan käytettävissä olevat resurssit sekä ohjauksen hajanaisuus. Tiedonhallintalain vaatimuksien osalta tutkimukseen osallistuneet kunnat olivat tehneet toimenpiteitä, mutta kokonaisuudessaan vaatimuksiin ei ollut päästy. Tiedonhallintalain vaatimuksien täyttämiseksi tutkimukseen osallistuneet henkilöt toivoivat ohjausta ja yhdenmukaisia toimintamalleja vaatimusten toteuttamiseksi.

Asiasanat: tietoturvallisuuden hallinta, kuntien tietoturva, tietoturvallisuuden prosessi

ABSTRACT

Laine, Elias
Tietoturvallisuuden hallinta kunnissa – Prosessi ja sen vaiheet
Jyväskylä: University of Jyväskylä, 2023, 49 pp.
Cyber Security, Master's Thesis
Supervisor: Lehto, Martti

This study examines the information security management process of small and medium-sized municipalities and the requirements of the Finnish data management act. The aim of the study was to find out the level of information security management in small and medium-sized municipalities and the factors that affecting it. Based on this, the research built a model of the information security management process for municipalities based on ISO27001. The presented model is harmonizing and collecting, which serves as a basis for the development of an organization-specific model.

The research was carried out as a literature review and thematic interview. The ISO27001 served as the research framework. The literature review discussed the information security management process and its stages. The material of the literature review was collected from national legislation and guidelines as well as international guidelines and standards. Thematic interviews were carried out as an interview with three people familiar with information security in different municipalities. The interview aimed to get a comprehensive description of information security management and the implementation of the Finnish data management act in small and medium-sized municipalities.

Based on the research, information security management and the factors affecting it varied by municipality. Information security management had not been implemented in all aspects in the municipalities as a whole, but as individual measures. Based on research, the municipalities' information security management was partly influenced by the available resources and the fragmentation of control. Regarding the requirements of the Finnish data management act, the municipalities that participated in the study had taken measures, but the requirements has not been fully met. In order to meet the requirements of the data management act, the people who participated in the study wanted guidance and uniform operating models to implement the requirements.

Keywords: information security management, information security in municipalities, information security process

KUVIOT

SISÄLLYS

1 JOHDANTO

1.1 Tutkimuksen tausta

Vuonna 2020 Jarkko Hännisen pro gradu -tutkielma ”Riskienhallinta pienien ja keskisuurien kuntien digitaalisessa turvallisuudessa - tapaustutkimus” käsitteli kuntien digitaalisen turvallisuuden ja riskienhallintaan liittyviä käytänteitä. Tutkimuksessaan Hänninen toteaa, että tutkimuksen perusteella digiturvallisuuden ja riskienhallinnan käytänteet eroavat kuntakohtaisesti. Tutkimuksen perusteella keskisuurien kuntien käytänteet ovat paremmalla tasolla, kuin pienissä kunnissa, mutta tarvetta digitaalisen turvallisuuden kehittämiselle löytyy lähes kaikissa kunnissa. Hänninen toteaa, että pienien ja keskisuurien kuntien digitaalisen turvallisuuden tutkimukselle on edelleen tarvetta. Jatkotutkimusehdotuksena Hänninen mainitsee digitaalisen turvallisuuden osa-alueiden syvällisemmän tai laajemman tutkimuksen. (Hänninen, 2020)

Tietoturvallisuuden hallintaan liittyvää kansallista ohjeistusta ylläpitää Valtiovarainministeriön VAHTI- verkosto (jota ylläpitää nykyisin Digi- ja väestötietovirasto), joka tuottaa julkaisuja tietoturvallisuuteen liittyen. Julkaisujen tarkoituksena on tuottaa parhaita käytäntöjä turvallisuuden eri osa-alueiden kehittämiseen. Julkaisut sisältävät laajasti materiaalia tietoturvallisuuden hallintaan liittyen, mutta kokoavaa ja helppokäyttöistä ohjetta kuntien tietoturvallisuuden hallintaan ei ole. Hännisen tutkimuksen (2020) lisäksi Tammelin (2021) tutkimuksen ”Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa” perusteella ohjeistusta on paljon, mutta yhdenmukaista tietoturvallisuuden hallintaa ei ole toteutettu pienissä ja keskisuurissa kunnissa.

Tietoturvallisuuden hallintaan kunnissa vaikuttaa muun muassa resurssit tietoturvatyön toteuttamiseen ja osaavan henkilöstön puute. Tämän vuoksi varsinkin pienissä kunnissa tietoturvallisuuden hallinta voidaan nähdä ennemmin reagoivana kuin ennakoivana toteutuksena. Keskisuurissa kunnissa resurssit ovat paremmat, joka heijastuu muun muassa riskienhallinnan tasoon. (Hänninen,

2020). Valtiovarainministeriön (2022a) selvityksen mukaan kuntien digitaalisen turvallisuuden osaamisessa ja resursoinnissa on suurta vaihtelua.

Valtiovarainministeriön (2022a) selvityksessä käy ilmi, että digitaalisen turvallisuuden toteuttamisesta on olemassa paljon määräyksiä, ohjeita, vaatimuksia, suosituksia ja työkaluja. Näiden osalta ei kuitenkaan ole selvää, mitkä niistä ovat velvoittavia. Tämän lisäksi ne ovat osittain ristiriidassa keskenään. Selvityksen perusteella kaikki julkiselle hallinnolle tarpeelliset digitaalisen turvallisuuden ohjeet ja määräykset olisi saatava samasta paikasta ja niiden olla keskenään ristiriidattomia. (Valtiovarainministeriö, 2022a)

Tutkimuksen tavoitteena on tarkastella tietoturvallisuuden hallintaa prosessina, jossa huomioidaan tietoturvallisuuden hallinnan tärkeimmät vaiheet. Tietoturvallisuuden hallinnan perustana toimii riskienhallinta prosessi, jolla pystytään selvittämään organisaation tietoturvallisuuden tilaa ja havaitsemaan tietoturvaan liittyvä ongelmakohtia. Tämä on tärkeää, jotta tietoturvallisuuden hallintajärjestelmä voi saavuttaa sille asetetut tavoitteet (Suomen standardisoimisliitto, 2022a).

Kansallisessa lainsäädännössä on otettu kantaa tietoturvallisuuden toteuttamiseen monelta osin. Viimeisimpänä ja vaikuttavimpana on Laki julkisen hallinnon tiedonhallinnasta 906/2019, joka tunnetaan myös nimellä tiedonhallintalaki. Tässä laissa määritellään tarkasti vaatimuksia tietoturvan toteuttamiseen julkisella sektorilla. Voidaan kuitenkin todeta, että muissa laeissa olevat vaatimukset ovat vaikeasti havaittavissa ja niiden hajanaisuus muodostaa vaatimuksien määrittelystä osin haastavaa.

1.2 Tutkimuksen tavoite, tutkimuskysymykset ja tietoturvallisuuden määritelmä

Tutkimuksen tavoitteena on vastata seuraaviin pääkysymyksiin:

- Miten tietoturvallisuuden hallinta tulisi toteuttaa pienissä ja keskisuurissa kunnissa?

Tutkimuksen apukysymyksinä ovat:

- Miten tietoturvallisuuden hallinta toteutetaan pienissä ja keskisuurissa kunnissa?
- Miten pienet ja keskisuuret kunnat ovat toteuttaneet tiedonhallintalain vaatimukset tietoturvaan liittyen?

Tutkimus toteutetaan laadullisena tapaustutkimuksena ja aineisto analysoidaan sisällönanalyysin menetelmin. Aineistoin keruumenetelmät ovat kirjallisuuskatsaus sekä teemahaastattelu. Tutkimuksen viitekehyksenä toimii ISO27001- standardin tietoturvallisuuden hallintajärjestelmän Plan, Do, Check, Act- malli, joka on vertailukohtana tutkimuksen tuloksia analysoitaessa. Tutkimuksen tuloksena

laaditun tietoturvallisuuden hallintaprosessin taustana käytetään ISO27001-standardin sisältämää tietoturvallisuuden hallintajärjestelmää ja sen sisältöä.

Tutkimus rajataan koskemaan tietoturvallisuuden hallintaa hallintaprosessina menemättä sen syvemmälle yksittäisiin toimenpiteisiin tai teknisiin ratkaisuihin. Tutkimuksen tavoitteena on luoda prosessikuvaus, jossa on huomioitu tietoturvallisuuden hallintaan liittyvät vaiheet ja niihin liittyvät vaatimukset kansallisesta lainsäädännöstä. Tutkimuksessa pyritään selvittämään pienten ja keskisuurien kuntien tämänhetkinen tietoturvallisuuden hallinnan taso, odotukset ja niihin vaikuttavat tekijät.

Tietoturvallisuuden termin määrittely perustuu tässä tutkimuksessa ISO 27000 (2016) standardiin, jonka mukaan tietoturvallisuus perustuu tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseen. Näiden lisäksi voidaan tietoturvallisuuden osina nähdä standardin mukaan tiedon aitous, vastuullisuus, kiistämättömyys ja luotettavuus.

2 VAATIMUKSET KUNTIEN TIETOTURVALLISUUTEEN

Valtiovarainministeriö on vuonna 2020 julkaissut Valtioneuvoston periaatepäätöksen, jossa kerrotaan julkisen hallinnon digitaalisen turvallisuuden nykytilasta ja tavoitteista. Periaatepäätöksen julkaisussa on mainittu myös erikseen kuntasektori. (Valtiovarainministeriö, 2020)

Valtiovarainministeriön julkaisussa todetaan, että kuntien toiminnan monialaisuus asettaa haasteita digitaaliselle turvallisuudelle. Julkaisussa mainitaan, että kuntien on vuoteen 2023 mennessä velvoitettu toteuttamaan tiedonhallintalain (laki julkisen hallinnon tiedonhallinnasta, 906/2019) mukaiset tietoturvallisuuden vähimmäisvaatimukset. (Valtiovarainministeriö, 2020)

Laki julkisen hallinnon tiedonhallinasta määrittelee vaatimuksia julkisen sektorin tietoturvasta ja lain tarkoituksena on: ”

1. *Varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi;*
2. *Mahdollistaa viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen, jotta viranomainen voi hoitaa tehtävänsä ja tarjota palvelunsa hallinnon asiakkaille hyvää hallintoa noudattaen tuloksellisesti ja laadukkaasti;*
3. *Edistää tietojärjestelmien ja tietovarantojen yhteen toimivuutta.”*
   (Laki julkisen hallinnon tiedonhallinnasta, 2019)

Laki määrittää tiedonhallintayksiköt, joiden tehtävänä on tiedonhallinnan järjestäminen. Lain mukaan kunta on tiedonhallintayksikkö ja sen tulee huolehtia: ”

1. *Määritelty tässä ja muussa laissa säädettyjen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut;*
2. *Ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta;*
3. *Tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa,*

tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista;

4. *Asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi;*
5. *Järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta."*
   (Laki julkisen hallinnon tiedonhallinnasta, 2019)

2.1 Laki julkisen hallinnon tiedonhallinnasta – vaatimukset tietoturvallisuudelle

Laki julkisen hallinnon tiedonhallinnasta luvussa 4 – tietoturvallisuus, käsitellään tietoturvallisuuteen liittyvät asiat. Luku sisältää pykälät 12–18:"

12 § - Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen
13 § - Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
14 § - Tietojen siirtäminen tietoverkossa
15 § - Tietoaineistojen turvallisuuden varmistaminen
16 § - Tietojärjestelmien käyttöoikeuksien hallinta
17 § - Lokitietojen kerääminen
18 § - Turvallisuusluokiteltavat asiakirjat valtionhallinnossa"
(Laki julkisen hallinnon tiedonhallinnasta, 2019)

Lain 12 §:n mukaan tiedonhallintayksikön on tunnistettava tehtävät, joissa toimijalta vaaditaan luotettavuutta ja varmistettava, että näissä tehtävissä työskenteleville toteutetaan henkilöturvallisuusselvitys.

Lain 13 §:n mukaan tiedonhallintayksikön on:

1. Seurattava toimintaympäristön tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko elinkaaren ajan
2. Selvitettävä olennaiset tietojen käsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimet riskiarvioinnin mukaan
3. Varmistettava tehtävien kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys riittävällä testauksella säännöllisesti
4. Suunniteltava tietojärjestelmät, tietovarantojen rakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa
5. Varmistettava hankintojen osalta, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet

Lain 14 §:n mukaan salassa pidettävien tietojen siirtäminen tulee toteuttaa yleisessä tietoverkossa salattuna tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa

käyttämällä. Lisäksi vastaanottaja on varmistettava tai tunnistettava riittävän tietoturvallisella tavalla ennen kuin hän pääsee käsittelemään salassa pidettävää tietoa.

Lain 15 §:n mukaan tietoturvallisuuden toimenpitein on varmistettava tietoaineiston muuttumattomuus, suojaus, alkuperäisyys, ajantasaisuus, virheettömyys, saatavuus ja käyttökelpoisuus. Lisäksi 15 § määrittää, että tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten mukaisesti turvallisia.

Lain 16 §:n mukaan tietojärjestelmistä vastuussa olevien on määriteltävä tietojärjestelmien käyttöoikeudet käyttäjien tehtäviin liittyvien käyttötarpeiden mukaan ja pidettävä ne ajantasaisena.

Lain 17 §:n mukaan lokitietoja kerätään tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista, jos järjestelmän käyttö edellyttää tunnistautumista tai kirjautumista.

Lain 18 §:ssä määritetään turvallisuusluokiteltujen asiakirjojen merkinnästä. (Laki julkisen hallinnon tiedonhallinnasta, 2019)

Tiedonhallintalautakunta on vuonna 2021 julkaissut suosituskokoelman tiedonhallintalain toteuttamisesta. Siinä opastetaan tiedonhallintalain vaatimusten täyttämisestä. Suosituskokoelmassa (2021) tiedonhallintalautakunta määrittää tiedonhallintalain vähimmäisvaatimukset tietoturvallisuuden osalta seuraavasti:”

1. Tehtävät, joiden suorittaminen edellyttää henkilöiltä erityistä luotettavuutta on tunnistettu, 12 §
2. Toimintaympäristön tietoturvallisuustilaa seurataan, 13.1 §
3. Tietoturvallisuus varmistetaan tiedon elinkaaren ajan, 13.1 §
4. Tietoriskien hallinta ja siihen perustuvat tietoturvatoimet on järjestetty, 13.1 §
5. Tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettu, 13.2 §
6. Julkisuus ja salassapitorakenne on huomioitu tietovarantojen tietorakenteissa, 13.3 §
7. Hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet 13.4 §
8. Salassa pidettävät tiedot on suojattu yleisessä tietoverkossa tietoja siirrettäessä, 14.1 §
9. Tietoaineistojen turvallisuus on varmistettu, 15 §
10. Tietoaineistoja käsitellään riittävän turvallisissa tiloissa, 15.2 §
11. Käyttöoikeudet on määritelty ja hallittu tietojärjestelmissä, 16 §
12. Tarpeelliset lokitiedot on kerätty tietojärjestelmien käytöstä ja luovutuksista, 17 §
13. Turvallisuusluokiteltavista asiakirjoista ja niiden käsittelystä on huolehdittu, 18 §”
    (Valtiovarainministeriö, 2021)

2.2 Muita lainsäädännön vaatimuksia kuntien tietoturvallisuuden hallinnasta

Suomen lainsäädännössä on useita lakeja ja asetuksia, jotka velvoittavat kuntia turvaamaan tietoa ja tiedon käsittely-ympäristöä. Kuntalaissa (410/2015) kuntia velvoitetaan toteuttamaan riskienhallintaa hallinnossa ja taloudessa. Tämän tulee ilmetä myös kunnan toimintakertomuksessa. Yksinomaan tietoturvallisuuteen liittyviä vaatimuksia ei kuntalaki sisällä.

Tietosuojalaissa (1050/2018) täsmennetään EU:n yleistä tietosuoja-asetusta (GDPR) Suomessa. Siinä mainitaan tietoturvaan liittyviä vaatimuksia, jotka velvoittavat myös kuntia rekisterinpitäjinä. 6§:ssä mainitaan, että rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava muun muassa seuraavia toimenpiteitä:

- Rekisterinpitäjän tulee kyetä varmistamaan ja todentamaan henkilötietojen tallennus, muutokset ja siirrot
- Henkilöstön osaaminen parantaminen
- Sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin
- Henkilötietojen pseudonymisointi ja salaaminen
- Käsittelyyn liittyen palveluiden luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, sekä kyky palautua teknisen tai fyysisen vian sattuessa nopeasti
- Teknisen ja organisatoristen toimenpiteiden tehokkuus tietojenkäsittelyn turvallisuuden varmistamiseksi
- Sekä muut tekniset, menettely ja organisatoriset toimenpiteet. (Tietosuojalaki, 2018)

Laki viranomaisen toiminnan julkisuudesta (621/1999) määrittää kunnallisten viranomaisten (kuten kunnan valtuusto, johtokunta ja lautakunnat) toiminnasta. Laki velvoittaa huolehtimaan asiakirjoihin ja tietojärjestelmiin sisältyvän tiedon saatavuudesta, käytettävyydestä, suojaamisesta ja eheydestä. Laki velvoittaa viranomaisen suunnittelemaan ja toteuttamaan asiakirja- ja tietohallintonsa sekä tietojärjestelmät ja tietojenkäsittely siten, että niiden sisältämän tiedon suoja, eheys ja laatu turvataan. Turvaamistoimina laissa mainitaan menettelytavat ja tietoturvajärjestelyt.

3 TIETOTURVALLISUUDEN HALLINTAPROSESSI

Raggad (2010) mukaan tietoturvallisuuden hallinta on prosessi, jolla 1. tunnistetaan organisaation tietoympäristö, määritellään sen kriittisyys ja priorisoidaan sen osuus liiketoiminnasta; 2. tunnistetaan, arvioidaan ja lievennetään riskejä suunnittelemalla riskilähtöinen tietoturvaohjelma; ja 3. toteutetaan organisaation jatkuvaa riskiaseman parantamista tarkastelemalla riskilähtöistä tietoturvaohjelmaa vaatimusten muuttuessa.

Raggad (2010) määrittelee tietoturvallisuuden hallintajärjestelmän viitekehykseksi, joka on jokaisen organisaation kehittämä tapa lähestyä tietoturvallisuutta. Kaikki tietoturvallisuuden toimenpiteet tulisi suunnitella, toteuttaa ja ylläpitää tässä viitekehyksessä. Valtiovarainministeriön (2007) Vahti-ohjeessa 3/2007 mukaan tietoturvallisuuden hallintajärjestelmän tärkeimmät osat ovat tietoturvapolitiikka ja siihen liittyvät asiakirjat sekä riskienhallinta.

Valtiovarainministeriön (2007) Vahti- ohjeessa 3/2007 viitataan ISO/IEC 27001- standardin vuoden 2005 versioon, jossa tietoturvallisuuden perustana toimii kehittämisen ja ylläpidon osalta prosessi ajattelu. ISO/IEC 27001- standardin (2022) prosessi on kirjattu PDCA (Plan, Do, Check, Act) -mallilla, joka sisältää vaiheet:

- Plan (suunnittelu), jossa prosessi käynnistetään, toteutetaan riskienhallinta prosessi ja liiketoimintavaikutusanalyysi ja muodostetaan jatkuvuusstrategia.
- Do (toiminta), jossa Plan vaiheessa suunnitellut ratkaisut toteutetaan vaatimusten täyttämiseksi
- Check (arviointi), jossa toteutetaan seuranta, mittaus, analysointi ja arviointi
- Act (parantaminen), jossa kerättyjen tietojen perusteella toteutetaan parannukset.
  (Valtiovarainministeriö, 2007 & Suomen standardisoimisliitto, 2022a)

3.1 Tietoturvallisuuden suunnittelu

ISO/IEC 27001 (2022) mukaan tietoturvallisuutta suunnitellessa tulee ymmärtää organisaatio ja sen toimintaympäristö. Tämä tarkoittaa sitä, että on ymmärrettävä sisäiset ja ulkoiset asiat, jotka ovat organisaatiolle olennaisia ja vaikuttavat sen tietoturvatavoitteisiin.

Traficomin (2020) julkaisussa ”Kyberturvallisuus ja hallituksen vastuu” käsitellään tietoturvatoimintaan liittyviä vaiheita. Sen ensimmäisessä vaiheessa selvitetään organisaation lähtötilanne ja liiketoimintaan vaikuttavat kriittiset tietoympäristön osat. Tämä tarkoittaa järjestelmien yhteyksiä toisiinsa, pääsynhallinnan tilan sekä kuka omistaa minkäkin verkon ja palvelun. Lähtötilanteen selvittäminen mahdollistaa tarvittavien tietoturvatoimenpiteiden toteuttamisen.

Raggad (2010) mukaan tietoturvallisuuden suunnittelu vaiheessa organisaation tulisi määritellä suojattavat kohteet, tietoturvapolitiikka, turvallisuustavoitteet sekä laajuuden, joka määrittelee turvallisuussuunnitelman syvyyden ja vaatimukset turvallisuustavoitteille.

Valtiovarainministeriön (2007) Vahti- ohjeen mukaan tietoturvallisuuden toteuttamista varten tulee organisaatiolla olla käsitys käytössä olevista ratkaisuista ja periaatteista. Kehittämisen lähtökohtana organisaation tulee tehdä keskeisten toimintojen ja niihin vaikuttavien tietojärjestelmien määrittely sekä toteuttaa riskikartoitus.

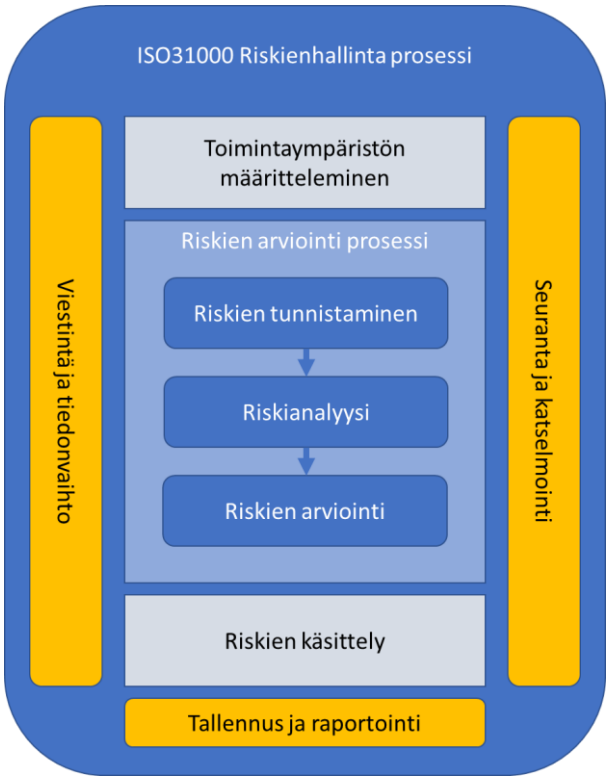
3.2 Riskienhallinta prosessi

Tietoturvallisuuden suunnitteluvaiheessa toteutetaan tietoturvariskien arviointi. (Suomen standardisoimisliitto, 2022a) Riskienhallinta on koko organisaation laajuinen kokonaisuus, jonka tulee kattaa sen kaikki tasot ja olla osana päätöksentekoa ja toimintaa (National Institute of Standards and Technology, 2011). Riskienhallinnan avulla pyritään tunnistamaan uhkat, jotka vaikuttavat jokapäiväiseen toimintaan ja organisaation tavoitteisiin (Valtiovarainministeriö, 2017). Riskienhallinta ei ole kertaluonteinen tapahtuma vaan jatkuva prosessi, johon sisältyy useita vaiheita riippuen käytettävästä mallista.

Wolke (2017) kuvaa riskienhallintaprosessin seuraavasti: Riskien tunnistaminen, riskien mittaaminen/ analysointi, riskien ohjaus ja riskienhallinta. NIST-julkaisussa 800-39 (2011) riskien hallintaprosessi sisältää riskien kehystämisen (strategia, jolla prosessi toteutetaan), riskien määrittelyn ja arvioinnin, riskeihin vastaamisen ja riskien seurannan.

ISO 31000- standardin mukaan riskienhallintaprosessi (kuvio 1) sisältää toimintaympäristön määrittämisen, riskienarvioinnin (riskien tunnistaminen, riskien analysointi, riskien arviointi) ja riskien käsittelyn. Prosessiin liittyy myös viestintä ja konsultointi, seuranta ja tarkastelu sekä raportointi. (International Organization for Standardization, 2018)

Raggad (2010) mukaan riskienhallinta on toimintaa, jolla riskit pidetään organisaatiolle hyväksytyllä tasolla. Prosessi sisältää riskisuunnitelman, riskianalyysin, jossa riskit tunnistetaan ja arvioidaan, riskienkäsittelyn ja riskien seurannan.



Kuvio 1: Riskienhallintaprosessi ISO 31000 mukaan.
(International Organization for Standardization, 2018)

3.2.1 Riskienhallinta suunnitelma

Riskienhallintaa voidaan toteuttaa monella eri tasolla ja eri laajuudessa organisaation mukaan. Tässä vaiheessa on tärkeää määritellä riskien arvioinnin kohde, siihen vaikuttavat tekijät (sisäiset ja ulkoiset) ja asettaa rajat tarkasteltavana olevalle kohteelle. Lisäksi on määriteltävä vastuut ja roolit riskienhallintaprosessin toteuttamisessa. ISO 31000- standardin mukaan riskienarviointiprosessin alussa tulee myös määritellä riskien hyväksymiskriteerit ja riskien arvioinnin suorittamista koskevat kriteerit. (International Organization for Standardization, 2018; Valtiovarainministeriö, 2017)

NIST 800-39- julkaisun (2011) riskienhallintaprosessin ensimmäisessä vaiheessa organisaation tulisi määritellä riskienhallinta ympäristö, jossa riskeihin perustuvia päätöksiä tehdään. Tämän vaiheen tarkoituksena on määritellä riskienhallintastrategia, jonka mukaan riskejä arvioidaan, käsitellään ja seurataan. Lisäksi tulee määritellä riskinsietokyky eli organisaatioon kohdistuvien riskien hyväksyttävä taso.

Raggad (2010) mukaan suunnitteluvaiheessa kehitetään ja dokumentoidaan valittu prosessi ja tavat riskienhallinnalle. Lisäksi määritellään

riskianalyysin kohdeympäristö, riskien käsittely suunnitelma ja määritellään tarvittavat resurssit.

3.2.2 Riskien tunnistaminen

Riskienhallintaprosessin ensimmäisessä vaiheessa määritellään riskit riskienhallinnan kohteena olevasta ympäristöstä. Wolke (2017) mukaan riskien tunnistamiseen ei ole yhtä ainoaa tapaa, koska organisaatioiden toimintaympäristöt ja tavoitteet eroavat toisistaan.

ISO 31000- standardin (2018) mukaan riskien tunnistamisvaiheen tarkoituksena on löytää, havaita ja kuvata riskit, jotka vaikuttavat organisaation tavoitteisiin ja riskien arvioinnin kohdealueeseen. NIST 800-39- julkaisun riskien tunnistamisvaiheessa pyritään löytämään uhat ja haavoittuvuudet organisaation tietojärjestelmissä ja ympäristöissä, joissa järjestelmät toimivat. Tunnistamisvaiheessa kirjataan kaikki riskit, jotka uhkaavat organisaation toimintaa, kuitenkaan puuttumatta niiden vaikutuksiin vielä sen syvemmin (Valtiovarainministeriö, 2017).

3.2.3 Riskien arviointi

ISO 31000- standardissa (2018) riskianalyysi ja riskien merkityksen arviointi on eritelty eri vaiheisiin. Analyysivaiheessa arvioidaan riskien todennäköisyyttä ja vaikutusta. Analyysivaiheessa tulisi ottaa huomioon riskilähteet, seuraukset, todennäköisyydet ja vaikutukset. Analyysitekniikan valinta riippuu monesta eri tekijästä ja siinä voidaan käyttää joko määrällistä tai laadullista menetelmää, tai näiden yhdistelmää. Riskien merkityksen arvioinnissa ISO 31000- standardin mukaan arvioidaan riskianalyysin tuloksia aikaisemmin määriteltyihin riskikriteereihin ja arvioidaan, että mitkä riskit vaativat toimenpiteitä. (International Organization for Standardization, 2018)

Vahti ohjeessa 22/2017 (2017) kuvataan ISO 31000- standardin prosessia. Vahti ohje suosittaa analyysivaiheessa käytettäväksi riskimatriisia (kvantitatiivinen), jossa x- akselilla on vaikutus ja y-akselilla todennäköisyys. Riskimatriisissa todennäköisyydelle ja vaikutukselle annetaan riskikohtaisesti numeerinen arvo, jonka perusteella riski luokitellaan. Riskimatriisi ei ohjeen mukaan ole ainoa tapa ja sen käytössä tulisi ottaa myös huomioon todennäköisyys ja vaikutus erikseen, ei pelkästään näiden yhteen laskettu summa tai tulo. (Valtiovarainministeriö, 2017)

NIST 800-39- julkaisun (2011) toinen vaihe sisältää riskien tunnistamisen lisäksi riskien arviointi osion. Riskien arviointi osiossa arvioidaan riskien vaikutus ja todennäköisyys, joiden perusteella riskien vaikutukset organisaation toimintaan arvioidaan.

3.2.4 Riskien käsittely

ISO 31000- standardissa (2018) riskien käsittely vaiheessa päätetään, kuinka riskejä käsitellään. Tämä vaihe sisältää toimintavaihtoehtojen valinnan, suunnittelun ja toteuttamisen. Toimintavaihtoehtojen valintaan vaikuttaa muun muassa

hyötyjen, kustannusten ja haittojen välinen suhde. Toimintavaihtoehtojen valinnassa voidaan päättää riskin poistamisesta, todennäköisyyden tai vaikutuksen pienentämisestä, riskin jakamisesta tai vähäisen riskin säilyttämisestä. Riskien käsittely vaiheessa on otettava huomioon organisaation velvoitteet ja sitoumukset. (International Organization for Standardization, 2018)

NIST 800-39- julkaisussa (2011) riskien käsittely (tai riskeihin vastaaminen) vaiheessa tunnistetaan, arvioidaan, päätetään ja toteutetaan toimintatavat, joilla riskit hyväksytään, vältetään, lievennetään, jaetaan tai siirretään:

- Riskien hyväksymisen voidaan katsoa olevan välttämätöntä tapauksissa, joissa riski on organisaatiolle hyväksyttävällä tasolla tai riskiin vaikuttaminen aiheuttaisi seurauksia organisaation tai yksilön etuihin.
- Riskien välttäminen (poistaminen) toteutetaan, mikäli riski ylittää organisaatiolle hyväksyttävän tason.
- Riskien lieventäminen toteutetaan, mikäli muut riskien käsittely toimenpiteet eivät ole mahdollisia. Riskien lieventäminen voi tapahtua esimerkiksi erillisellä ohjeella työntekijöille, jotta riskin todennäköisyyttä pienennetään.
- Riskien jakaminen tai siirto toteutetaan, mikäli organisaatiolla on tahto ja kyky siirtää tai jakaa riski organisaation ulkopuolelle. Riskien jakaminen voi olla esimerkiksi vakuutuksen ottamista tai riskin siirtämisestä organisaatiolle, joka on pätevämpi käsittelemään riskiä.
  (National Institute of Standards and Technology, 2020)

Raggad (2010) kuvaa riskien käsittely vaiheen prosessiksi, jossa määritellään, valitaan ja otetaan käyttöön toimenpiteitä, joilla riskit palautetaan hyväksytylle tasolle. Tämä vaihe sisältää ehdot, mitä tulee tehdä, milloin, kuka on vastuussa, aikataulutuksen sekä mahdolliset kustannusarviot.

3.2.5 Riskien seuranta

ISO 31000- standardissa (2018) riskien seuranta ja arviointi vaiheen tarkoituksena on varmistaa ja parantaa prosessien suunnittelua, toteutusta sekä tulosten ja toteutuksen laatua ja tehokkuutta. Seurannan tulee olla jatkuvana osana riskienhallintaprosessia kaikissa sen vaiheissa. Seuranta ja arviointi vaihe sisältää suunnittelun, tiedon keräämisen ja analysoinnin, tulosten kirjaamisen sekä palautteen antamisen.

NIST 800-39- julkaisussa (2011) riskien seuranta vaiheessa varmistetaan, että suunnitellut riskien hallinta toimenpiteet on toteutettu halutulla tavalla, toimenpiteet vaikuttavat oikein ja tuottavat halutun vaikutuksen riskien pienentämiseksi sekä tunnistetaan riskien muutokset.

3.3 Tietoturvatoimenpiteet

Vaatimukset tietoturvatoimenpiteille voivat tulla monesta eri lähteestä. Ulkoisina vaatimuksen lähteinä voi olla esimerkiksi lait, asetukset, toimintaohjeet, direktiivit. Sisäisinä esimerkiksi organisaation politiikka, tehtävät tai riskienhallinta prosessi. (National Institute of Standards and Technology, 2020)

Raggadin (2010) mukaan tietoturvakontrollit ovat kaikki ne toimenpiteet, joilla rajoitetaan tietoturvariskejä. Toimenpiteisiin sisältyy tietoturvapolitiikat, käytännöt, menettelyt ja mekanismit. Raggad (2010) jakaa tietoturvaratkaisut tietoturvallisuuden hallintaan, salakirjoitukseen (kryptologia/ kryptografia), pääsynhallintaan, verkkoliikenteen hallintaan, tietoturvallisuuden analysointiin ja fyysisiin tietoturvatoimiin.

NIST 800-53- julkaisussa (2020) tietoturvakontrollit jaetaan pääsynhallintaan, koulutukseen ja tietoisuuteen, tarkastukseen ja vastuullisuuteen, turvallisuuden arviointiin ja valtuutukseen, konfiguraation hallintaan, jatkuvuuden suunnitteluun, identifiointiin ja todennukseen, poikkeamiin vastaamiseen, ylläpitoon, median turvaamiseen, fyysiseen suojaamiseen, suunnitteluun, henkilöturvallisuuteen, riskienarviointiin, järjestelmien ja palveluiden hankintaan, järjestelmien ja yhteyksien turvaamiseen, järjestelmien ja informaation eheyteen sekä ohjelman hallintaan.

ISO/IEC 27001 (2022) jakaa hallintakeinot organisaatioon liittyviin hallintakeinoihin, henkilöstöön liittyviin hallintakeinoihin, fyysisiin hallintakeinoihin sekä teknologisiin hallintakeinoihin. Valtiovarainministeriön (2022b) Julkri- kriteerit jaetaan hallinnolliseen turvallisuuteen, fyysiseen turvallisuuteen, tekniseen turvallisuuteen, varautumiseen ja jatkuvuuden hallintaan sekä tietosuojaan.

Tässä tutkimuksessa käsitellään hallinnollisina tietoturvatoimenpiteinä tietoturvapolitiikkaa, koulutusta ja organisaation ulkopuolelta hankittavia tietoturvapalveluita. Teknisinä tietoturvatoimenpiteitä käsitellään yleisesti ja fyysisen turvallisuuden osalta käsitellään toimitilaturvallisuutta.

3.3.1 Tietoturvapolitiikka

Riippuen standardista tai ohjeesta, tietoturvapolitiikka toteutetaan tietoturvaprosessin alussa, kuten kansainvälisissä lähteissä tai osana toimenpiteitä, kuten Vahti- ohjeessa. Tähän vaikuttavina tekijöinä voivat olla se, mitä tietoturvapolitiikan halutaan sisältävän. Kansainvälisistä lähteistä voi päätellä, että tietoturvapolitiikka on lyhyt ja ytimekäs kuvaus organisaation johdon tavoitteista ja tahtotilasta. Kun taas Vahti- ohjeessa olevassa mallirungossa tietoturvapolitiikka sisältää paljon laajemmin käsiteltäviä asioita. Yleisesti kuntien tietoturvapolitiikkojen voidaan katsoa sisältävän strategian, politiikan ja käytännön ohjeiden sekoituksen, kuten Tammelin (2021) tuloksissaan toteaa.

Valtiovarainministeriön (2007) Vahti-ohjeen 3/2007 mukaan tietoturvapolitiikka ilmaisee johdon tahtotilan tietoturvallisuuden toteutuksesta, kehittämisestä sekä vastuut. Tietoturvapolitiikkaa ohjaa organisaation strategia, riskianalyysi, lait ja määräykset sekä organisaation toiminnan tarkoitus. Whitmanin

(2008) mukaan onnistuneen tietoturvapolitiikan tulee olla jaettu, luettu, ymmärretty ja hyväksytty työntekijöiden osalta. Tietoturvapolitiikka on kehittyvä asiakirja, jota tulee ylläpitää ajantasaisena organisaation tarpeiden ja ympäristön kehittyessä.

Raggad (2010) mukaan tietoturvapolitiikka ilmaisee tietoturvallisuuden kannalta hyväksyttävän tavan toimia. Raggad (2010) esittelee SANS- instituutin vaatimukset tietoturvapolitiikalle, jossa tulisi olla syy politiikalle, kertoa mitä politiikka kattaa, määritellä yhteyshenkilöt ja vastuut sekä keskustella, kuinka rikkomukset käsitellään. Lisäksi Raggad (2010) kertoo SANS- instituutin määritellyistä avainpolitiikoista, joita jokaisessa organisaatiossa tulisi olla:

- Tiedon luokituksen turvallisuuspolitiikka
- Hyväksyttävän käytön politiikka
- Vähimmäispääsyn politiikka
- Tietoverkkoon pääsyn politiikka
- Etäpääsyn politiikka
- Hyväksyttävän salaamisen politiikka
- Verkko palvelimen turvallisuuspolitiikka
- Sisäisen verkkopalvelun politiikka
- Ohjelmisto palveluntarjoajan politiikka
- Todennustietojen politiikka

Whitman (2008) jakaa tietoturvapolitiikat kolmeen tasoon, joissa jokaisella on oma painopiste ja tarkoitus. Ensimmäisenä yrityksen tietoturvapolitiikka (engl. Enterprise Information Security Policy), joka on organisaation yleinen tietoturvapolitiikka, joka määrittää strategisen tason suunnan kaikille organisaation turvallisuustoimille. Toisena on toimintakohtainen tietoturvapolitiikka (engl. Issue-Specific Security Policy), jossa määritellään organisaation eri teknologioihin ja prosesseihin liittyvät tarkemmat tietoturva lausunnot. Kolmantena on järjestelmä kohtainen tietoturvapolitiikka (engl. Systems-SpecificPolicy), jossa määritellään tietoturvaa järjestelmäkohtaisesti, kuten ketkä kaikki saavat valtuudet käyttää tiettyä järjestelmää.

Tietoturvapolitiikan sisältö on organisaatio riippuvainen. Organisaation yleinen tietoturvapolitiikka voidaan nähdä Whitmanin (2008) tapaan ylätason suunnan näyttäjänä organisaation tietoturvatoiminnalle, joka määrittää strategisen suunnan ja laajuuden kaikille tietoturva toimille. Tämän politiikan pituus on yleensä vain kahdesta viiteen sivua pitkä. Tämän jälkeen tätä ylätason tietoturvapolitiikkaa täydennetään alemman tason tietoturvapolitiikoilla.

Valtiovarainministeriön (2007) Vahti-ohjeen 3/2007 mukaan johto määrittelee tietoturvapolitiikassa tietoturvatoiminnan tavoitteet, vastuut ja toimintalinjat. Tietoturvapolitiikkaa ohjaa organisaation strategia, riskianalyysi sekä lait ja asetukset. Vahti-ohjeessa ei puhuta alemman tason tietoturvapolitiikoista, vaan tietoturvapolitiikka toimii perustana erillisille ohjeistuksille ja suunnitelmille. Valtiovarainministeriön (2007) Vahti-ohje 3/2007 kuvaa tietoturvapolitiikan mallin seuraavasti:

1. Johdanto

2. Tietoturvapolitiikan tavoite
   2.1. Tietoturvallisuuden käsite ja merkitys
   2.2. Määritelmät
3. Tietoturvatoimintaa ohjaavat tekijät
4. Tietoturvallisuuteen kohdistuvat uhat
5. Tietoturvallisuuden merkitys organisaatiolle
   5.1. Toiminnan kannalta elintärkeät palvelutehtävät
   5.2. Tietoturvaperiaatteet
   5.3. Tietoturvallisuuden toteutumista tukevia käytäntöjä
6. Turvatoimien priorisointi
7. Tietoturvallisuuden hallintajärjestelmä
8. Tietoturvavastuut
   8.1. Organisaation tietoturvavastuut
   8.2. Organisaation yhteistyökumppaneiden vastuut
9. Tietoturvakoulutus ja -ohjeet
10. Tietoturvallisuudesta tiedottaminen
11. Tietoturvallisuuden toteutumisen valvonta
12. Toiminta poikkeustilanteissa ja -oloissa

3.3.2 Koulutus

Toimiva tietoturvallisuuden toteuttaminen vaatii organisaatiolta henkilöstön kouluttamista sekä tietoturvatietoisuuden lisäämistä ja ylläpitämistä. Koulutusohjelmaa suunniteltaessa on tärkeää ottaa huomioon organisaation ja työntekijöiden todellinen tarve. NIST SP 800-50 -julkaisussa (2003) tietoturvallisuuden koulutus jaetaan kolmeen osaan: tietoisuus, koulutus ja tutkintoon tai pätevyyteen tähtäävä koulutus. Tietoturvatietoisuudella tarkoitetaan tapahtumia, joissa osallistujien ajattelua pyritään suuntaamaan tietoturvallisempaan suuntaan. Koulutuksella pyritään luomaan tarvittavia tietoturvataitoja ja suurimpana erona tietoisuuden lisäämiseen on, että koulutuksessa henkilön tulisi oppia jokin tietty tietoturvallisuutta lisäävä toimenpide. Tutkintoon tai pätevyyteen tähtäävällä koulutuksella tarkoitetaan esimerkiksi yliopistojen yksittäisiä kursseja tai tutkintoja, joilla organisaatio pyrkii tuottamaan itselleen tietoturva-asiantuntijoita ja ammattilaisia.

Tietoturvallisuuden koulutusohjelma sisältää suunnittelu-, valmistelu- ja toteutusvaiheen. Suunnitteluvaiheessa toteutetaan koulutusmallin jäsentely, tarvearviointi, kehityssuunnitelma, toteutusaikataulu, tavoitteet ja rahoitus. Koulutusmallin jäsentelyssä tehdään päätös, kuka suunnittelee, kehittää ja toteuttaa koulutusohjelman. Tähän voi olla useita malleja, joista NIST SP 800-50 (2003) julkaisussa esitellään kolme yleisintä:

- Malli 1: Keskitetty, jossa vastuu ja rahoitus on keskitetty yhdelle toimijalle organisaatiossa koulutusohjelman osalta. Tämä on käytössä organisaatioissa, jotka ovat kohtalaisen pieniä ja niiden eri osastojen tehtävät ovat pääosin samantyyppisiä.

- Malli 2: Osin hajautettu, jossa tarvearviointi ja koulutusohjelman strategia laaditaan keskitetysti, mutta eri osastot toteuttavat itse koulutuksen ja siihen liittyvän materiaalin. Tämä on käytössä organisaatioissa, jossa osastot sijaitsevat laajalla alueella ja tehtävät ovat erilaisia.
- Malli 3: Hajautettu, jossa organisaation tietoturvasta vastaava toimija antaa ylätason linjaukset ja odotukset koulutuksesta, mutta vastuu on organisaation eri osastoilla. Tämä on käytössä organisaatioilla, joiden yksiköt ovat hyvin itsenäisiä ja tehtävät erilaisia.

Koulutusohjelman tarvearvioinnissa tulisi määrittää ne osa-alueet ja tasot, joita koulutettava henkilöstö tarvitsee. Tässä on huomioitava lähtötason ja tarpeellisen tason ero ja täyttää se. Mikäli tämä ero on suuri, on aloitettava koulutus kriittisimmistä osa-alueista. Tarvearvioinnin pohjalta voidaan luoda suunnitelma koulutusohjelman kehittämiseksi, toteuttamiseksi ja ylläpitämiseksi. Suunnitelman pohjalta luodaan toteutusaikataulu, jossa tehdään päätös siitä, mikä on kriittistä ja koulutettava ensimmäiseksi. Tavoitteet eri koulutusohjelman osalta riippuu koulutettavan henkilön asemasta organisaatiossa sekä vaatimukset tätä asemaa kohtaan tietoturvan osalta. Tavoitteet täytyy asettaa jokaiselle koulutusohjelman tasolle. Rahoituksen osalta tietoturvatietoisuuden lisääminen ja kouluttaminen on nähtävä vähimmäisvaatimuksena, joka on täytettävä. (National Institure of Standards and Technology, 2003b)

Tietoturvan koulutusohjelman valmisteluvaiheessa tärkeimmäksi osaksi muodostuu koulutusmateriaali. Tietoisuuden lisäämisessä pääpainona tulee olla oikeanlaisessa tietoturvakäyttäytymisessä, kun taas koulutuksessa yleisönä on tietty joukko, jolle koulutetaan tiettyä asiaa, joka heidän tulee osata työssään. Tietoisuuden lisäämisessä aiheina voi olla esimerkiksi internetin käyttö tai salasanojen käyttö ja hallinta. Tämän koulutusmateriaalin hankintaan voidaan käyttää yleisiä tietoturvasta kertovia uutis- ja ohjesivustoja sekä organisaation tietoturvaammattilaisia. Tietyille ryhmille tarkoitetussa koulutuksessa tulee arvioida kyseisen tehtävän vaatimukset tietoturvan kannalta ja kouluttaa henkilöstöä sen perusteella. Nämä ryhmät voivat olla esimerkiksi IT-hankinta osasto, jolle tulee kouluttaa hankintoihin liittyvää tietoturva osaamista. Tämänlaiseen koulutuksen materiaaliin liittyen tulee organisaation arvioida, että riittääkö omassa organisaatiossa kyky ja resurssit luoda koulutusmateriaalia vai tuleeko se hankkia ulkopuoliselta palveluntarjoajalta. (National Institure of Standards and Technology, 2003b)

Koulutusohjelman toteutus tulisi aloittaa organisaation tiedottamisella siitä, mitä koulutusohjelmalta odotetaan ja mitkä ovat sen hyödyt. Tietoisuuden lisääminen voidaan toteuttaa usealla eri tavalla. Valittu tapa riippuu käsiteltävän aiheen monimutkaisuudesta ja käytettävissä olevista resursseista. Se voidaan toteuttaa esimerkiksi viikoittain toistuvina uutisviesteinä tai tietoturvapäivinä, vaihtoehtoja on monia. Tietyille ryhmille tarkoitetut koulutukset voidaan toteuttaa esimerkiksi luokkaharjoituksena tai verkkopohjaisesti. Koulutusohjelman toteuduttua on arvioitava sen saavuttamat tulokset sekä kerätä kaikilta prosessiin

osallistuneilta palautetta toiminnasta ja luotava kehityssuunnitelma jatkoa varten. (National Institure of Standards and Technology, 2003b)

Valtiovarainministeriön (2007) Vahti- ohjeessa 3/2007 käsitellään lyhyesti tietoturvakoulutusta, jonka mukaan koulutuksen suuntaviivat linjaa organisaation johto, organisaation koulutuksesta vastaava osasto liittää tietoturvakoulutuksen osaksi henkilöstön koulutussuunnitelmia ja koulutuksen tuloksia sekä kattavuutta seurataan säännöllisesti.

Valtiovarainministeriön (2022b) julkisen hallinnon tietoturvallisuuden arviointikriteeristön mukaan perehdytyksellä, koulutuksella ja viestinnällä tulee varmistaa henkilöstön tuntemus voimassa olevista määräyksistä ja ohjeista. Vaatimuksessa mainitaan erityisesti korkean riskin käsittelytilanteet. Koulutuksen toteuttaminen tulee toteuttaa työtehtävien tarpeen mukaan ja koulutuksiin osallistuneista tulisi pitää kirjaa.

3.3.3 Tietoturvapalvelut

Organisaatioiden on usein valittava ulkoisia tietoturvapalveluita ylläpitämään ja kehittämään organisaation tietoturvakokonaisuutta. Tietoturvapalveluiden valinnassa on tärkeää, että valittava palvelu täyttää tietoturvan kannalta määritetyt vaatimukset. Tietoturvapalveluiden käyttöönottoa varten tulee organisaation arvioida suojattavan tietojärjestelmän arvo ja kriittisyys, sekä riskitasoon sopivat riskien hallinta menetelmät. (National Institure of Standards and Technology, 2003a)

NIST 800-35- julkaisussa (2003) tietoturvapalvelut jaetaan kolmeen eri tasoon: johtamispalvelut, operatiiviset palvelut ja tekniset palvelut. Johtamispalveluilla tarkoitetaan organisaation johdon käsittelemiä aiheita, joihin johto tarvitsee ulkopuolista palvelua, kuten tietoturvaohjelman laadinta ja riskien hallinnan suunnittelu. Operatiivisilla palveluilla tarkoitetaan palveluita tietoturvakontrollien implementointiin ja toteuttamiseen, jotka vaativat teknistä tai muuten erikoistunutta asiantuntemusta. Tekniset palvelut ovat kontrolleja, joita rakennetaan tietojärjestelmän sisälle.

Valtiovarainministeriön (2007) Vahti- ohjeen 3/2007 mukaan ulkoistamisen osalta on tärkeää määrittää velvoitteet ja tehtävät palveluntarjoajalle. Ulkoistamisesta huolimatta kokonaisvastuu säilyy palvelun tilaajalla ja tämän takia on tärkeää toteuttaa seurantaa ja tarkistettava tietoturvatarpeet, jotta palvelun haluttu tietoturvallisuuden taso saavutetaan ja se säilyy koko ulkoistamisen ajan.

Tietoturvapalvelut voivat olla myös tietoturvan auditointiin liittyviä ulkopuolisia palveluita. Auditoinneilla pyritään tunnistamaan tietoturvan hallinnassa tai teknisessä toteutuksessa olevia puutteita, joiden perusteella toimintaa voidaan kehittää. ISO/IEC 27002- standardin (2022) mukaan organisaatioon liittyvänä yhtenä hallintakeinona on riippumaton katselmointi, jossa tietoturvallisuuden hallintaa arvioidaan sopivuuden, riittävyyden ja vaikuttavuuden osalta ulkopuolisen toimesta.

3.3.4 Tekniset tietoturvatoimenpiteet

Tekninen turvallisuus kattaa tietojärjestelmien ja tietoliikenneyhteyksien turvallisuuden. Nämä toimenpiteet suoritetaan ICT- ja tietoturva-ammattilaisten toteuttamana. Valtiovarainministeriön (2012) Vahti- ohjeessa 3/2012 erittelee teknologia ratkaisuja tietoturvan osalta:

- Käyttöoikeuksien hallinta
- Käyttäjän tunnistaminen
- Tiedon salaaminen
- Tietojen varmistaminen
- Koventaminen
- Haittaohjelmatorjunta
- Tietoturvapäivitykset
- Lokien hallinta
- Palomuuri
- IDS/IPS- järjestelmät
- Yhdyskäytäväratkaisut

NIST SP 800-53- julkaisussa (2020) teknisiin tietoturvatoimenpiteisiin kuuluu pääsynhallinta, konfiguraation hallintaan, identifiointiin ja todennukseen, ylläpitoon, järjestelmien ja yhteyksien turvaamiseen, järjestelmien ja informaation eheyteen sekä ohjelman hallintaan. Raggad:n (2010) jaottelun perusteella tekniseen turvallisuuteen kuuluu salakirjoitus (kryptologia/ kryptografia), pääsynhallinta ja verkkoliikenteen hallinta.

Valtiovarainministeriön (2007) Vahti- ohjeessa 3/2007 eritellään teknisinä turvallisuustoimina tietoliikennepalveluiden turvallisuus, johon liittyy esimerkiksi verkon valvonta ja hallinta sekä viestinnän salaaminen. Laitteistoturvallisuus käsittää laitteistoin koko elinkaaren hallintaa, joka sisältää suojauksen, varmuuskopioinnin, valvonnan ja päivitykset. Käyttöturvallisuuden osalta määritellään käyttöoikeuksien hallintaa, lokien valvontaa, haittaohjelmasuojausta sekä etäkäyttöön liittyviä toimenpiteitä.

3.3.5 Toimitilaturvallisuus

Toimitilaturvallisuuden perustana toimii turvallisuusvyöhykkeet, jotka organisaatio määrittää. Määrittelyyn vaikuttaa riskien arviointi, tiedon suojaustaso ja tiedon käsittelytapa. (Valtiovarainministeriö, 2013) Toimitilaturvallisuuteen liittyy toimia, joilla estetään tai rajoitetaan toimitiloihin ja säilytysratkaisuihin pääsyä. (Valtiovarainministeriö, 2022b)

Tietoturva standardit ja ohjeet, kuten NIST SP 800-53 (2020) sekä ISO 27002 (2022) julkaisuissa on useita hallintatoimia toimitilaturvallisuuteen liittyen. Ne liittyvät turva-alueisiin, kulunvalvontaan, laitteistojen ja tilojen suojaamiseen (ympäristölliset uhkat, kuten tulipalo tai tulva sekä ulkopuolisilta henkilöiltä), sekä toimitilojen ulkopuolelle vietävän materiaalin turvallisuus (etätyö tai asiapaperit).

Valtiovarainministeriön (2007) Vahti- ohjeessa 3/2007 on fyysisen turvallisuuden osa-alueeseen esimerkkinä listattu:

- Kulunvalvonta
- Kameravalvonta
- Muu tekninen valvonta
- Vartiointi
- Palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta

3.4 Toimenpiteiden arviointi

Tietoturvallisuuden tilan arviointi ja mittaaminen on keskeistä tietoturvatyössä ja se on osa organisaation riskienhallintaa. Arvioinnin tulee olla jatkuvaa ja sen tuloksia käytetään tietoturvallisuuden kehittämiseen. Arviointia voidaan toteuttaa sisäisesti jonkin tietoturvastandardin tai ohjeen vaatimuksien perusteella, kuten Julkri, Katakri tai ISO27001. Ulkoinen arviointi voidaan suorittaa esimerkiksi yksiköiden välillä arviointiryhmiä apuna käyttäen. Arviointia voidaan suorittaa myös vertailemalla oman organisaation tietoturvatoimintaa muihin organisaatioihin, joilla tietoturvatoiminta on kehittyneemmällä tasolla ja sieltä on otettavissa parhaita käytäntöjä osaksi omaa toimintaa. (Valtiovarainministeriö, 2006)

Tietoturvallisuuden mittaaminen voidaan toteuttaa laadullisesti ja määrällisesti. Laadullisessa mittauksessa voidaan arvioida toiminnan tuloksia. Määrällisessä mittaamisessa voidaan seurata esimerkiksi tietoturvapoikkeamien tai tietoturvakoulutuksen määrää. (Valtiovarainministeriö, 2006)

Valtiovarainministeriön (2014) Vahti- ohjeessa 2/2014 tietoturvallisuuden arviointi jaetaan hallinnollisen tietoturvallisuuden arviointiin sekä tietojärjestelmien ja tietoliikennejärjestelyiden arviointiin. Hallinnollisen tietoturvallisuuden arvioinnissa tietoturvallisuuden hallintajärjestelmän kattavuutta ja toimivuutta, joka kohdistuu prosesseihin ja menettelyihin. Arviointitapoina hallinnollisen tietoturvallisuuden arvioinnissa on haastattelut, katselmoinnit sekä dokumentaation ja ohjeiden tarkastelu. Tietojärjestelmiin ja tietoliikennejärjestelyihin kohdistuvat arvioinnit toteutetaan teknisenä testauksena, joilla pyritään varmistamaan, että järjestelmä täyttää sille asetetut vaatimukset. Digi- ja väestötietoviraston (2021) mukaan tietoturvallisuuden seurannassa hyödynnetään toimenpiteiden toteutumisesta kertyvää tietoa. Nämä voivat olla esimerkiksi teknisiä testauksia, sisäisiä auditointeja tai tietoturvapolitiikan ajantasaisuuden varmistamista.

NIST SP 800-100 (2006) ohjeessa määritellään jatkuvasta seurannasta, jossa tietoturvallisuuden tilannetta tarkastellaan jatkuvasti. Ohjeen mukaan tehokas valvonta edellyttää tietojärjestelmän konfiguraation hallintaa ja ohjausta, tietojärjestelmän muutosten vaikutusanalyysiä sekä tietoturvatoimenpiteiden arviointia ja turvallisuustilan raportointia. Tietoturvallisuuden tilan tarkastuksia tulisi toteuttaa vuotuisina testaus- ja arviointitoimina. Myös tietoturvallisuusohjelmaan tulee toteuttaa tarkastuksia, jotta tietoturvan hallintaa voidaan kehittää.

Raggad (2010) määrittelee tietoturvallisuuden tilan tarkastukset mahdollisuudeksi yksilöidä, arvioida ja lieventää riskejä, joka on tärkeää riskilähtöiselle tietoturvallisuuden hallinnalle. Hän jakaa tarkastustoiminnan haavoittuvuuksien arviointiin, tunkeutumistestaukseen, järjestelmätilantestaus, tietoturvapolitiikan arviointi, fyysisen turvallisuuden testaus ja tapahtumahallinnan testaukseen.

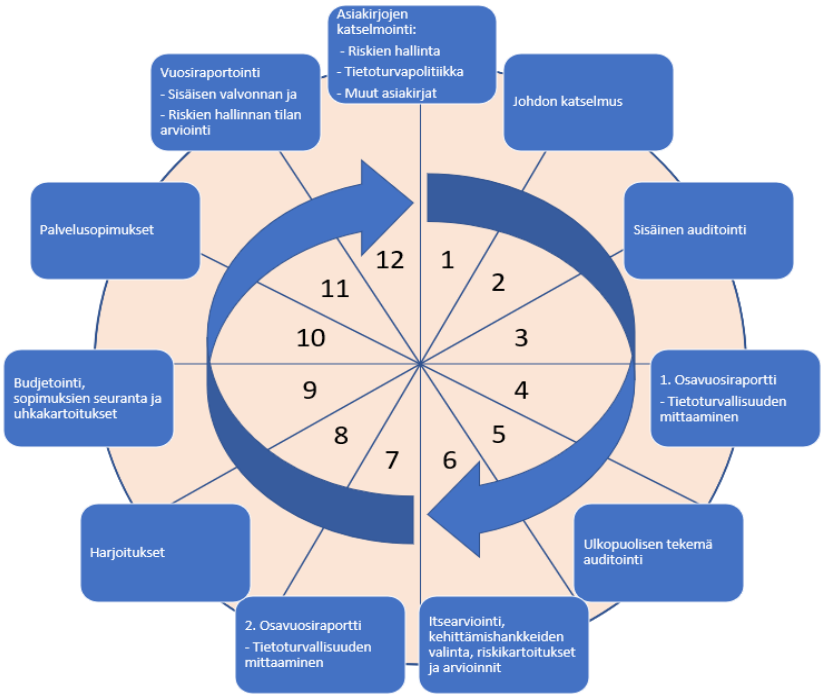
ISO 27001- standardin (2022) mukaan tietoturvan suorituskyvyn arviointiin liittyy seuranta, mittaus, analysointi sekä arviointi. Tätä varten organisaation on luotava suunnitelma, miten suorituskykyä arvioidaan. Suunnitelmassa on käytävä ilmi mitä seurataan ja mitataan, millä menetelmillä se toteutetaan, milloin arviointi toteutetaan ja tulokset analysoidaan sekä ketkä toteuttaa arvioinnin ja analysoi tulokset. Suorituskyvyn arviointia voidaan toteuttaa sisäisinä auditointeina ja johdon katselmuksina. Arviointi vaiheen jälkeen tietoturvallisuuden hallinnassa käytettävään prosessiin toteutetaan tarvittavat parannus- ja kehittämistoimet.

3.5 Kehittäminen

Organisaation on parannettava jatkuvasti tietoturvallisuuden hallintaa. Parantamisen kohteena on tietoturvallisuuden hallintajärjestelmä ja sen eri vaiheet. Kehittäminen voi tapahtua toiminnan arviointien perusteella tai tietoturvapoikkeaman perusteella. (Suomen standardisoimisliitto, 2022a)

Valtiovarainministeriön (2007) Vahti- ohjeen 3/2007 mukaan organisaation tulee laatia kehittämissuunnitelma, joka ohjaa toimenpiteitä, joilla tietoturvallisuuden arvioinnissa havaitut puutteet korjataan ja kehitetään tietoturvan tavoitetasolle. Digi- ja väestötietoviraston (2021) mukaan jatkuvan parantamisen tavoitteena on ylläpitää tietoturvallisuuden hallintaa toimintaympäristön muuttuessa. Kehittämisen toteuttaminen voidaan sitoa tietoturvallisuuden vuosikelloon (kuvio 2), mutta mikäli toimintaympäristö muuttuu nopeammin, tulee kehittämisvaiheen toimenpiteet toteuttaa sen mukaisesti.

Raggadin (2010) ”Information security life cycle” vaihe kuusi (viimeinen vaihe) sisältää toimenpiteet jatkuvan turvallisuuden ylläpitämiseksi. Se koostuu seurannasta, jolla varmistetaan, että riskientasot pysyvät hyväksytyllä alueella. Tämän vaiheen tärkeimmät toimenpiteet ovat säännöllinen riskienarviointi, säännöllinen tietoturvapolitiikan ja toimenpiteiden tarkastus, tietoturvakoulutus, määräajoin toteutettava testaus ja arviointi, puutteiden korjaaminen sekä toimenpiteet tietoturvapoikkeamien tapahtuessa.



Kuvio 2: Esimerkki tietoturvallisuuden vuosikellosta
(Mukailtu Valtiovarainministeriö, 2007)

4 TUTKIMUSMENETELMÄT

Tämä tutkimus toteutetaan kvalitatiivisena tapaustutkimuksena, jossa toteutetaan kirjallisuuskatsaus sekä asiantuntijoiden haastatteluja. Aineisto analysoidaan sisällönanalyysin avulla. Kirjallisuuskatsaukseen tietoa kerätään tietoturvallisuuden hallintaan liittyvistä kansallisista ja kansainvälisistä laeista ja ohjeista sekä tietoturvallisuuden hallintaan liittyvästä kirjallisuudesta. Haastattelut toteutetaan teemahaastatteluna, joissa haastatellaan pienten ja keskisuurien kuntien tietoturvallisuuden hallinnan parissa työskenteleviä henkilöitä.

Laadullisessa tutkimuksessa keskitytään kohteen laatuun, ominaisuuksiin ja merkitykseen, kun taas määrällisessä tutkimuksessa kohteen kuvaus ja tulkinta perustuu tilastoihin ja numeroihin. Tässä tutkimuksessa pyritään käsittelemään tietoturvallisuuden hallintaa yksityiskohtaisesti, joten kvantitatiivisen tutkimuksen menetelmät eivät sovellu aiheen käsittelyyn tutkimuksen näkökulman takia.

4.1 Tapaustutkimus

Tapaustutkimus on menetelmä, jolla pyritään kuvaamaan, ymmärtämään, ennustamaan ja kontrolloimaan tutkittavaa tapausta. Syvän ymmärryksen hankkiminen tutkittavasta tapauksesta vaatii tutkijalta tapauksen tarkkailua kohdeympäristössä, tulkintojen hankkimista osallistujilta sekä kirjallisten dokumenttien ja tapausympäristössä esiintyvän toiminnan analyysiä. (Woodside, 2017)

Tapaustutkimus on empiirinen tutkimus, jossa eri tavoilla monipuolista tietoa hankkimalla tutkitaan tapahtumaa tai toimintaa rajatussa ympäristössä (Anttila, 1998). Tapaustutkimukselle tyypillisiä piirteitä ovat:

- Tapaustutkimukset ovat syvätutkimuksia
- Suppea kohde ja suuri määrä muuttujia
- Intensiivisenä menetelmänä havaitaan oleelliset tekijät, prosessit ja vuorovaikutussuhteet

- Saavutetaan yksityiskohtaista tietoa
- Yleistettävyyden tasoa ei saavuteta
  (Anttila, 1998)

Tapaustutkimuksen vaiheita ovat:

- Tavoitteiden määrittely
- Tutkimussuunnitelman laatiminen
- Aineiston kokoaminen
- Aineiston järjestäminen
- Tutkimustulosten raportointi ja merkitsevyyden tarkastelu.
  (Anttila, 1998)

4.2 Aineistonkeruumenetelmät

Tutkimuksessa käytettävän aineiston keruumenetelmät ovat kirjallisuuskatsaus sekä asiantuntijahaastattelut. Kirjallisuuskatsauksella tuotetaan teoreettinen pohja tutkittavalle aiheelle, yhdistämällä tietoa erilaisista kansallisista ja kansainvälisistä laeista, ohjeista ja muusta tietoturvallisuuden hallintaan liittyvästä kirjallisuudesta. Asiantuntijahaastatteluilla selvitetään asiantuntijoiden näkemyksiä tietoturvallisuuden hallinnan tasosta, odotuksista ja niihin vaikuttavista tekijöistä pienissä ja keskisuurissa kunnissa.

Kirjallisuuskatsauksen tarkoituksena on tarkastella aiempaa tutkimusta tutkittavasta aiheesta sekä näyttää miten ja mistä näkökulmista aiempaa tutkimusta on aiheeseen liittyen toteutettu (Tuomi & Sarajärvi, 2002). Kirjallisuuskatsauksen aineistoa kerättiin tutkimukseen kansallisesta lainsäädännöstä ja ohjeista sekä kansainvälisistä ohjeista ja standardeista. Nämä julkaisut valikoituivat, koska ne edustavat kansallisesti ja kansainvälisesti laajasti käytettyjä ohjeita. Kansallisista lähteistä käytettiin pääasiassa tiedonhallintalakia (906/2019) sekä VAHTI- verkoston julkaisemia ohjeita. Kansainvälisistä tunnetuista tietoturvallisuutta käsittelevistä ohjeista ja standardeista kirjallisuuskatsauksessa käytettiin International Organization for Standardization (ISO)- standardisarjan teoksia 27001, 27002 ja 31000 sekä National Institute of Standards and Technology (NIST)- erikoisjulkaisuja. ISO27001 ja ISO27002 käsittelevät tietoturvallisuuden hallintajärjestelmää ja hallintakeinoja, ISO31000 käsittelee riskienhallintaa. NIST:n erikoisjulkaisut käsittelevät riskienhallintaa, tietoturvallisuuden hallintaa, hallintakeinoja sekä koulutusta. Näiden lisäksi tutkimuksessa käytettiin Raggadin (2010) ”Information security management”- teosta, joka kokoaa tietoa tietoturvallisuudesta ja sen hallinnasta. Tämä kirjallinen lähdeaineisto luo vankan pohjan tutkimuksen teoreettiselle osuudelle.

Asiantuntijahaastattelut toteutettiin teemahaastatteluina. Teemahaastattelu valikoitui toiseksi tutkimuksen aineistonkeruumenetelmäksi, koska tutkimuksessa pyritään selvittämään erilaisia tietoturvallisuuden hallintaan liittyviä kokonaisuuksia, jotka vaihtelevat kunnittain. Teemahaastattelun pohjana toimii

valitut teemat tutkimuksen viitekehyksen mukaisesti ja niitä voidaan täydentää tarkentavilla kysymyksillä. Teemahaastattelussa korostuu ihmisten tulkinnat ja asioille annettava merkitys (Tuomi & Sarajärvi, 2002).

Asiantuntijahaastatteluiden pohjaksi tutkija esitteli tietoturvallisuuden hallintaprosessin vaiheet ja toimenpiteet kirjallisuuskatsauksen pohjalta, sekä tiedonhallintalain vaatimukset tietoturvallisuuden osalta. Asiantuntijahaastatteluiden teemat olivat:

- Tietoturvallisuuden hallinta kunnassa
    - Prosessi – Vaiheet
    - Riskienhallinta
    - Tietoturvatoimenpiteet
    - Jatkuvuuden hallinta
- Tiedonhallintalain vaatimustenmukaisuus kunnassa
    - Tiedonhallintalain 4. luvun vaatimukset
- Tietoturvallisuuden tilan arviointi kunnassa
- Tietoturvallisuuden hallintaan vaikuttavat tekijät
    - Resurssit
    - Osaaminen
    - Jääkö jotain tekemättä?
- Tietoturvallisuuden hallinta tulevaisuudessa
    - Odotukset ja ohjaus
    - Painopisteet

Kuntien koot määräytyvät tässä tutkimuksessa niiden asukasluvun mukaan. Kuntia Suomessa on Tilastokeskuksen (2022) mukaan 309, näistä kunnista 108 käyttää kaupunki nimitystä ja 201 kunta nimitystä. Tilastokeskuksen (Noudettu 3.2.2023) tilastollisen kuntaryhmityksen mukaan kaupunkimaisiin kuntiin lasketaan kunnat, joissa on vähintään 15000 asukasta. Taajaan asutuiksi kunniksi lasketaan kunnat, joissa on alle 15000 asukasta. Kuntaliiton verkkosivuilla (Noudettu 3.2.2023) ”Suurten ja keskisuurten kaupunkien sosiaali- ja terveystoimen kustannukset” selvitys määrittelee Kauniaisen, Kirkkonummen, Lohjan, Porvoon, Salon ja Sipoon keskisuuriksi kunniksi. Näiden kuntien asukasluvut ovat Tilastokeskuksen (2022) tilaston mukaan Kauniaisten 10396 asukkaan ja Salon 51400 asukkaan välillä. Tässä tutkimuksessa pienillä kunnilla tarkoitetaan alle 15000 asukkaan kuntia ja keskisuurilla alle 50000 asukkaan kuntia, koska virallista määritelmää pienille ja keskisuurille kunnille ei ole tehty. Asiantuntijahaastattelut toteutettiin kolmeen kuntaan, joista yksi oli keskisuuri ja kaksi pieniä kuntia. Haastateltavina oli jokaisesta kunnasta yksi henkilö. Henkilöiden työnkuvat, joita haastateltiin, olivat tietohallintosuunnittelija (lisäksi tietosuojavastaava), tietohallintopäällikkö ja kansliapäällikkö.

4.3 Aineiston analyysi

Tutkimuksessa kerätty aineisto analysoidaan aineistolähtöisen sisällönanalyysin avulla. Tuomen ja Sarajärven teoksessa (2002) viitataan Milesin ja Hubermanin vuoden 1984 teokseen, jossa he jakavat aineistolähtöisen sisällönanalyysin kolmeen vaiheeseen. Nämä vaiheet ovat aineiston pelkistäminen, ryhmittely ja teoreettisten käsitteiden luominen. Sisällönanalyysissä on tarkoituksena yhdistää käsitteitä ja saada näiden avulla vastaukset tutkimustehtävään. (Tuomi & Sarajärvi, 2002)

Sisällönanalyysissä tutkittavasta ilmiöstä hankitusta materiaalista (tekstistä) pyritään saamaan kuvaus tiiviissä ja yleisessä muodossa. Pelkistämisvaiheessa aineistonkeruu vaiheessa hankitusta tekstistä karsitaan pois tutkimuksen kannalta epäolennainen tieto. Pelkistämisen voi toteuttaa joko tiivistämällä tai pilkkomalla tietoa osiin. Ryhmittelyvaiheessa pelkistämisvaiheen aineisto ryhmitellään tai yhdistetään luokkiin samankaltaisuuksien perusteella. Luokitteluyksikkönä voi tutkimuksen mukaan toimia esimerkiksi jokin ominaisuus tai piirre. Teoreettisten käsitteiden luomisvaiheessa tutkimukselle valikoidusta tiedosta muodostetaan teoreettisia käsitteitä. Siinä aineistossa esiintyvistä kielellisistä ilmauksista muodostetaan teoreettisia käsitteitä ja johtopäätöksiä. (Tuomi & Sarajärvi, 2002)

5 TULOKSET

Tässä luvussa käsitellään teemahaastatteluiden tuloksia. Otsikko rakenne on määritelty teemahaastattelu aiheiden sekä haastattelumateriaalin teemoittelun perusteella.

5.1 Tietoturvallisuutta ohjaavat tekijät

Tietoturvallisuuden toteuttamista ohjaa organisaation ICT- ympäristö, tietoturvallisuuden johtaminen sekä lakien vaatimukset. ICT- ympäristöön vaikuttaa ICT- palvelutuotannon toteutus ja siihen liittyvät kumppanuudet, jotka voivat olla joko yhteistoimintaa toisten kuntien kanssa tai ostettuna palveluna palveluntarjoajalta. Tietoturvallisuuden hallinta ja sen vaatimukset tulisi määritellä organisaation johdon toimesta, jolla asetetaan suuntaviivat tietoturvallisuuden toteuttamiselle.

5.1.1 ICT- ympäristö

ICT- palvelut ostetaan organisaatioissa yhä useammin palveluna, jolloin organisaation omaa palvelutuotantoa vähennetään. ICT- palvelutuotannolla tarkoitetaan muun muassa laite-, tuki-, asiantuntija-, tietoliikenne- ja sovelluspalveluita. ICT- palvelutuotanto voidaan toteuttaa organisaation mukaan omana, kokonaan ulkoistettuna tai näiden yhdistelmänä eli hybridi mallina.

Haastatteluihin osallistuneista kunnista kaksi kolmesta toteuttaa ICT- palvelutuotantoa pääasiassa ulkoistettuna palveluna. Näistä toisessa kunnassa tietohallinnon henkilöstöä toimii käyttö- ja lähitukitehtävissä sekä muutamia hajautettuna hallinnon tehtävissä, toisessa pienemmässä kunnassa tietohallinnon työntekijöitä on päätoimisena vain yksi. Kolmannessa kunnassa, jossa palvelut pääosin tuotetaan omana palvelutuotantona, tietohallinnon työntekijöiden määrä on pystytty pitämään maltillisena toisen kunnan kanssa toteutettavan yhteistoiminnan takia.

ICT- ohjelmistojen käyttötapoja on useita. Ääripäinä voidaan pitää vain pilvipalveluihin pohjautuvia ratkaisuja sekä omaa paikallista konesalipalvelua, josta ohjelmistojen käyttöä toteutetaan. Haastatellut kunnat, joilla ICT- palvelutuotanto on pääasiassa ulkoistettu, ei omaa konesalipalvelua ole, vaan sovelluspalvelut tuotetaan palveluntarjoajan konesalista ja SaaS- palveluna. Kolmannella kunnalla on käytössä sekä omia palvelimia, että SaaS- palveluita.

5.1.2 Johtaminen

Tietoturvallisuuden johtaminen haastateltujen kuntien osalta toteutuu kunnan ylimmän johdon toimesta pääosin tietoturvapolitiikan muodossa. Kunnan johto hyväksyy tietoturvapolitiikan, mutta tietoturvapolitiikan valmistelusta vastaa yleensä tietohallinto. Haastatteluissa kävi ilmi, että tietoturvapolitiikkaa valmistelevien työntekijöiden kädenjälki näkyy vahvana tietoturvapolitiikassa.

Johtamisessa tärkeää on tavoitteiden asettelu, joka ohjaa tietoturvallisuuden hallintaa. Yksi haastateltavista kertoi, että kunnan johdolla on joitain tavoitteita, mutta varsinaista kiinnostusta tietoturvallisuuteen ei ole, joka taas näkyy siinä, ettei vaatimuksia luoda tietoturvasta alemmille tasoille. Toisessa kunnassa nähtiin, että heidän kunnassaan tietoturvallisuuden toteuttamisen periaatteet on tuotu esille. Lisäksi heillä on aloitettu kunnan luottamushenkilöiden koulutus osana toista projektina, jonka tavoitteena on luottamushenkilöiden tietoturvatietoisuuden lisäys ja tätä kautta johdolle kyky tuottaa selkeämpiä näkemyksiä tietoturvatoiminnasta.

5.2 Tietoturvallisuuden hallinta

Tietoturvallisuuden hallintaa käsiteltiin haastatteluissa prosessina, joka on esitelty tutkimuksen kolmannessa luvussa.

Kaksi kolmesta haastateltavasta kertoivat heidän kunnassaan olevan käytössä Digiturvamalli, joka on Microsoft Teams- alustalla toimiva sovellus. Digiturvamalli purkaa organisaation haluamat vaatimuskehikot (esim. ISO27001 tai tiedonhallintalaki) erillisiksi tehtäviksi, jonka tarkoituksena on helpottaa tietoturvatyön jakamista, toteuttamista ja seurantaa. Digiturvamallin käyttö on näissä kunnissa koettu hyväksi. Toisessa kunnassa mallin käytössä on edetty pidemmälle, toisessa kunnassa sen käyttö on vasta alussa ja ensisijaisesti siellä keskitytään tiedonhallintalain ja tietosuojalain vaatimuksien täyttämiseen. Kunnassa, jossa digiturvamalli ei ole käytössä, ei ole käytössään dokumentoitua tietoturvallisuuden hallintajärjestelmää tai -prosessia. Tässä kunnassa tietoturvallisuuden hallinta toteutuu lähinnä yksittäisinä toimenpiteinä, joiden dokumentointi on vähäistä.

5.2.1 Riskienhallinta

Riskilähtöisyyttä voidaan pitää tietoturvallisuuden hallinnassa keskeisen tekijänä. Haastateltavissa kunnissa oli toteutettu riskien arviointia vaihtelevasti, mutta varsinaista riskienhallinta prosessia ei ollut toteutettu. Kaikissa haastatelluissa kunnissa riskit on huomioitu, mutta kahdessa kolmesta ei riskienhallintaprosessia ollut dokumentoitu. Yhdessä kunnassa tietoturvariskit oli arvioitu digiturvamallin avulla ja riskienhallinta kokonaisuuteen haettiin hyviä käytänteitä erillisen hankkeen muodossa.

Riskienhallintaa oli suorittanut yksi kunta ja toinen kunta aikoi aloittaa riskilähtöisen toiminnan, kun digiturvamallin käytössä päästään siihen vaiheeseen. Kahdessa kunnassa, joissa riskienhallinta prosessia ei ollut dokumentoitu, riskit arvioitiin esimerkiksi uusia järjestelmiä käyttöönottaessa, mutta laaja-alaisempaa riskienhallintaprosessia tai sen osia ei toteutettu.

Tämän perusteella voidaan päätellä, että haastateltavista kunnista kahdella kolmesta riskienhallinta toteutettiin vain satunnaisiin kokonaisuuksiin liittyen, mutta jatkuvana ja päivittyvänä dokumenttina ja toimintatapana sitä ei toteutettu. Kolmannessa kunnassa tietoturvariskien hallinta oli toteutettu usealla tasolla, jossa riskienhallinta käytännön tasolla toteutettiin digiturvamallin avulla ja ylätason riskit huomioitiin kunnan strategiassa.

5.2.2 Tietoturvatoimenpiteet

Tietoturvatoimenpiteet pitävät sisällään koulutuksen, viestinnän, tekniset toimenpiteet ja tietoturvapalveluiden käytön. Nämä ovat käytännön toimenpiteitä, joilla korjataan, ylläpidetään ja parannetaan tietoturvallisuuden tilaa organisaatiossa. Kunnassa, jossa ei palvelutuotantoa ollut ulkoistettu, tietoturvatoimenpiteet esimerkiksi koulutuksiin liittyen tuli henkilöstöltä ja teknisiä toimenpiteitä toteutettiin havaintojen sekä kansallisten ohjeiden tai tiedotteiden perusteella. Kahdessa muussa kunnassa, joissa palvelutuotantoa oli ulkoistettu, varsinkin tekniset toimenpide esitykset ja toteutus tulivat palveluntarjoajalta.

Haastatelluissa kunnissa tietoturvatoimenpiteet olivat keskittyneet pääasiassa koulutuksiin, joita toteutettiin näissä kunnissa verkkokoulutuksina koko henkilöstölle sekä satunnaisina lähikoulutuksina. Verkkokoulutuksia toteutettiin vuosittain, mutta muita koulutuksia ei ollut järjestetty määräajoin. Yhden kunnan osalta oli käytössä niin sanottu ”huoneentaulu”, jossa esitellään lyhyesti tärkeimmät tietoturvalliset toimintatavat. Tämän lisäksi kunnassa oli haastateltavan mukaan tarjolla riittävästi koulutusta, mutta osallistumismäärät koulutuksiin eivät olleet odotetulla tasolla. Koulutuksen osalta kahdessa kunnassa tietoturvakoulutusta on toteutettu erityisesti johto- ja esimiestasolle.

Tietoturvaan liittyvä viestintä koettiin tärkeänä ja pääasiallisena viestintäkanavana toimi kuntien omat Intra-sivut. Yksi kunnista toteutti tiedottamista aktiivisesti välittömillä tiedotteilla, jos jotain poikkeavaa havaittiin. Toisessa kunnassa ei viestintä ollut niin aktiivista, mutta neljännesvuosittain tietoturvasta viestittiin koko kunnan henkilöstölle. Kolmannessa kunnassa viestittiin pääasiassa vain uusista tietoturvaohjeistuksista.

Teknisiä toimenpide- ja korjausehdotuksia haastatellut kunnat saivat kumppaneiltaan. Varsinkin kunnat, joilla palvelutuotantoa oli ulkoistettu, toteutettiin aktiivista yhteistoimintaa. Näissä kunnissa myös teknisiä toimenpiteitä suorittivat palveluntarjoajat. Yksi haastateltavista mainitsi, että luottamus palveluntarjoajaan on iso, mutta varsinainen valvonta palveluntarjoajan toimintaan oli vähäistä.

Haastatelluilla kunnilla oli kaikilla käytössä palveluntarjoajia ICT- ympäristön suojaamiseen, valvontaan ja/tai seurantaan. Valvontatoiminnalla yleisesti tarkoitetaan verkkoliikenteen seurantaa ja sen avulla voidaan havaita esimerkiksi epäilyttävä toiminta organisaation järjestelmissä.

Kunnat seurasivat tietoturvaan liittyvää uutisointia ja tiedotteita kyberturvallisuuskeskuksen julkaisuista, joihin kunnissa pyrittiin tarpeen mukaan reagoimaan.

5.2.3 Arviointi ja kehittäminen

Arvioinnin ja kehittämisen avulla pyritään selvittämään tietoturvallisuuden parantamiseksi toteutettujen toimenpiteiden toimivuus ja luoda kehittämissuunnitelma tietoturvallisuuden parantamiseksi.

Tietoturvallisuuden hallinnassa tärkeänä osana on arvioida toteutettujen tietoturvatoimenpiteiden vaikuttavuutta. Kukaan haastateltavista ei kuitenkaan tuonut esille, että heillä olisi tietoturvallisuuden tilan arviointiin liittyviä toimintatapoja. Yksi haastateltava mainitsi, että Digi- ja väestötietoviraston kyselyt toimivat hyvin oman toiminnan arviointina ja ne antoivat jonkin tason tilannekuvan omasta tietoturvatoiminnasta. Kaksi kolmesta kunnasta toi esille, että heidän palveluntarjoajansa toimenpitein tietoturvallisuuden tilaa seurattiin ja arvioitiin.

Varsinaisia kehittämisen tueksi rakennettuja käytäntöjä ei kunnissa ollut toteutettu. Yhdessä kunnassa kenttätason kehittäminen tapahtui eri yksiköissä työskentelevien tietohallinnon henkilöiden toimesta, jotka myös puuttuivat joiltain osin tietoturvallisuutta vaarantaviin tapahtumiin. Kunnissa, joilla palvelut oli pääosin ulkoistettu, raportointi tietoturvallisuuden tilasta oli pääasiassa palveluntarjoajien toteuttamaa. Yksi haastateltavista kertoi, että strategisia palavereita, joissa kunnan johto oli myös mukana, toteutettiin kaksi kertaa vuodessa palveluntarjoajan kanssa. Haastatteluiden perusteella kehittäminen tapahtui pääasiassa palveluntarjoajien toimesta, mutta kuntien omana toimintana kehittämistä ei ollut laajassa mittakaavassa toteutettu.

5.3 Tiedonhallintalain toteutus

Haastateltavat kertoivat, että heidän kunnissaan tiedonhallintalakiin liittyviä tietoturvavaatimuksia on toteutettu joiltain osin. Yhden kunnan osalta haastateltava kertoi, että tiedonhallintalain vaatimuksia tietoturvan osalta on joiltain osin tehty, osa puoliksi ja osaa ei tehtynä ollenkaan. Toisessa kunnassa arvioitiin, että osa vaatimuksista on täytetty paremmin ja osa huonommin, mutta

tiedonhallintalautakunnan vähimmäisvaatimukset olisivat jollain tasolla täytetty, joskaan siitä ei dokumentaatio ollut tuotettu. Kolmannessa kunnassa arvioitiin, että tiedonhallintalautakunnan vähimmäisvaatimukset olisi heidän osalta täytetty.

Yksi haastateltava kertoi, että digiturvamallia pyritään käyttämään tiedonhallintalain vaatimuksien täyttämiseksi, mutta työtä ei vielä täysi painoisesti ole aloitettu. Kaksi kolmesta kunnasta näkivät tiedonhallintalain täyttämisen ongelmalliseksi siihen käytettävissä olevien resurssien takia. Lisäksi tiedonhallintalain vaatimuksien toteuttamista ei kaikilta osin oltu vastuutettu.

Yksittäisinä lain vaatimuksien kohtina nostettiin käyttövaltuushallinta kahden kunnan osalta, joissa tähän oli panostettu erityisesti. Lisäksi kaikissa kunnissa toteutettiin joiltain osin tietoturvallisuuden toimintaympäristön seurantaa Kyberturvallisuuskeskuksen tiedotteiden seuraamisen muodossa.

Kokonaisuudessaan voidaan arvioida, että haastateltavat kunnat ovat lähestyneet tiedonhallintalain vaatimuksia eri näkökulmista. Voidaan todeta, että joitain toimenpiteitä on jokaisen kunnan osalta tiedonhallintalain tietoturvavaatimuksien osalta toteutettu, mutta kattavaa dokumentaatiota ja seurantaa ei ole kaikkien osalta toteutettu.

5.4 Tietoturvallisuuden tila ja vaikuttavat tekijät

Tietoturvallisuuden tilaa haastateltavat arvioivat kohtalaiseksi. Yksi haastateltava kertoi, että tietoturvallisuus on huomioitu kunnassa, mutta johtamisessa ja joiltain osin myös suhtautumisessa olisi parantamisen varaa. Toinen haastateltava kertoi, että he ovat kunnassaan onnistuneet tunnistamaan heille tietoturvan kannalta tärkeimmät asiat, niihin on panostettu ja siten tietoturvallisuus on parantunut.

5.4.1 Resurssit

Tietoturvallisuuden hallintaan vaikuttaa käytössä olevat resurssit. Resursseina voidaan pitää tietoturvaan kohdistettua budjettia, henkilöstöä ja osaamista.

Yksi haastateltava kertoi, että heillä tietohallinto henkilöstö on osaavaa ja henkilöstö määrä on saatu pidettyä kohtalaisen pienenä kuntien yhteistoiminnalla, jossa kunnat tukevat tietohallinnon osalta toisiaan ja heillä on näkyvyys toistensa palvelimiin ja verkkoihin. Kahdella muulla kunnalla palvelut ovat suurilta osin ulkoistettu, joka osaltaan pienentää henkilöstöresurssin tarvetta. Toisessa kunnassa, jossa palvelut on pääosin ulkoistettu, kerrottiin, että tietohallintohenkilöstöä on sijoitettu eri yksiköihin lähitukeen, jolloin kentällä reagointi ja tuki on nopeampaa, mutta vastuutettuja tietoturvan osalta ei ole ja aikaa tietoturvan toteuttamiseen ei ole tarpeeksi. Kolmas haastateltava kertoi, että henkilöstöresurssit eivät ole kokonaisuudessaan tietoturvan osalta riittävät ja heillä on vain yksi päätoiminen henkilö hoitamassa tietohallinnon tehtäviä.

Tietoturvaa hoitavan henkilöstön osaaminen nähtiin osittain haasteena. Kaksi haastateltavaa kertoi, että osaaminen ei ole tietoturvan osalta tarpeeksi hyvällä tasolla. Yksi haastateltava kertoi, että heiltä on neljä henkilöä Kyberturvaaja- koulutuksessa, jonka avulla tietoturvallisuuden osaamista pyritään kunnassa laajentamaan ja syventämään. Haastateltava kuitenkin esitti huolensa mahdollisesta poistumasta koulutuksen jälkeen saadun osaamisen takia.

Rahallisen resursoinnin osalta budjetointi kunnissa vaihteli. Yhden kunnan osalta nähtiin, että vastuun tietoturvasta ollessa johdolla, rahaa tietoturvaan oli saatavilla, mikäli perusteet rahantarpeelle oli olemassa. Toisessa kunnassa taas tietoturvaan ei suoraa budjetointia ollut, mutta tietohallinnolle kohdentamatonta budjettia käytettiin tietoturvaan ainakin osittain. Kolmannessa kunnassa kunnanjohto oli vaatinut priorisointia tietoturvaan käytettävän rahoituksen osalta, joka johti osaltaan esitetyn budjetin leikkaamiseen.

5.4.2 Ohjaus

Tietoturvallisuuden ohjauksen päätekijöinä voidaan käsittää lait, tietoturvallisuuden hallintaprosessi, kansallista tietoturvallisuutta ohjaavat toimijat sekä yhteistyötahot. Kaksi kolmesta kunnasta näki, että digiturvamalli luo suunnan tietoturvallisuuden hallinnalle ja he kokivat, että sen ohjaamana tunnistetaan tarpeelliset tietoturvaan liittyvät tehtävät. Kolmas kunta näki, että tiedonhallintalautakunta on tuonut tarpeellista konkretiaa tietoturvallisuudesta selvityspyynnöin ja ohjein.

Vaikka tiedonhallintalautakunnan ohjeet ja digiturvamalli koettiin hyvinä, jokaisen haastateltavan kunnan osalta toivottiin selkeämpää ohjeistusta ja konkreettisia malleja muun muassa tiedonhallintalain vaatimuksien toteuttamiseksi. Kaksi kolmesta kunnasta näki, että yhdenmukaistaminen ja yhdessä tekeminen pienentäisi kuntien tietoturvabudjetteja. Se, että tulisiko valmiit mallit miltä instanssilta, ei ollut selkeää näkemystä.

Yhdessä kunnassa nähtiin, että lainsäädännön vaatimukset voivat ajaa julkishallintoa isompiin yksiköihin, koska lain vaatimuksien toteuttaminen on pienille kunnille haastavaa. Toisessa kunnassa nähtiin, että palveluntarjoajalta odotettiin enemmän konkreettisia työkaluja kunnan tiedonhallintalain toteuttamiseen. Lisäksi yhden kunnan osalta nähtiin, että digi- ja väestötietoviraston hankkeet ja ohjeet ovat toimivia, mutta valtion tuottamia linjauksia esimerkiksi tiedonhallintalain vaatimuksiin kaivattiin, koska jokaisen kunnan toteuttaessa vaatimukset omilla tavoilla, kokonaishinta toteutuksen osalta nousee.

5.4.3 Kehityskohteet ja tulevaisuuden painopisteet

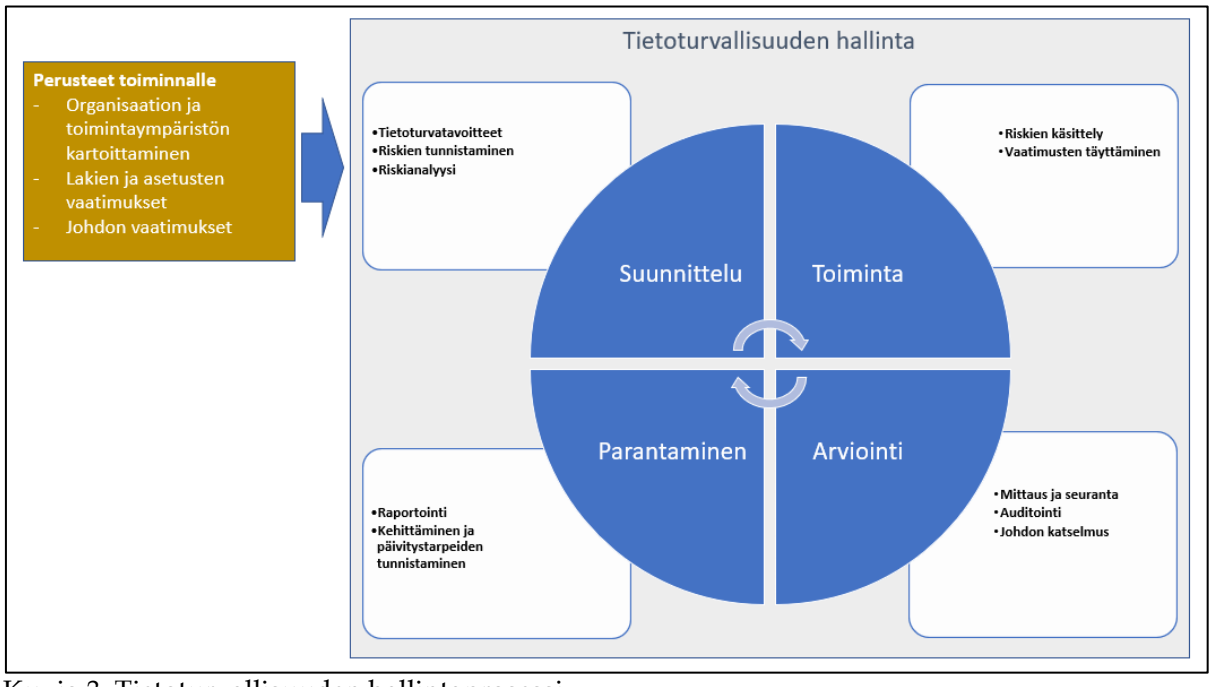
Haastateltavista kunnista kaksi kertoivat, että he aikovat panostaa jatkossa koulutukseen. Lisäksi digiturvamallin käytön jatkaminen ja kokonaisuuden hallinta oli tavoitteena yhdessä kunnassa. Lisäksi painopisteenä nähtiin tekniset ratkaisut ja jatkuvuuden ylläpito. Jokaisen kunnan osalta haastattelujen aikana kävi ilmi, että jatkuvaan ja kaikilta osin aktiiviseen tietoturvatoimintaan ei ole kyetty

resurssien ja vastuutuksien takia, mutta tahtotila tietoturvallisuuden kehittämiseen tuli esille.

6 TIETOTURVALLISUUDEN HALLINTAPROSESSI KUNNILLE

Tässä luvussa esitellään tutkimuksen perusteella luotu tietoturvallisuuden hallintaprosessi (kuvio 3), jossa kuvataan prosessin vaiheet. Tässä luvussa esitellään vaiheiden toteutus sekä dokumentaatio ja/tai toimenpiteet, jotka tulisi vaiheen aikana toteuttaa.

Esiteltävän hallintaprosessin on tarkoitus yhdenmukaistaa ja koota vallitsevaa ohjeistusta tietoturvallisuuden hallintaan kunnissa. Aikaisemmin tutkimuksessa esitetty ISO/IEC 27001- standardi on raskas käyttöönotettava tietoturvallisuuden hallinnan osalta, huomioiden kuntien käytössä olevat resurssit. Vahtiohjeiden mallit ovat hajanaisia ja ne pohjautuvat pitkälti ISO/IEC27001- standardiin. Esiteltävä malli luo perustan tietoturvallisuuden hallinnan kehittämiselle, joka muotoutuu organisaatiokohtaisesti sen käytön edetessä.



Kuvio 3: Tietoturvallisuuden hallintaprosessi.

6.1 Perusteet tietoturvallisuuden hallintaan

Tietoturvallisuuden hallinta ei ole kertaluontoinen tai aina johdonmukaisesti etenevä prosessi. Kun prosessi on suoritettu parantamisvaiheen jälkeen, aloitetaan prosessi alusta. Prosessin kulkuun ja uudelleen käynnistämiseen voi vaikuttaa muun muassa lakimuutokset, johdon tahtotilan muutos ja tietoteknisen ympäristön muutokset.

Prosessin tässä vaiheessa luodaan pohja tietoturvallisuuden hallintaprosessille. Tähän vaiheeseen kuuluu tietoturvallisuuden hallintaprosessiin liittyvät vaatimukset, jotka tulevat kunnan johdolta, laeista ja asetuksista sekä toimintaympäristön ominaispiirteistä.

Organisaatiosta ja sen toimintaympäristöstä on luotava kokonaiskuva perustaksi toiminnalle. Organisaation on kuvattava sen tietotekninen ympäristö sekä sisäiset ja ulkoiset toimijat. Suomen laissa on määritelty erilaisia vaatimuksia tietoturvallisuuteen liittyen. Muun muassa tiedonhallintalain vaatimukset koskevat kuntia ja lain vaatimukset on otettava huomioon tietoturvallisuuden hallintaprosessia luotaessa ja ne on suunniteltava osaksi tietoturvallisuuden hallintaprosessia.

Lisäksi kunnan johdon tulee määrittää vaatimukset tietoturvallisuuden osalta. Nämä vaatimukset voivat tulla esille esimerkiksi tietoturvapolitiikassa tai tietoturvastrategiasta. Lisäksi tietoturvallisuuden hallinnassa tulee huomioida kuntastrategia, joka voi määrittää erityisiä vaatimuksia tietoturvallisuuden osalta.

Perustevaiheessa luotavat dokumentit ja toimenpiteet:

- Verkko- ja järjestelmäarkkitehtuurikuvaukset
- Vaatimuslistaukset
    - Lait, asetukset, ohjeet
    - Kunnan johdon vaatimukset
- Tietoturvapolitiikka ja/tai -strategia

6.2 Suunnittelu

Suunnitteluvaiheessa luodaan suunnitelma tietoturvallisuuden hallintaprosessin toteuttamiselle, tämän lisäksi toimintaympäristöstä kartoitetaan tietoturvaan kohdistuvat riskit ja analysoidaan ne. Tietoturvallisuuden suunnittelussa on otettava huomioon aikaisemmassa vaiheessa esitetyt vaatimukset ja luotava niiden pohjalta tavoitteet. Suunnittelussa on esitettävä tietoturvallisuuden hallinnan prosessi ja määritellä vastuut. Hallintaprosessin lisäksi toteutettavia asioita ovat jatkuvuudenhallinnan suunnitelmat, toimintaympäristön seuranta ja haavoittuvuuksien hallinta.

Tässä vaiheessa toteutetaan myös riskien käsittely suunnitelma, jossa määritetään riskien raja-arvot, tämän jälkeen riskit kartoitetaan ja analysoidaan.

Riskien analysointiin voidaan käyttää esimerkiksi vakavuus – todennäköisyys laskentaa, jonka lopputuloksena riskille saadaan arvo.

Suunnitteluvaiheessa luotavat dokumentit ja toimenpiteet:

- Tietoturvasuunnitelma
    - Tietoturvallisuuden hallintaprosessin toteutussuunnitelma (vuosikello)
    - Tietoturvatavoitteet
    - Riskienkäsittely suunnitelma
    - Toimintaympäristön seuranta
    - Jatkuvuudenhallinnan suunnittelu
- Riskianalyysi
    - Riskien tunnistaminen
    - Riskien analysointi

6.3 Toiminta

Toiminta vaiheessa toteutetaan riskien käsittely sekä muut tietoturvallisuuteen liittyvät vaatimukset. Aikaisemman vaiheen perusteella riskit luokitellaan niiden arvon mukaan. Riskeille toteutetaan toimenpiteet, joita voi olla riskin poistaminen, lieventäminen, hyväksyminen tai jakaminen riippuen siitä, mitkä raja-arvot ja suunnitelmat riskienkäsittelyyn on tehty. Tämän lopputuloksena on luotava toimenpiteet riskien hallitsemiseksi sekä muiden vaatimuksien täyttämiseksi ja toteutettava ne. Tietoturvariskien hallitsemiseksi tulee myös huomioida ulkoiset tietoturvapalvelut, joille tulee toteuttaa vaatimustenmäärittely, jotta palvelu tuottaa siltä vaadittavan hyödyn.

Toimintavaiheessa luotavat dokumentit ja toimenpiteet:

- Toimenpidesuunnitelma riskien hallitsemiseksi
    - Vastuut, toimenpiteet ja aikamääreet
- Vaatimukset tietoturvapalveluille

6.4 Arviointi

Arviointi vaiheessa selvitetään, kuinka toimintavaiheessa toteutetut toimenpiteet on saavuttaneet niille annetut tavoitteet. Tämä tarkoittaa mittausta ja seurantaa, auditointia sekä johdon katselmuksia.

Mittausta ja seurantaa voidaan toteuttaa muun muassa koulutuksiin, tietoturvauhka havaintoihin sekä -poikkeamiin liittyen. Mittaukseen ja seurantaan liittyy myös näiden tarkempi analysointi.

Auditointia voidaan suorittaa sisäisinä sekä ulkoisina auditointeina. Sisäisiä auditointeja voi olla esimerkiksi työpaikkakäynnit, joissa arvioidaan tiettyä tietoturvallisuuden osa-aluetta organisaation oman henkilöstön toimesta.

Ulkoiset auditoinnit voivat olla esimerkiksi järjestelmien turvallisuuden testausta (esim. penetraatiotestaus) tai tietoturvallisuuden hallintaprosessin auditointia ulkopuolisen palveluntarjoajan toimesta. Johdon katselmuksessa kunnan johto arvioi tietoturvallisuuden hallintaprosessia, jossa arvioidaan ja tarkastellaan sen toimivuutta.

Arviointivaiheessa luotavat dokumentit ja toimenpiteet:

- Mittaus ja seuranta työkalut
- Auditointisuunnitelma
- Johdon katselmus

6.5 Parantaminen

Parantamisvaiheessa tarkastetaan tietoturvallisuuden hallintaprosessin tulokset ja niiden pohjalta luodaan kehittämissuunnitelma. Tähän vaiheeseen liittyy raportointi omalle organisaatiolle, sekä yhteistyökumppaneille tarvittavilta osin. Tämän vaiheen tärkein tavoite on havaita hallintaprosessin toimivuus ja toteuttaa tarvittavat kehittämistoimet hallintaprosessiin sekä organisaation tietoturvallisuuteen.

Parantamisvaiheessa luotavat dokumentit ja toimenpiteet:

- Raportointi prosessin tuloksista
- Kehittämissuunnitelma

7 JOHTOPÄÄTÖKSET JA KESKUSTELU

Tietoturvallisuuden hallinta tulisi toteuttaa parhaalla mahdollisella tavalla ottaen kaikki mahdolliset keinot käyttöön. Todellisuudessa tietoturvallisuuden hallintaan kunnissa on kuitenkin rajalliset resurssit. Kuten tutkimuksen haastatteluissa kävi ilmi, on organisaatioilla erilaisia rajoitteita, jotka vaikuttavat tietoturvallisuuden hallintaan.

Tutkimuksen tuloksien perusteella tutkimuksen kuudennessa luvussa esitellään malli tietoturvallisuuden hallintaprosessista kunnille, joka mukailee VAHTI- ohjeiden sekä ISO27001:n linjaa. Siinä on eritelty eri vaiheissa toteutettavat toimenpiteet, joka helpottaa sen käyttöä ja kokonaisuuden hahmottamista. Prosessia voidaan käyttää pohjana, mutta on huomioitava, että jokainen kuntaorganisaatio on erilainen, joten kaikille sellaisenaan malli ei sovi, mutta voi toimia pohjana.

Kuudennessa luvussa esitetyssä mallissa tietoturvallisuuden hallintaprosessista huomioidaan pääosin myös tiedonhallintalain tietoturvavaatimukset. Kansallisessa lainsäädännössä on myös muita vaatimuksia julkisorganisaation tietoturvaan liittyen, joista tärkeimmät on esitetty tutkimuksen toisessa luvussa.

Tutkimuksen haastatteluiden perusteella voidaan todeta, että tietoturvallisuuden hallinta toteutetaan kunnissa vaihtelevasti. Haastatelluissa kunnissa ei ollut erikseen tietoturvatehtävään nimettyä henkilöä, vaan se hoidettiin muun toiminnan ohella. Haastatteluissa kävi ilmi, että kahdella kolmesta kunnasta oli käytössään digiturvamalli, jonka avulla tietoturvallisuutta pyrittiin parantamaan. Yhden kunnan osalta tietoturvallisuuden hallinnalle ei ole luotu mallia sen toteuttamiseksi. Kaikkien kuntien näkemyksien mukaan tietoturvallisuuden hallinta heidän kunnassansa oli kohtalaisella tasolla, mutta jokaisen kunnan osalta haastateltavat kertoivat, että tarvetta parannuksille löytyy.

Tutkimuksen perusteella tietoturvallisuuden hallinnan toteutuksen taso pohjautuu käytettäviin resursseihin, haastatteluiden perusteella on selvää, että halua kehittää tietoturvallisuutta löytyi, jokaisesta haastatellusta kunnasta. Resursseista tärkeimpiä ovat aika ja osaaminen. Ajan käytöllisesti organisaatioilla ei ollut kykyä resursoida henkilöstöä tietoturvallisuuden

hallinnan toteuttamiseen. Aikaresurssiin vaikuttaa myös johdon tahtotila, joka kävi ilmi haastatteluissa yhden kunnan osalta, jossa motivaatiota tietoturvan parantamiseen ei kaikilta osin päätöksentekijöiltä löytynyt. Tietoturvallisuuden hallintaa toteutetaan kunnissa pääosin tietohallintohenkilöstön toimesta, joiden tehtäviin kuuluu muun muassa lähitukipalveluita ja muita tietoteknisen ympäristön ylläpitoon liittyviä tehtäviä. Tilanne ei siis mahdollista täyttä panostusta tietoturvallisuuden hallintaan.

Osaamisen osalta, kaikilla haastatelluilla kunnilla ei ollut selkeää käsitystä, kuinka tietoturvallisuuden hallintaa tulisi toteuttaa. Ohjeita muun muassa VAHTI- verkoston toimesta, seminaareja sekä lain vaatimuksia löytyy, mutta niiden kokoaminen järkeväksi kokonaisuudeksi ja oikeiden toimintatapojen löytäminen vaikutti aiheuttavan haasteita. ICT- palveluiden ulkoistamista oli toteutettu kahdessa haastatellussa kunnassa, jolloin osa tietoturvallisuuden toimenpiteistä on myös palveluntarjoajan toteuttamaa.

Tutkimukseen osallistuneet kunnat eivät kaikilta osin ole saaneet toteutettua tiedonhallintalain tietoturvavaatimuksia. Haastatellut kunnat kertoivat, että tiedonhallintalakia on pyritty soveltamaan ja haastatteluiden perusteella lain tietoturvaan liittyvät toimet on otettu huomioon, mutta sen tavoitteisiin ei kaikilta osin ollut päästy. Kaksi kolmesta kunnasta kertoi, että heidän käytössään olevan Digiturvamallin avulla tiedonhallintalain vaatimuksia pyritään laittamaan kuntoon. Kaksi kolmesta kunnasta arvioivat, että tiedonhallintalain vähimmäisvaatimukset oli saatu täytettyä.

Osassa tiedonhallintalain vaatimuksista on ollut siirtymä aikaa vuoden 2023 alkuun asti, joiltain osin lain vaatimukset ovat tulleet voimaan jo aikaisemmin. Dokumentaatiota tiedonhallintalain vaatimuksien täyttämisestä ei haastateltavien kuntien osalta kaikilla ollut. Tähän syinä haastateltavat mainitsivat muun muassa vastuutuksen ja resurssit. Tiedonhallintalain vaatimuksien täyttämiseen tulisi kunnissa olla selkeät prosessit, joita ei haastatelluissa kunnissa ainakaan vielä ollut toteutettu kaikilta osin. Osaan lain vaatimuksista oli panostettu, mutta osa oli vaatimuksen täyttämisen haasteen takia vielä kesken. Yksi haastateltava mainitsi, että tällaiset lait saattavat ajaa kuntaorganisaatioita isompiin organisaatioihin, koska pienillä kunnilla ei ole resursseja täyttää tämän muotoisten lakien kaikki vaatimuksia.

Tiedonhallintalaissa on selkeästi pyritty kokoamaan tietoturvaan liittyviä säännöksiä yhteen, mutta julkisorganisaation tietoturvaan liittyviä säännöksiä löytyy monista eri laeista edelleen. Tämä pirstaleisuus voi aiheuttaa haasteita ottaa huomioon kaikki tärkeimmät lakien vaatimukset tietoturvaan liittyen.

7.1 Tutkimuksen arviointi

Tutkimuksessa käsiteltävä aihe on ajankohtainen. Viime vuosina uutisista on saatu lukea, kuinka useat suomalaiset organisaatiot ovat joutuneet tietoturvahyökkäysten uhreiksi yhä enenevissä määrin. Myös kuntaorganisaatiot ovat joutuneet hyökkäyksien kohteeksi, kuten Säkylän kunta vuoden 2022

loppupuolella ja hyökkäyksistä aiheutuneissa kuluissa puhutaan usein sadoista tuhansista. Hyökkäyksen toteuttaminen on riskeihin nähden halpaa ja tutkinta-ajat ovat pitkiä. Verkkorikosten selvittämisprosentit jäävät myös alhaisiksi. Säkylän tapauksessa hyökkäyksen vahingoiksi on arvioitu noin 400 000 euroa (Kykkänen, 2023). Tutkimuksen tuloksista voidaan päätellä, että tarvetta tutkimukselle ja keinoille kuntien tietoturvallisuuden hallintaan liittyen on.

Tutkimuksen aineisto kerättiin aihetta käsittelevästä kirjallisuudesta sekä haastatteluina kolmen kunnan haastatteluina. Tutkimuksesta ei saatu tehtyä tavoitellun kattavaa haastateltavien osalta. Tutkimuksen tulokset eivät ole kattavia tai yleistettäviä kaikilta osin. Tutkimukseen haastatellut kunnat olivat kooltaan 4000, 8000 ja 25000 asukkaan kuntia. Vaikka yleistettävyyttä ei tutkimuksessa saavutettu, voidaan kuitenkin todeta, että tietoturvallisuuden hallinta kunnissa toteutetaan vaihtelevasti ja sen kehittämiseen on tarvetta. Tietoturvallisuuden hallintaan liittyviä prosesseja ei ole käytössä, siten kuin laki velvoittaa. Tutkimuksen kirjallisuuskatsauksessa käytettyä aineistoa voidaan pitää laadukkaana ja varsinkin ISO-standardit ovat kansainvälisesti hyväksyttyjä, jolla laatu voidaan todentaa. Kirjallisuuskatsauksen sekä haastatteluiden perusteella luotu luvun kuusi malli tietoturvallisuuden hallintaprosessista voidaan pitää perusteltuna.

Tutkimuksen aiheen laajuudesta takia tutkimuksessa ei paneuduttu hallintaprosessin vaiheiden yksityiskohtaisempaan tarkasteluun. Luvussa kuusi esitelty malli toimii pohjana, joka on muokattavissa organisaatiokohtaisesti. Tutkimuksen tarkoituksena oli tuoda esiin tietoturvallisuuden hallintaprosessin tärkeys ja tiedonhallintalain vaatimukset, jotta kuntaorganisaatiot toteuttaisivat tietoturvallisuutta hallitusti ja johdetusti. Tutkimuksen kantavana ajatuksena oli luoda malli, joka palvelisi kuntaorganisaatioiden tietoturvallisuuden hallintaa.

7.2 Tutkimuksen hyödynnettävyys ja jatkotutkimus

Tutkimuksen luvussa kuusi kuvattu malli tietoturvallisuuden hallintaprosessista on hyödynnettävissä useissa eri organisaatioissa, vaikka tutkimus keskittyikin kuntaorganisaatioihin. Jatkotutkimuksessa voitaisiin pureutua syvemmälle tietoturvallisuuden käytännön toteutuksiin kunnissa tai laajentaa tutkimuksessa saatuja havaintoja kohti yleistettävyyttä esimerkiksi määrällisen tutkimuksen menetelmin.

Jatkotutkimusaiheita voisivat olla:

- Tietoturvallisuuden hallintatoimet kuntaorganisaatioissa, jossa tarkasteltaisiin tarkemmin tietoturvatoimenpiteitä kunnissa. Täten päästäisiin pureutumaan syvemmälle tietoturvallisuuden toteutukseen.
- Tietoturvallisuuden tila kuntaorganisaatioissa, jossa määrällisen tutkimuksen keinoin hankittaisiin tietoa yleisesti tietoturvallisuuden tilasta ja siihen vaikuttavista tekijöistä.

- Digiturvamallin toteutus ja käytettävyys kuntaorganisaatioissa, jossa tämänkin tutkimuksen haastatteluissa ilmi tulleen Digiturvamallin hyötyjä ja ongelmakohtia tarkasteltaisiin tietoturvallisuuden hallinnan näkökulmasta.

LÄHTEET

Anttila, P. (1998). Tutkimisen taito ja tiedonhankinta. Metodix Oy. Noudettu osoitteesta: https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Digi- ja väestötietovirasto. (2021). Digiturvallisuuden hallinta: VAHTI hyvät käytännöt tukimateriaali. Noudettu osoitteesta: https://dvv.fi/digiturvajulkaisut

Hänninen, J. (2020). Riskienhallinta pienien ja keskisuurien kuntien digitaalisessa turvallisuudessa – tapaustutkimus. Pro gradu -opinnäytetyö. [pro gradu -tutkielma, Jyväskylän yliopisto]. JYX-julkaisuarkisto. Noudettu osoitteesta: http://urn.fi/URN:NBN:fi:jyu-202011136636

International Organization for Standardization. (2016). ISO/IEC 27000:2016. Noudettu osoitteesta: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

International Organization for Standardization. (2018). ISO/IEC 31000:2018. Noudettu osoitteesta: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

Kuntalaki 10.4.2015/410

Kuntaliitto. Sosiaali- ja terveystoimen tilastot. Suurten ja keskisuurten kaupunkien sosiaali- ja terveystoimen kustannukset. Noudettu 3.2.2023 osoitteesta: https://www.kuntaliitto.fi/sosiaali-ja-terveysasiat/tilastot-ja-erillisselvitykset/suurten-ja-keskisuurten-kaupunkien-sosiaali-ja-terveystoimen-kustannukset

Kykkänen, V. (8.2.2023). Eduskunnassa on havaittu verkkohyökkäyksiä, joilla tavoitellaan yhä laajempaa vahinkoa: ”Muuttuneet teknisesti haastavammiksi”. MTV. Luettu 30.3.2023. Noudettu osoitteesta: https://www.mtvuutiset.fi/artikkeli/eduskunnassa-on-havaittu-verkkohyokkayksia-joilla-tavoitellaan-yha-laajempaa-vahinkoa-muuttuneet-teknisesti-haastavammiksi/8628896#gs.txmqsx

Laki julkisen hallinnon tiedonhallinnasta 9.8.2019/906

National Institute of Standards and Technology. (2003a) NIST Special Publication 800-35: Guide to Information Technology Security Services. Noudettu osoitteesta: https://csrc.nist.gov/publications/detail/sp/800-35/final

National Institute of Standards and Technology. (2011) NIST Special Publication 800-39: Managing Information Security Risk. Noudettu osoitteesta: https://csrc.nist.gov/publications/detail/sp/800-39/final

National Institute of Standards and Technology. (2003b) NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program. Noudettu osoitteesta: https://csrc.nist.gov/publications/detail/sp/800-50/final

National Institute of Standards and Technology. (2020) NIST Special Publication 800-53 revision 5: Security and Privacy Controls for Information Systems and Organizations. Noudettu osoitteesta: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

National Institute of Standards and Technology. (2006) NIST Special Publication 800-100: Information Security Handbook: A Guide for Mangers. Noudettu osoitteesta: https://csrc.nist.gov/publications/detail/sp/800-100/final

Raggad, B.G. (2010). Information Security Management. Taylor & Francis Group. Boca raton.

Suomen Standardisoimisliitto SFS. (2022a) ISO/IEC 27001:2022.

Suomen Standardisoimisliitto SFS. (2022b) ISO/IEC 27002:2022.

Tammelin, J. (2021). Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa. Pro gradu -opinnäytetyö. [pro gradu -tutkielma, Jyväskylän yliopisto]. JYX- julkaisuarkisto. Noudettu osoitteesta: http://urn.fi/URN:NBN:fi:jyu-202102171681

Tilastokeskuksen väestörakennetilasto (2022). Kuntajako. Noudettu osoitteesta: https://www.kuntaliitto.fi/kuntaliitto/tietotuotteet-ja-palvelut/kaupunkien-ja-kuntien-lukumaarat-ja-vaestotiedot

Tilastokeskus. Tilastollinen kuntaryhmitys. Noudettu 3.2.2023 osoitteesta: https://www.stat.fi/meta/kas/til_kuntaryhmit.html

Traficom (2020). Kyberturvallisuus ja yrityksen hallituksen vastuu. Traficomin julkaisuja 2/2020. ISBN 978-952-311-465-4

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

Valtiovarainministeriö (2020). Julkisen hallinnon digitaalinen turvallisuus. Valtiovarainministeriön julkaisuja 2020:23. http://urn.fi/URN:ISBN:978-952-287-857-1

Valtiovarainministeriö (2022a). Julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys. Valtiovarainministeriön julkaisuja – 2022:76. Noudettu osoitteesta: https://julkaisut.valtioneuvosto.fi/handle/10024/164465

Valtiovarainministeriö (2022b). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö. Valtiovarainministeriön julkaisuja – 2022:43. Noudettu osoitteesta: https://julkaisut.valtioneuvosto.fi/handle/10024/164183

Valtiovarainministeriö (2021). Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta. Valtiovarainministeriön julkaisuja – 2021:65. http://urn.fi/URN:ISBN:978-952-367-897-2

Valtiovarainministeriö (2014). VAHTI- ohje 2/2014. Tietoturvallisuuden arviointiohje. Suomi

Valtiovarainministeriö (2013). VAHTI- ohje 2/2013. Toimitilojen tietoturvaohje. Suomi

Valtiovarainministeriö (2007). VAHTI- ohje 03/2007. Tietoturvallisuudella tuloksia. Suomi.

Valtiovarainministeriö (2012). VAHTI- ohje 3/2012. Teknisen ICT- ympäristön tietoturvataso- ohje. Suomi

Valtiovarainministeriö (2006). VAHTI- ohje 06/2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. Suomi.

Valtiovarainministeriö (2017). VAHTI- ohje 22/2017. Ohje riskienhallintaan. Suomi

Whitman, M.E. (2008). Security Policy: From Design to Maintenance. Teoksessa S. Goodman, D. W. Straub & R. Baskerville (toim.), Information Security: Policy, Processes, and Practices (s. 123-151). Routledge.

Wolke, T. (2017). Risk Management. Walter de Gryuter GmbH, Berlin.

Woodside, A.G. (2017) Case study research: Core Skill Sets in Using 15 Genres. Secon edition. Emerald Group, Bingley.