Jussi Tammelin

TIETOTURVASTRATEGIAN JA -POLITIIKAN MERKITYS KYBERHYÖKKÄYKSEN TORJUNNASSA KUNNISSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Tammelin, Jussi

Tietoturvastrategian ja -politiikan merkitys kyberhyökkäyksen torjunnassa kunnissa.

Jyväskylä: Jyväskylän yliopisto, 2021, 71 s.

Tietojärjestelmätiede, pro gradu

Ohjaaja(t): Martti Lehto, Viinikainen, Ari

Eri julkisia organisaatioita kohtaan on tapahtunut viime vuosi useita onnistuneita ja julkisuuteen nousseita kyberhyökkäyksiä. Vuonna 2019 muun muassa Lahden ja Kokemäen kaupunkien tietojärjestelmiin toteutettiin onnistuneet hyökkäykset. Hyökkäysten tekninen tutkinta ja siitä tehtävät analyysit kuuluvat poliisille, mutta kuntien tietoturvallisuuden ohjausta voidaan tutkia hyökkäysten viitekehyksessä. Tässä tutkimuksessa tutkittiin näitä kahta onnistunutta kyberhyökkäystä ja selvitettiin, miten kaupunkien tietoturvapolitiikka vaikutti hyökkäysten torjuntaan, rajaamiseen sekä niistä palautumiseen. Teoreettinen pohja rakennettiin asiakirjatutkimuksella tietoturvastrategiasta ja politiikasta, lainsäädännöstä sekä tietoturvan hallintajärjestelmistä. Tapaustutkimus toteutettiin asiantuntijoiden haastattelulla. Tutkimusten tulosten perusteella voidaan päätellä, että tietoturvastrategian ja -politiikan sisältöä on määritelty riittävästi käytettäväksi kunnissa, lainsäädäntöä on Suomessa paljon ja se on hajanaista sekä tietoturvan hallintajärjestelmää voidaan käyttää julkisessa organisaatiossa. Varsinaisten tapausten tutkimuksessa selvisi, että tutkimuskohteiden tietoturvapolitiikat olivat rakenteellisesti varsin erilaisia, niiden muodostamiseksi ei ollut kunnollista ohjausta ja Kokemäen tietoturvapolitiikalla oli suurempi merkitystä kyberhyökkäyksen torjunnassa kuin Lahdessa. Tutkimuksen tulosten perusteella löytyi useita eri osa-alueita, joihin tutkimusta voidaan laajentaa ja konkreettisia toimenpiteitä, joilla kuntien tietoturvapolitiikkaa voidaan parantaa.

Asiasanat: Tietoturvastrategia, tietoturvapolitiikka, tietoturvallisuuden hallintajärjestelmä, kunnat, kyberhyökkäys, tietoturva

ABSTRACT

Tammelin, Jussi

The role of the information security strategy and policy in combating cyber-attack in municipalities.

Jyväskylä: University of Jyväskylä, 2021, 71 s.

Cyber security, master's thesis

Instructors: Martti Lehto, Viinikainen, Ari

There have been a number of successful and publicized cyber-attacks against various public organizations over the past year. In 2019, successful attacks were carried out on the information systems of the cities of Lahti and Kokemäki, among others. The technical investigation and analysis of attacks is the responsibility of the police, but municipal information security guidance can be examined in the context of these attacks. This thesis examined these two successful cyber-attacks and examined how urban security policies affected the prevention, containment, and recovery from these attacks. The theoretical basis was built through document research on information security strategy and policy, legislation, and information security management systems. The case study was conducted through an interview with experts. Based on the results of the research, it can be concluded that the content of the information security strategy and policy has been sufficiently defined for use in municipalities, there is a lot of legislation in Finland and it is fragmented, and the information security management system can be used in a public organization. The study of the actual cases revealed that the information security policies of the research subjects were structurally quite different, there was no proper guidance for their formation, and Kokemäki's information security policy in particular had a important role in combating cyber-attacks. Based on the results of the study, several different areas were found to which the study can be extended and concrete measures to improve the information security policy of municipalities.

Keywords: Information security strategy, information security policy, information security management system, municipalities, cyber-attack, information security

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

1.1 Tutkimuksen tausta

Tietoturvallisuus on illuusio siitä, miten hyvin omat toimenpiteet toiminnan jatkuvuudeksi kohtaavat sitä vastaan oletetut riskit. Kun illuusio murtuu esimerkiksi onnistuneen kyberhyökkäyksen vuoksi, palataan perusasioiden äärelle ja alkaa pohdinta, mitä olisi pitänyt tehdä toisin. Mitä isompi organisaatio ja mitä laajemmat tuhot, sitä laajemmat kustannukset. Ja usein kustannukset eivät ole suhteessa tapahtuneen mahdollisesti estäneen varautumisen kustannuksiin.

30.10.2020 Mikkelin puhelinyhdistyksen tietohallintopäällikkö Toni Sivupuro totesi Yleisradion haastattelussa, että tulevaisuudessa verkkohuijaukset ja tietomurrot tulevat yleistymään. Hän ei ollut ainoa asiantuntija, joka ennusti tällaista tulevaisuutta, sillä kaksi viikkoa aiemmin oli tullut julkisuuteen Vastaamo Oy:n tietomurto, jossa ihmisten potilastietoja oli varastettu laajasti. Sitä ennen muun muassa Kokemäen kaupunki ja Lahden kaupunki olivat joutuneet kyberhyökkäyksen kohteeksi, joissa jokaisessa kaupungin tietoverkkoon oli onnistuneesti murtauduttu. Molempien kaupunkien kyberhyökkäykset olivat julkisuudessa tapahtuma-aikoina 2019. Lahden kaupungin kyberhyökkäyksen vaikutusten laajuus nosti hyökkäyksen uutisiin muun muassa YLE-uutisissa 12.6.2019. (Yleisradio, 2019) Kaupunkien kohdalla toiminnan jatkuvuus kärsi, syntyi merkittävä toimintakatkos, suuret kustannukset ja lopulta ei edes täysin tiedetty, mitä menetettiin.

Julkisuuteen annettujen tietojen perusteella voi päätellä, ettei kyseisten yksityisten tai julkisten organisaatioiden tietoturva ollut ajan tasalla. Lahden kaupungin hyökkäyksen jälkeen Traficomin johtava asiantuntija Kauto Huopio totesi YLE-uutisten haastattelussa, että kaikilla kunnilla on tekemistä tietoturvan kehittämiseksi. (Yleisradio, 2019) Jokaisen julkisuuteen nousseen onnistuneen hyökkäyksen taustalla vaikuttaa olleen puutteellinen varautuminen tietoturvauhkiin eri osa-alueille. Hyökkäykset kohdistuivat tietoverkon teknisen konfiguraation puutteeseen, toimintatapoihin ja ylläpitäjien oletuksiin. Tämä voisi viitata siihen, että korkeamman tason ohjauksessa kuten

tietoturvastrategiassa ja -politiikassa on ollut puutteita ja nämä puutteet ovat voineet johtua osin tai kokonaan julkisen ohjeistuksen määrästä tai laadusta.

Tässä tutkimuksessa tutkitaan, auttoiko tutkimuskohteissa muodostettu tietoturvastrategia ja -politiikka kyberhyökkäyksen torjunnassa, mikä oli niiden merkitys kyberhyökkäyksen rajaamisessa sekä selvittämisessä ja kehittyykö strategia ja politiikka hyökkäyksen jälkeen.

1.2 Tutkimuksen viitekehys

Tutkimuksen viitekehyksenä toimii strategiasta johdettu tietoturvastrategia ja sen johdannaiset, politiikan käsitteestä johdettu tietoturvapolitiikka, ISO27000-standardisarja, julkishallinnon lainsäädännöllinen ohjaus sekä kunnat. Tutkittavana ilmiönä on tietoturvastrategian ja -politiikan vaikutus kyberhyökkäykseen. Ajallinen ja toiminnallinen viitekehys on kyberhyökkäystä ennen ja jälkeen tapahtuneet muutokset tietoturvan ohjauksessa, tietoturvastrategiassa ja -politiikassa.

Tutkimuksen tietoturvan hallintamallin viitekehyksenä käytetään eurooppalaista ISO27000-standardisarjaa ja ISO27001-standardissa esitettyä tietoturvallisuuden hallintajärjestelmän rakennetta. Valtionhallinnon digitaalinen turvallisuuden johtoryhmä (VAHTI) on käyttänyt valtionhallinnon ohjeistuksessa ISO27001-standardin rakennetta, jolloin sen soveltaminen kuntatasolle on jo osin ohjeistettu. Valtion toimijoista terveyden ja hyvinvoinnin laitos on aloittanut ISO27001-standardin tutkimisen osana tietoturvan hallintajärjestelmän kehittämistä. Tutkimuksessa ei oleteta, että tietoturvan hallintajärjestelmän käyttöönotto johtaisi järjestelmän auditointiin.

Viitekehyksessä toimija on kunta. Toimijaan kuuluu organisaatio, jonka tehtävänä on toteuttaa toimijalle määritettyjä tehtäviä, kuten tietoturva.

Tutkimuksen viitekehyksessä materiaali muodostuu haastatteluista ja julkisista asiakirjoista. Kuntien toimintaa ohjaa dokumentoitu strategia, jolla kunnan johdon tavoite viestitään. Julkisyhteisöille on tyypillistä, että strategian rinnalla on useita osastrategioita tai politiikka ohjaamassa eri toimialojen työtä. Nämä asiakirjat ovat suurelta osin julkisia ja siksi tutkimuksen kannalta yleisesti saatavilla.

Tutkittava ilmiö on tietoturvastrategian ja politiikan muodostuminen sekä niiden muutos kyberhyökkäyksen jälkeen. Tutkimus ajoittuu lähihistoriassa tapahtuneisiin kyberhyökkäyksiin sellaisia toimijoita kohtaan, joilla on ollut tietoturvapolitiikka ja siinä voidaan olettaa tapahtuneen muutoksia hyökkäyksen jälkeen.

1.3 Tutkimuksen tavoite ja kysymykset

Lahden ja Kokemäen kyberhyökkäyksiä 2019 voidaan luonnehtia onnistuneeksi, koska kohdeorganisaatioiden toiminta estyi osin tai kokonaan ja tietoverkoissa käsiteltyä tietoa menetettiin pysyvästi. Molemmilla kaupungeilla oli

muodostettu tietoturvapolitiikka, mutta ei strategiaa. Miksi hyökkäykset sitten lamauttivat kaupunkien toimintaa ja opittiinko niistä jotain?

Tutkimuksen tavoitteena on selvittää, vaikuttiko kohdeorganisaatioiden mahdolliset tietoturvastrategiat ja -politiikat kyberhyökkäykseltä suojautumiseen, sen torjuntaan ja siitä palautumiseen. Tutkimuksella selvitetään tietoturvan hallintajärjestelmän merkitystä tietoturvapolitiikan kehittymiselle. Tutkimus selvittää, miten voimassa ollut tietoturvaohjaus vaikutti hyökkäyksen torjuntaan ja siitä palautumiseen ja mitä muutoksia tietoturvapolitiikassa julkisessa organisaatiossa tapahtuu sen jälkeen, kun se on joutunut kyberhyökkäyksen kohteeksi. Tutkimuksen viitekehyksestä on selvitettävä strategian yleinen rooli tietoturvan muodostamisessa, siitä johdetun politiikan yleinen sisältö ja sen vaikutus tapahtumiin. Lisäksi tutkimuksesta on tultava ilmi, millä menetelmillä toimijat hyödyntävät kyberhyökkäyksestä saadut havainnot ja vievät ne osaksi tietoturvan kehitystä.

Tutkimuksen pääkysymykset ovat:

- Vaikuttiko voimassa ollut tietoturvastrategia ja -politiikka kyberhyökkäyksen torjuntaan, rajaamiseen ja siitä palautumiseen
- Muuttuuko toimijan tietoturvapolitiikka kyberhyökkäyksen seurauksena

Tutkimuksen apukysymykset ovat:

- Mikä oli toimijan tietoturvastrategia ja -politiikka ennen hyökkäystä?
  - Miten siihen oli päädytty?

Mitä tietoturvastrategian ja -politiikan tulisi sisältää?

- Mikä on kansallinen lainsäädännöllinen ohjaus
- Mikä on tietoturvan hallintajärjestelmien hyödynnettävyys?

Tutkimuksen tuotteena kohdeorganisaatioiden tietoturvastrategia ja -politiikkaa käydään läpi ja arvioidaan voimassa ollutta lainsäädäntöä ja ISO27001 tietoturvan hallintajärjestelmän sisältöä hyödyntäen. Erityisesti tietoturvapolitiikan vaikuttavuutta tapahtuneen kyberhyökkäyksen torjuntaan ja siinä tapahtunutta muutosta arvioidaan tietoturva-alan yleisten hyvien käytäntöjen pohjalta.

Tutkimuksen tuloksena kohdeorganisaatiolle tulisi syntyä kuva, mikä on tietoturvastrategian ja -politiikan vaikutus kyberhyökkäyksen torjunnassa, miten ne voidaan muodostaa sekä miten käytössä olevaa strategiaa ja politiikka voisi edelleen parantaa.

1.4 Tutkimuksen tavoitteet, rajaukset ja yleistettävyys

Tutkimus kohdistetaan Suomessa tapahtuneisiin kahteen kyberhyökkäykseen Lahdessa ja Kokemäellä ja referensseinä käytetään Espoon ja Virtain kaupunkien tietoturvapolitiikkaa. Kohteet ovat julkishallinnon organisaatioita, jolloin kohdeorganisaation suojautumiseen vaikuttaneet strategiat ja politiikat ovat julkisia ja lähdeaineisto on saatavilla. Lisäksi hyökkäykset ovat riittävät uusia, jolloin kohdeorganisaatioiden tietoturvastrategia ja -politiikkatyön osallistuneet henkilöt ovat vielä osin samoissa tehtävissä. Espoon ja Virtain kaupungit on

valittu tutkimuksen vertailukaupungeiksi, koska niillä on olemassa tietoturvapolitiikka, mutta niitä kohtaan ei ole vielä toteutettu kyberhyökkäystä tai sitä ei ole tunnistettu ja/tai raportoitu.

Tutkimus kohdistuu kohdeorganisaatioiden tietoturvallisuuteen tietoturvan hallintajärjestelmän kautta. Tutkimuksen tarkoituksena on tarkastella tietoturvallisuuden kokonaisuutta keskittymättä yksittäisiin teknisiin tai toiminnallisiin tietoturvan tai tietosuojan osa-alueisiin. Tietoturvallisuuden määritelmänä käytetään VAHTI 2008 ”Valtionhallinnon tietoturvasanasto” määritelmää: ”Järjestelyt, joilla pyritään varmistamaan tiedon eheys, luotettavuus ja käytettävyys”. (Valtiovarainministeriö, 2008)

Tutkimuksessa käsite ”toimija” kuvaa organisaatiota tai sen osaa, joka suunnittelee, toteuttaa tai kehittää tietoturvaan liittyvää tietoturvastrategiaa tai politiikkaa. Käsitteellä pyritään yleistämään yksityiset ja julkishallinnolliset organisaatiot yhden käsitteen alle tutkimuksen viitekehyksessä.

Vaikka tutkimuksen kohteena on strategia ja politiikka, tutkimus ei ota kantaa siihen, millä menetelmillä kyseisiin dokumentteihin on päädytty ja miten niitä mitataan. Julkishallinnon osalta käsitellään ainoastaan päätöksentekoon liittyvää prosessia yleisesti, jotta lukijalle syntyy käsitys kunnallisesta päätöksenteosta.

Tutkimus ei selvitä teknisiä yksityiskohtia kohdeorganisaation varautumisessa eikä hyökkääjän keinoja hyökkäyksen toteutuksessa. Suojautumiskeinot ovat tyypillisesti organisaatiossa salaista tietoa. Hyökkääjän hyökkäysmenetelmät eivät kummassakaan tapauksessa ole täysin tiedossa eikä niiden yksilöinti teknisesti muuta tutkimusasetelmaa strategian tutkimuksena.

Tutkimukseen on valittu kaksi lähihistoriassa tapahtunutta kyberhyökkäystä. Tutkimus ei luo kattavaa asetelmaa yleistettäväksi kaikkiin julkishallinnon organisaatioihin. Tutkimusta voidaan laajentaa lisäämällä tapauksia sekä laajentamalla kohdeorganisaatioita yksityisen sektorin toimijoihin. Tämä luo mahdollisen pohjan tulosten yleistämiseksi kohdeorganisaation tyypistä riippumatta.

Tietoturvan osalta tietosuojaa ei käsitellä tässä tutkimuksessa, vaikka se onkin merkittävä osa tietoturvallisuutta. Kohdeorganisaatioiden tietoturvapolitiikoista ennen hyökkäyksiä sitä ei otettu vielä huomioon eikä sen käsittely tarjoa olennaista lisäarvoa tutkimuksen tuloksiin.

Tässä tutkimuksessa oletetaan, että kohdeorganisaatioilla on tehty jotain kirjallisia tietoturvastrategisia tai -poliittisia linjauksia ennen kyberhyökkäystä. Lisäksi oletetaan, että kohdeorganisaatiot ovat reagoineet hyökkäykseen ja muuttaneet ohjeistustaan havaintojensa perusteella.

2 TUTKIMUSMENETELMÄT

Tässä empiirisessä tutkimuksessa tutkimusmenetelmänä käytetään kvalitatiivista tutkimusta, joka toteutetaan tapaustutkimuksena sisältäen asiakirjatutkimusta ja asiantuntijoiden teemahaastatteluja. Tutkittava kokonaisuus muodostuu tutkittavista tapauksista, joiden ymmärtämiseksi on rakennettava teoreettinen pohja. Tutkittavat tapaukset ovat riittävän uusia, jotta keskeisten tapauksiin liittyneiden asiantuntijoiden tehtävät eivät ole vielä vaihtuneet, mutta tapauksia on ehditty reflektoimaan.

Kvalitatiivinen tutkimusmenetelmä on valittu, koska kvantitatiivisen tutkimuksen tekeminen aiheesta ei sovellu aiheen yksityiskohtaiseen käsittelyyn eikä varsinaista tutkimuksen loppuasetelmaa voida ennustaa tutkimuksen alkuvaiheessa. Tutkimusta ei myöskään voi mallintaa tai eksperimentoida, sillä varsinaisia tapauksia ei voi irrottaa niiden todellisen elämän kontekstista. Kvalitatiivinen menetelmä antaa tutkijalle vapauden ohjata tutkimusta koko tutkimuksen keston ja näin lopputuloksesta tulee paremmin tietotarpeita vastaava. (Metodix Oy, 1998) Lisäksi tutkimuksen tavoitteena on ymmärtää tietoturvastrategian ja -politiikan yksityiskohtia ja kehitystä kohteena olevilla toimijoilla. Työskentelyn ajattelumallina käytettiin Hans-Georg Gadamerin mallia hermeneuttisesta kehästä (esiymmärrys – osien ymmärrys – kokonaisuuden tarkastelu – syvempi ymmärrys).

Tutkimuksen ja siinä käytettyjen menetelmien arviointi ja soveltuvuus tutkimukseen ovat tutkimuksen pohdintaosuudessa.

2.1 Tapaustutkimus

Tapaustutkimus on menetelmä, joka pyrkii kuvailemaan, ymmärtämään, ennustamaan ja ohjaamaan yksittäistä prosessia, ihmistä, taloutta, organisaatiota, teollisuuden alaa, kulttuuria tai kansallisuutta. (Woodside & Woodside, 2017) Määritelmä on laajempi, kuin Robert K. Yinin määritelmä, joka rajautuu tutkimaan ilmiöitä todellisessa kontekstissa varsinkin silloin kuin todellisuuden ja teorian välinen raja ei ole selvä. (Yin, 2018)

Tapaustutkimus soveltuu sellaiseen tutkimukseen, jossa tietoa on saatavissa ja hankitaan useilla eri tavoilla, tutkittavana oleva asia voidaan rajata tiettyyn tapaukseen tai ympäristöön. Tapaustutkimuksen tutkimusmenetelmänä voidaan käyttää sekä kvantitatiivisen tutkimuksen että kvalitatiivisen tutkimuksen menetelmiä.

Tapaustutkimukselle tyypillisiä piirteitä ovat:

- tutkimukset ovat luonteelta syvätutkimuksia, jotka antavat tutkittavasta kohteesta hyvin tarkan kuvan
- tapaustutkimus pyrkii tutkimaan suppeaa kohdetta suurella määrällä muuttujia

- tapaustutkimus tuottaa usein taustainformaatiota, joiden pohjalta tutkimusta voidaan suunnata tai uusia tutkimuskohteita avata. Se soveltuu myöhempien tutkimusten kartoitukseen ja taustoitukseen
- tutkimusmenetelmä tuottaa tietoa esimerkiksi tilastollisen tutkimuksen tuloksista johdetuista lisäkysymyksistä
- tapaustutkimuksen heikkous on sen kapea-alaisuus, ja tulokset eivät välttämättä ole yleistettävissä. (Metodix Oy, 1998)

Tapaustutkimuksessa tutkija ja tutkittava ovat vuorovaikutuksessa, joka voi hallitsemattomana vaikuttaa tutkimuksen etenemiseen. Tutkittavat tapaukset ovat tutkijan tulkintaa tapauksesta ja useiden tutkimuksessa tulisi olla useita näkökulmia tutkittavaan tapaukseen. Tapaustutkimukseen liittyy myös toistettavuus, joskin reaaliajassa tutkittavan tapauksen osalta täysi toistettavuus on usein mahdotonta. (Metodix Oy, 1998)

Tapaustutkimuksen käytössä on viisi keskeistä haastetta:

- tapaustutkimuksen tutkimusotteen löystyminen kesken tutkimuksen
- tapaustutkimuksen menetelmien sekoittaminen ei-tieteellisiin menetelmiin
- tapaustutkimuksen yleistettävyys
- tapaustutkimuksen työmäärän hallittavuus
- tuottaako tapaustutkimus etua verrattuna muihin tutkimusmenetelmiin. (Yin, 2018)

Näihin haasteisiin pyritään vastaamaan seuraavasti tässä tutkimuksessa:

- tutkimustapaukset ovat rajautuneet ajallisesti ja niiden aineiston keruuta rajataan tutkimuksessa
- tutkimus ei perustu yksittäisiin lähteisiin
- tutkittavien kohteiden lisäksi on valittu referenssikohteita, jotka edustava kansallisesti samankaltaista kohdetta
- tutkimustapausten määrää on rajoitettu ja niihin liittyvien haastatteluiden määrää on rajoitettu. Tämän keinon sivuvaikutus voi olla tutkimuksen yleistettävyyden heikkeneminen
- tutkimusmenetelmä soveltuu kyseessä olevien tapausten tutkimuseen sekä viitekehyksen että rajauksen puolesta ja se pystyy vastaamaan tutkimuskysymyksiin. Menetelmän valinnalla on vaikutus tutkimuksen yleistettävyyteen.

2.2 Aineistonkeruumenetelmät

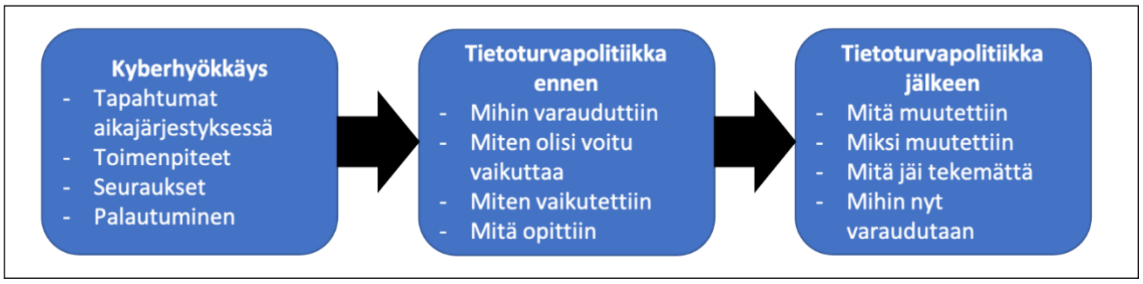
Tutkimuksen aineiston keruumenetelminä ovat asiakirjatutkimus ja asiantuntijahaastattelut. Asiakirjatutkimuksella luodaan teoreettinen valittujen tutkimuskohteiden tietoturvallisuuden muodostumisesta ja sen mahdollisuuksista sekä haasteista. Haastattelututkimuksella selvitetään tutkittuihin tapauksiin osallistuneiden asiantuntijoiden näkemyksen kautta tapahtumien kulku sekä tietoturvallisuuden tila ennen ja jälkeen tutkittujen kyberhyökkäysten.

Asiakirjatutkimus ja haastattelut soveltuvat hyvin tapaustutkimuksen aineiston keräämiseen. Tutkimuksen viitekehyksessä myös muita

aineistonkeruumenetelmiä kuten kyselytutkimus olisi voitu soveltaa täydentämään näkökulmia. (Metodix Oy, 1998)& (Yin, 2018)

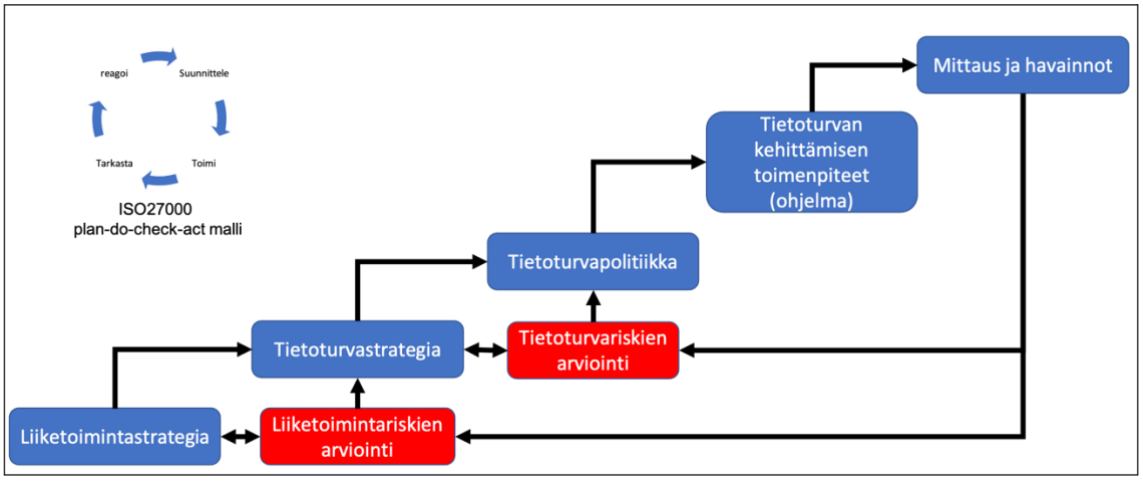
Tutkimuksen asiakirja-aineiston kartoittaminen toteutettiin tutustumalla aihepiirin muuhun tutkimukseen ja keskeisiin painettuihin teoksiin sekä tietoverkkohauilla. Näiden pohjalta materiaali jaettiin tutkimuksen teorialukujen mukaisesti ja materiaali tutkittiin. Tämän pohjalta koostettiin tutkimuksen kannalta keskeinen teoria. Teoriatutkimukseen materiaalia oli tarjolla riittävästi, joskin tutkittaessa suomalaista lainsäädäntöä sen suuri määrä ja tietoturvallisuuteen liittyvät lainsäädännön hajanaisuus hidastivat materiaalin kartoittamista.

Tutkimuksen asiantuntijahaastattelut toteutettiin teemahaastatteluna ja niissä noudateltu kehys on kuviossa 1. Haastattelulla pyrittiin selvittämään tapauksiin osallistuneilta henkilöiltä, mikä on heidän näkemyksestään tietoturvallisuuden ohjauksen (tietoturvastrategia- ja politiikka) tila ennen kyberhyökkäystä, mikä oli kyberhyökkäyksen kulku ja se seuraukset sekä hyökkäyksen jälkeiset muutokset tietoturvallisuuden ohjauksessa. Haastateltaville lähetettiin kehys ennen haastattelua tutustuttavaksi.



KUVIO 1 Asiantuntijahaastatteluiden rakenne

Haastatteluiden aluksi tietoturvallisuuden muodostumisen rakenne tietoturvallisuuden hallintajärjestelmän näkökulmasta avattiin haastateltaville kuvion 2 viitekehyksessä. Lisäksi haastateltavien kanssa käsiteltiin ISO27000-sarjan aiemmissa osissa esiintynyt Plan-Do-Check-Act-malli, jota ei enää käytetä vuoden 2020 julkaisussa. (Suomen standardisoimisliitto SFS, 2020)



KUVIO 2 Tietoturvallisuuden hallintajärjestelmän viitekehys ja plan-do-check-act-malli

Kerättävän aineiston luotettavuus ja laatu on keskeistä laadullisessa tutkimuksessa. Tutkija usein olettaa, että hänen löytämänsä aineisto on totta. Tätä oletusta tulee välttää ja pyrkiä löytämään totuus tutkimalla tapausta useista näkökulmista sekä lähteistä. Aineiston keruuprosessi on otettava huomioon arvioitaessa tutkittavan materiaalin laatua. (Metodix Oy, 1998)

2.3 Aineiston analyysi

Tiedon analyysin strategiaksi valittiin tiedon kertyminen ja sen kautta teorian rakentaminen sekä tämän yhdistäminen ennalta tunnettuun viitekehykseen ISO27000-standardisarjassa. Tiedon kerryttäminen ja siitä teorian rakentaminen on yksi Robert K. Yinin mainitsemista keskeisistä tiedon analyysin menetelmistä. (Yin, 2018)

Analyysitekniikaksi valittiin selityksen muodostaminen kerätystä tiedosta. Tässä tekniikassa pyritään selvittämään, miten tai miksi tapaus eteni lopputulokseensa. Tapauksiin sovellettiin myös aikaan sidottua tekniikkaa, jossa tapausta tutkitaan sen ajallisessa ilmenemisjärjestyksessä. Tämä mahdollistaa tietoturvapolitiikan kehittymisen vertailun ennen ja jälkeen kyberhyökkäyksen. (Yin, 2018)

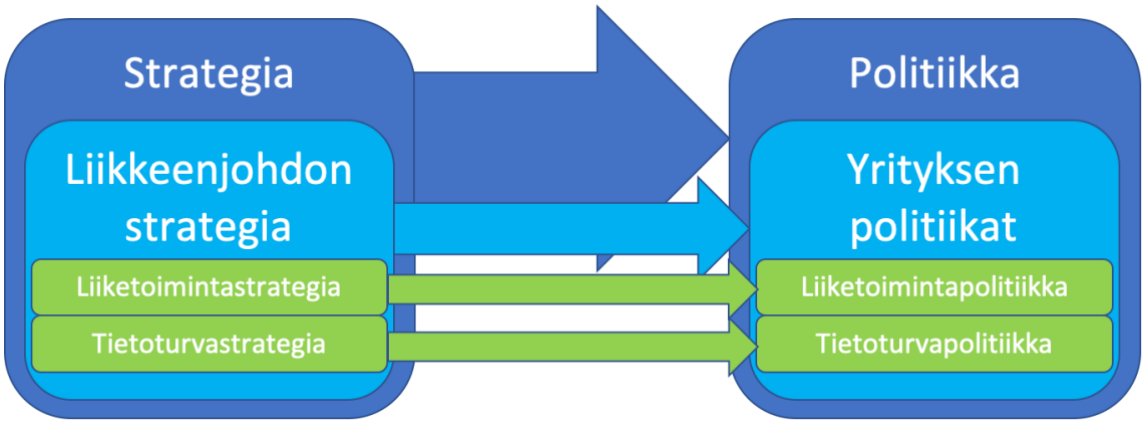
Tutkimuksen tulokset analysoitiin vertaamalla teoriaosuudessa selvinneitä tietoturvastrategian ja -politiikan yleistä rakennetta ja sisältöä viitekehyksenä käytetyn ISO27000-sarjan kautta kohdeorganisaatioiden tietoturvapolitiikkaan ennen kyberhyökkäystä ja sen jälkeen. Analyysin jälkeen arvioitiin, mitä tutkimuksen kohteissa olisi voitu tehdä toisin ja tulisi korjata sekä arvioitiin, miten muidenkin vastaavien organisaatioiden tietoturvallisuutta voitaisiin tutkia ja parantaa.

3 STRATEGIASTA POLITIIKKAAN

Tässä luvussa kuvataan käsitteet strategia, operaatiotaito, liiketoimintastrategia, tietoturvastrategia sekä -politiikka. Luvun tarkoituksena on taustoittaa tutkimuksen käsitteet ja ymmärtää niiden väliset suhteet. Lisäksi luvussa pyritään määrittelemään tietoturvaan liittyen, mikä on tyypillinen tietoturvastrategian ja -politiikan sisältö.

Tutkimuksen viitekehys ohjaa määrittämään käsitteet "strategia" ja "liikkeenjohdon strategia", jotta niistä liiketoiminnan kannalta seuraavat liiketoimintastrategia ja tietoturvastrategia voidaan määrittää. Samoin viitekehyksen täydentämiseksi on määritettävä käsitteet politiikka ja tietoturvapolitiikka, joista seuraa varsinaiset toimet tietoturvan tekemisellä. Tutkimuksen viitekehyksessä tietoturvastrategian johdannainen tietoturvapolitiikka seuraa tietoturvastrategian muodostamaa käsitemaailmaa, eli tietoturvapolitiikka on alisteinen tietoturvastrategialle.

Tietoturvastrategian määrittely on edelleen hieman epämääräinen ja tässä luvussa käsitteelle tarjotaan liiketoiminnan viitekehys, jossa tutkittua tapausta voidaan analysoida. Viitekehys on johdettu kirjasta "Information security: Policy, processes and practices" – Baskerville, Goodman, Straub (2008), jossa strategian muodostamisessa viitataan aiempaan tutkimukseen.



KUVIO 3 Strategian ja politiikan yhteys

3.1 Strategia ja liikkeenjohdon strategia

Strategian tehtävä on vastata kysymykseen miten. Se kertoo, mitä pitää tehdä, jotta yritys saavuttaa tavoitteensa ja visionsa." – Annika Tidström, Vaasan yliopiston yrittäjyyden professori, www.y-studio.fi, 5.4.2018.

Käsiteen "strategia" tunnettu kirjallinen historia ulottuu muun muassa Euroopassa kreikkalaiseen kirjallisuuteen, Lähi-Idän alueella Juutalaiseen Raamattuun ja Aasian alueella kiinalaiseen sotilas ja strategi Sunzi. Kreikkalaisessa kirjallisuudessa strategia perustuu filosofiseen pohdintaan ja

koostuu sotilaallisen voiman käyttämiseen älykkäästi. Raamatun käsite "strategia" viittaa usein alivoimaisen toimijan kykyyn voittaa älyn ja resurssien voimalla ylivoimainen vihollinen. (Freedman, 2013) Zunzi:n teos "Sodankäynnin taito" käsittelee strategiaa sodankäynnin kautta ja liittää siihen samoja käsitteitä kuin edeltävä: viisaus, tilanteen arviointi, resurssien suuntaaminen oikein ja vihollisen strategian lyöminen. (Fa, 2005)

"Strategia" yleiskäsitteenä tarkoittaa johtajan taitoa saavuttaa päämäärä. Koska käsitteen alkuperä on sotilaallinen, kyseessä on alun perin komentajan taito johtaa joukkojaan saavuttamaan haluttu päämäärä. Sotilaallisesti termi jaettiin kahteen termiin: Osataktiikka, josta tuli myöhemmin vain taktiikka sekä suurtaktiikka, josta tuli strategia. (Freedman, 2013) Sotataidon tutkimuksessa käsitteeseen strategia liitetään operaatiotaito, joka on komentajan kyky toteuttaa strategiaa. A.A. Svechin kirjassa "Strategia" operaatiotaito määritellään "kokonaisuus, joka on suunnattu yhteisen päämäärän saavuttamiseksi etukäteen määrätyssä aikataulussa". (Svechin, 1995)

Liiketoiminnan määritelmä on sellainen toiminta, jolla on ansiotarkoitus. (Kotimaisten kielten keskus, 2020) Mikäli ei tavoitella rahallista voittoa, voidaan pyrkiä saavuttamaan myös muuta lisäarvoa toimintaan, toiminnan kohteille tai välillisesti esimerkiksi yhteisölle. Kaupallista liiketoimintaa varten perustetaan yrityksiä ja voittoa tavoittelematonta liiketoimintaa varten julkisia organisaatioita ja yleishyödyllisiä järjestöjä. (Vuorinen, 2017)

Strategia-käsite on liitetty liiketoimintaan jo hyvin aikaisessa vaiheessa. Sunzi:n kirjan teksteistä jo johdettu analogiaa muun muassa torikaupankäyntiin. Strategisen ajattelun soveltaminen liike-elämään tapahtui laajamittaisesti 1950 ja 1960-luvuilla. Tuolloin sotilaallisen lähestymisen oppeja sovellettiin liiketoiminnan käytäntöön esikuvina muun muassa Aleksanteri suuri ja Napoleon. (Freedman, 2013) Strategia-sanan toinen liiketoimintaa sivuava merkitys on perusluontoinen toimintasuunnitelma. (Kotimaisten kielten keskus, 2020)

Tieteeseen perustuva liiketoimintastrategia eli taylorismi on syntynyt 1900-luvulle teollistumisen myötä. Sitä voidaan pitää suunnitteluun pohjautuvien strategioiden esiasteena ja mallina myöhemmin 1900-luvulla tuotettuihin liiketoiminnan johtamisen strategioihin. Ajattelun lähtökohta oli, että toiminta on suunniteltu tieteellisesti ennalta riittävän laajasti ja tavoitteellisesti, jotta työntekijöiden ei tarvitse sitä suunnitella. (Vuorinen, 2017) Taylorismin ensimmäisiä sovellutuksia olivat muun muassa Henry Fordin ajoneuvojen liukuhihnatuotanto.

Organisaatioiden osalta strategia kuvaa sitä, millä keinoilla organisaatio tuottaa arvoa omistajille, asiakkaille ja julkisissa organisaatioissa kansalaisille. Julkisen sektorin strategian onnistuminen on sen perustehtävän (mission) toteutumista. (Kaplan & Norton, 2004)

Toimijan strategian ja sen johdannaisten tulee olla toimijan liiketoimintafilosofian mukainen. Usein kuitenkin turvallisuus erottuu liiketoiminnasta omaksi kokonaisuudekseen ja toimii liiketoimintastrategian ulkopuolella. (Tufano, 2014)

3.2 Tietoturva, tietoturvallisuuden hallinta ja tietoturvastrategia

Tietoturvalla (engl. information security, data security) tarkoitetaan niitä menetelmiä ja keinoja, joilla taataan tiedon eheys, luotettavuus ja käytettävyys mukaan lukien fyysinen infrastruktuuri ja ohjelmistot sekä tiedon prosessointi, säilytys ja jakelu. Termin on korvannut termi kyberturva. (Paulsen & Byers, 2019) Kyberturvallisuus on käsite, jolla tarkoitetaan tässä yhteydessä kyberturvan ymmärtämistä, hallintaa, kontrollia ja riskien hallintaa osana toimijan kriittisen suorituskyvyn suunnittelua, käyttöä ja kehittämistä. Tämän ymmärtämiseksi toimijalla on oltava käsitys muun muassa toimijan kriittisistä resursseista ja/tai kriittisestä tiedosta, mitkä yrityksen osa-alueet tarvitsevat kriittistä tietoa toimiakseen ja mitkä uhat estävät näiden osa-alueiden toiminnan. (Cole;Krutz;& Conley, 2009)

Tietoturvallisuuden hallintaa tulisi rakentaa riskilähtöisesti ja prosessipohjaisesti, jolloin tietoturvan kehittäminen olisi määrätietoista ja jatkuvaa. Tietoturvan hallinta itsessään on prosessi, joka varmistaa, että tieto on oikein suojattu ja suojaus on kustannustehokasta. Tietoturvan rakentaminen tulisi perustua organisaation tietoturvatavoitteisiin ja siihen liittyvään tietoturvan riskiarviointiin. (Stallings & Brown, 2018)

Tietoturvastrategia kertoo, miten organisaation tavoitteisiin päästään. Tavoitteet tulevat joko organisaation liiketoimintastrategiasta tai voidaan muodostaa tietoturvallisuuden tavoitteita erikseen määrittämällä. Tietoturvastrategiaa tulee päivittää, jotta se vastaa sekä organisaation tavoitteita että toimintaympäristöä. (Stallings & Brown, 2018)

Suomessa tietoturva määritellään muun muassa julkishallinnossa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) toimesta. Tietoturva on tietojen, palveluiden, järjestelmien ja tietoliikenteen suojaamista, niihin kohdistuvien riskien hallintaa kaikissa tilanteissa hallinnollisilla, teknisillä ja muilla keinoilla. Tietoturvallisuus on tavoitteellista toimintaa, jolla taataan tiedon eheys, luottamuksellisuus ja käytettävyys ja taataan nämä eri tilanteissa. (Valtiovarainministeriö, 2007)

Tietoturvallisuuden hallinta on formaali menetelmä, jolla pyritään riittävästi turvaamaan organisaation kriittiset resurssit kustannustehokkaalla tavalla. (Stallings & Brown, 2018) Sen tulisi perustua turvallisuusstrategiaan ja ymmärrykseen organisaation tavoitteista yleisesti sekä tietoturvan osalta. (Stallings & Brown, 2018)& (Barton;Gurvirender;Lane;& Terrell, 2016) ISO27000-standardiperheessä tietoturvallisuuden hallinnoinnilla tarkoitetaan järjestelmää, jolla organisaation tietoturvatoimenpiteitä valvotaan ja hallitaan. (Suomen standardisoimisliitto SFS, 2020)

Tietoturvallisuuden hallintaan liittyy turvallisuuden arviointi, siihen liittyvien riskien kartoitus, arviointi sekä riskeihin reagointi, eli riskien hallinta. Riskien hallinnalla luodaan pohja tarvittavien ohjeiden ja toimenpiteiden

muodostamiseksi, jotta tietoturvaan liittyvät riskit ja niiden mahdolliset seuraukset voidaan hallita. Tietoturvallisuuden hallinnan edellytys on, että ymmärretään organisaatio, liiketoiminnan prosessit ja tarkoitus sekä tunnetaan käytössä oleva tietojärjestelmä. (Barton;Gurvirender;Lane;& Terrell, 2016) Tähän liittyvä kustannustietoisuus näkyy parhaiten strategisella tasolla. Myös tällä tasolla tulisi pohtia käytettyjen resurssien suhdetta saatavaan hyötyyn varsinaiselle liiketoiminnalle. Samalla tulisi laskea, mikä on kustannusten alin mahdollinen taso suhteessa suurimpaan mahdolliseen riskiin, joka toteutuessaan aiheuttaa suurimmat mahdolliset kustannukset. (Anderson & Choobineg, 2008)

Tietoturvallisuutta voidaan hallinta tietoturvallisuuden johtamis- ja hallintajärjestelmällä (ISMS information security management system), joka on ”osa yleistä toimintajärjestelmää, joka luodaan ja toteutetaan toimintariskien arviointiin perustuen ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus. Se sisältää organisaatiorakenteen, politiikat, suunnittelu- ja kehittämistoimenpiteet, vastuut, menettelytavat, menetelmät, prosessit, mittarit ja resurssit.” (Valtiovarainministeriö, 2008)

Tietoturvastrategia voidaan määritellä useilla eri tavoilla. Määrittelyyn vaikuttaa mm. lähestymistapa, joka voi olla esimerkiksi tavoite ja keino-, suunnitelma- tai prosessilähtöinen. (Horne;Ahmad;& Maynard, 2015) Tavoite ja keinolähtöinen malli on vahvasti sotilasstrategiaan viittaava malli, jossa toimijan tavoitteet ja niiden saavuttaminen ovat strategian ytimessä. Myös suunnitelmalähtöinen malli on vahvasti sotilastaustainen. ((Beeby & Rao, 2010) & (Park & Ruighaver, 2008)) Prosessilähtöinen lähestyminen nojautuu tietoturvan parantamiseen ja joidenkin tutkijoiden mukaan jatkuvuuden hallintaan. (Sveen;Torres;& Sarriegi, 2009)

Suomessa tietoturva rakennetaan tietoturvariskien tunnistamisen pohjalle ja tietoturvastrategia tulisi valtionhallinnon organisaatioissa rakentaa riskianalyysin pohjalta. Tietoturvastrategialla tarkoitetaan johdon linjausta siitä, mitkä ovat tietoturvan tavoitteet ja keinot, joilla näihin pyritään. Tietoturvastrategia rakentuu osaksi toimintastrategiaa, jolloin se voi olla osa sitä tai itsenäinen kokonaisuus. (Valtiovarainministeriö, 2007) Julkishallinnon lähestyminen on siis tavoite ja keinolähtöinen.

Tietoturvastrategian sisältöä ei ole tutkitussa materiaalissa erikseen määritelty. Tarkasteltaessa Suomen tietoturvastrategiaa 2016, sen keskeinen sisältö on:

- visio, joka määrittelee tietoturvan tilan määrittelemättömässä tulevaisuudessa
- tavoitteet ja niiden edistämiseksi tehtävät toimenpiteet
- perustelut strategisten linjausten taustalla. (Liikenne- ja viestintäministeriö, 2016)

Suomen kyberturvallisuusstrategiaa 2013 voidaan rinnastaa tietoturvastrategiaan. Sen keskeinen sisältö kattaa vision, johtamisen sekä toimintamallin ja varsinaiset strategiset linjaukset. Visiossa määritellään Suomen kyberturvallisuuden tilaa vuodelle 2016. Johtaminen ja toimintamalli kattavat keskeiset periaatteet, miten strategiaa toteutetaan. Strategiset linjaukset

sisältävät varsinaiset strategiset toimenpiteet sekä niiden resursoinnin. Tätä kyberturvallisuusstrategiaa on täydennetty toimenpideohjelmalla, jossa strategisia tavoitteita ja keinoja niihin pääsemiseksi tarkennetaan. (Valtioneuvosto, 2013) (Turvallisuuskomitea, 2014)

3.2.1 Kuntien strategiat

Suomessa kunnilla on kuntalain mukaan oltava strategia, jonka sisällön on kunnan valtuusto päättänyt ja kuntaa tulee johtaa hyväksytyn strategian mukaisesti. Strategian tulee kattaa kunnan pitkän toiminnan ja talouden pitkän aikavälin tavoitteet. Strategiassa on otettava huomioon seuraavat asiat:

1. kunnan asukkaiden hyvinvoinnin edistäminen;
2. palvelujen järjestäminen ja tuottaminen;
3. kunnan tehtäviä koskevissa laeissa säädetyt palvelutavoitteet;
4. omistajapolitiikka;
5. henkilöstöpolitiikka;
6. kunnan asukkaiden osallistumis- ja vaikuttamismahdollisuudet;
7. elinympäristön ja alueen elinvoiman kehittäminen. (Kuntalaki, 2015)

Kunnan strategian tulee perustua arvioon nykytilanteesta, arvioon siihen kohdistuvista muutoksista sekä niiden vaikutuksista kunnan tehtäviin. Lisäksi strategia tulee ottaa kantaa strategian toteutumisen mittaamiseen ja arviointiin. (Kuntalaki, 2015)

Tutkimuksessa käytetyssä lainsäädännöstä tai muusta materiaalista ei löydy vaatimusta tietoturvastrategian muodostamisesta kunnissa. On todennäköistä, ettei sellaista ole määritetty Suomessa.

3.3 Politiikka ja tietoturvapolitiikka

Määritelmässä politiikka tarkoittaa muun muassa toimintalinjaa tietyllä kohdealueella, kuten tietoturvassa (tietoturvapolitiikka). Sisältää yleisesti toimintatapoja ja reunaehtoja toiminnalle, mutta ei usein kerro tarkkaan toiminnan yksityiskohtaista sisältöä. (Kotimaisten kielten keskus, 2020) Politiikka voi myös tarkoittaa käytäntöä, jolloin se on esimerkiksi yksityiskohtainen sääntö tai rajaus. (Stallings & Brown, 2018)

Suomessa valtionhallinnossa käytettävä tietoturvapolitiikan määritelmä löytyy VAHTI-ohjeesta 8/2008 ”Valtionhallinnon tietoturvasanasto”. Määritelmä kuuluu: ” 1) valtakunnan tasolla tietoturvanormien ja niiden täytäntöönpanon muodostama kokonaisuus, 2) organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Voidaan puhua myös tietoturvaperiaatteista. Tietoturvapolitiikka ja -strategia ovat osa organisaation toiminta- ja tietohallintopolitiikkaa ja -strategiaa.” (Valtiovarainministeriö, 2008)

Tietoturvapolitiikka voi olla organisaatiossa oma itsenäinen politiikka tai osa yrityksen laajempaa politiikkaa organisaation johtamiseksi. Siinä missä tietoturvastrategia kertoo, miten organisaation tavoitteisiin päästään, politiikka

kertoo mitä pitää tehdä. Politiikkaa tulee päivittää säännöllisesti vastaamaan toimintaympäristö ja siinä tapahtuvia muutoksia. Sen tulee myös olla toimijan ylimmän johdon hyväksymä ja tukema. (Stallings & Brown, 2018)

Tietoturvapolitiikka muodostetaan organisaation strategian pohjalta. Politiikka voidaan koostaa yhdeksi asiakirjaksi tai se voidaan pilkkoa osiksi. Politiikan tulisi sisältää tai vastata seuraaviin kokonaisuuksiin:

- sisältää politiikan tarkoitus
- olla suhteessa organisaation tavoitteisiin, voimassa oleviin lakeihin ja säädöksiin
- vastata tietoturvallisuuden peruskäsitteistöön
- ohjata vastuut organisaation sisällä
- noudattaa organisaatioon valittua riskienhallinnan menetelmää
- ottaa kantaa tietoturvallisuuden koulutukseen
- määrittää tietoturvan kannalta tärkeimmät roolit
- määrittää mahdolliset sanktiot ja niiden soveltaminen
- määrittää tietoturvan integraatio kehitykseen sekä hankintoihin
- määrittää tietoturvallisuuden merkinnät ja niiden käyttö
- muodostaa yhteys toiminnan jatkuvuuteen
- muodostaa tietoturvapoikkeaminen havainnoinnin menetelmät sekä ilmoittamiskäytännöt
- politiikan tarkastaminen ja sen määräajat
- tietoturvapolitiikan päivittäminen ja sen seuranta. (Stallings & Brown, 2018)

Tietoturvapolitiikka tulisi olla hajautettu läpi toimijan organisaation, mutta useimmat tietoturvan hallintajärjestelmät tukevat ajatusta, että organisaatiossa on yksi nimetty tietoturvallisuudesta vastaava henkilö, jolla on riittävä koulutus ja osaaminen tehtävän hoitamiseksi. (Stallings & Brown, 2018)

Tutkimuksen viitekehyksen ISO27001-standardin mukaan tietoturvapolitikka on toimijan ylimmän johdon laatima kirjallinen ja kaikille organisaatiossa työskenteleville sekä sidosryhmille saatavissa oleva asiakirja. Se sisältää seuraavat kokonaisuudet tai täyttää seuraavat vaatimukset:

- soveltuu toimijan toiminta-ajatukseen tai strategiaan
- sisältää tavoitteet tai muodostaa pohjan tavoitteiden asettamiselle
- sisältää organisaation sitoutumisen tavoitteiden saavuttamiseksi
- sisältää sitoumuksen tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen. (Suomen standardisoimisliitto SFS, 2017)

Tietoturvapolitiikan tulisi sisältää tietoturvallisuuden tavoitteet. ISO27001 määrittelee, että tietoturvatavoitteiden tulisi täyttää nämä vaatimukset:

- tavoitteiden tulisi olla tietoturvapolitiikan mukaiset
- tavoitteet tulisi asettaa niin, että niitä voidaan mitata
- tavoitteet ottavat huomioon niihin soveltuvat tietoturvavaatimukset sekä riskienhallintaprosessin tulokset
- tavoitteista on pystyttävä viestimään
- tavoitteet tulisi olla päivitettävissä. (Suomen standardisoimisliitto SFS, 2017)

Tavoitteiden osalta tulisi määrittää jokaisen tavoitteen osalta seuraavat asiat:

- mitä on tarkoitus tehdä
- millä resursseilla työ tehdään
- kuka tai ketkä ovat työstä vastuussa
- milloin tavoite tulisi olla saavutettu
- kuinka tavoitteen saavuttamista mitataan. (Suomen standardisoimisliitto SFS, 2017)

Valtionhallinnossa tietoturvallisuus tulee olla ministeriön, viraston tai laitoksen ylimmän johdon hyväksymä. Se vahvistaa organisaation turvallisuus- ja varautumisperiaatteet sekä määrittelee turvallisuutta toteuttavan organisaation. Turvallisuuden toteutumisesta vastataan tulosjohtamisen periaatteiden mukaisesti ja siitä vastaa tulosyksikkö ja sen päällikkö. Turvallisuuden toimintaperiaatteisiin pitää sisältyä tavoitteet ja menettelytavat. (Valtiovarainministeriö, 2007)

Tietoturvallisuuden osalta valtionhallinnon laitosten pitää turvata sen päätehtävät ja määriteltävä sen turvaamiseksi tietoturvapolitiikka. (Valtiovarainministeriö, 2004)

Valtionhallinnon tietoturvapolitiikalle on määritelty esimerkkirakenne VAHTI-ohjeessa 04/2007. Rakenne on seuraava:

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. (Valtiovarainministeriö, 2007)

Samassa asiakirjassa on myös mallipohjat tietoturvallisuuden kehittämiseksi, keskeisten periaatteiden ja käytäntöjen määrittämiseen, valmiussuunnitelmaan, jatkuvuuden hallintaan ja palautumiseen.

3.4 Johtopäätökset

Tässä tutkimuksessa strategia ymmärretään toimijan työtä ohjaavana ja kokoavana kattokäsitteenä ja sen tehtävän on resurssien kohdentaminen tavoitteen saavuttamiseksi. Toimijalla on siitä kirjallinen muoto ja toiminnan johto on sitoutunut toteuttamaan strategiaa. Toimijan päästrategia ohjaa siitä muodostettuja sille alisteisia strategioita sekä toimijan tehtävien suorittamiseksi laadittua politiikkaa.

Tietoturvastrategia on organisaatiossa tyypillisesti liiketoimintastrategiaa tukeva strategia, joka voi sisältyä osaksi varsinaista liiketoimintastrategiaa tai olla oma itsenäinen strategia. Tietoturvastrategia määrittelee osastrategiana, miten tietoturvallisuus toteutetaan. Varsinaista määritelmää tietoturvastrategialle ei ole vakiintunut.

Tietoturvastrategiassa olennaista on, että se on muodostettu riskienhallintaprosessin pohjalta ja tämä tulee esille kaikissa lähteissä. Lisäksi tietoturvastrategian tulisi olla varsinaisen liiketoimintastrategian mukainen eikä erillinen liiketoiminnasta irtonainen kokonaisuus. Tietoturvastrategian sisällölle ei erikseen löytynyt määritelmää, joten sisällön voidaan olettaa kattavan vision, strategian tavoitteet ja niiden reunaehdot sekä resurssit tavoitteiden saavuttamiseksi.

Tutkitusta materiaalista ei löydy varsinaisen kuntastrategian lisäksi muita osastrategioita, joita kuntien tulisi lainsäädännön pohjalta muodostaa toiminnan ohjaamiseksi. Tietoturvastrategia ei siis ole pakollinen kunnan toimintaa ohjaava osastrategia. Toisaalta kuntalaki ei kiellä osastrategioiden tekemistä.

Tässä tutkimuksessa politiikka ymmärretään toimijan strategiaa täsmällisempänä ohjauksena strategian toteuttamiseksi, joskaan politiikka ei usein ole tarkka kuvaus siitä, miten tavoite saavutetaan. Politiikka voidaan myös ymmärtää käytäntöä, jolloin se määrittelee tarkkaan jonkin asian toteuttamisen ja sen reunaehdot.

Tietoturvapolitiikka tulee olla toimijan johdon hyväksymä, ylläpidetty ja organisaation ja sen sidosryhmien saatavilla oleva dokumentoitu kokonaisuus. Politiikan toteuttamiseksi ja ylläpitämiseksi tulisi organisaatiossa olla määritelty taho, jonka tehtäviin se kuuluu.

Tietoturvapolitiikka tarkentaa tietoturvastrategiaa. Tutkitussa materiaalissa ei kuitenkaan löydy viittausta, että tietoturvapolitiikan muodostamisen edellytyksenä olisi tietoturvastrategia. Materiaalin perusteella voidaan kuitenkin olettaa, että tietoturvapolitiikka perustuu vähintään löyhästi organisaation toiminnan päästrategiaan eli mahdollistaa sen toteutumisen, palautumisen ja jatkuvuuden.

Tietoturvapolitiikan sisältöä on määritelty sekä viitekehyksen ISO27000-sarjassa että VAHTI-ohjeissa varsin tarkasti. Näiden pohjalta voidaan tutkimukseen muodostaa tietoturvapolitiikan rakenne sekä sisältö verrattavaksi tapaustutkimuksen kohteiden voimassaolleisiin vastaaviin dokumentteihin.

4 JULKISEN HALLINNON MÄÄRÄYKSET JA OHJEET SEKÄ TIETOTURVALLISUUDEN HALLINNON JÄRJESTÄMINEN

Julkisen hallinnon tietoturvallisuuden kehittymistä ohjaavat lait, asetukset ja tietoturvaan liittyvät ohjeet ja suositukset, kuten VAHTI-ohjeet. Tässä luvussa käsitellään näistä tutkimuksen kannalta olennaisimpia kansallisia ohjausasiakirjoja, asetuksia, lakeja ja ohjeita, niissä käskettyjä tietoturvaan liittyviä kokonaisuuksia sekä tietoturvatyön resursointia. Ne on valittu sen perusteella, että niissä käsketään suoraan tietoturvaan liittyviä asioita julkisille organisaatioille. Käsittelyn ulkopuolelle on jätetty kansainvälinen lainsäädäntö, jonka vaikutukset kunnallisen tason tietoturvan käytännön toteuttamiseen ovat rajalliset. Lisäksi tarkastelun ulkopuolelle on jätetty asetuksia ja määräyksiä, joilla ei ole tutkittujen tapausten tietoturvan kannalta olennaista vaikutusta. Tarkasteltavien kokonaisuuksien valinnassa on otettu huomioon, ettei tutkimuksen tarkoituksena ole listata yksittäisiä asioita, joilla tutkimuksen kohteet olisivat voineet parantaa tietoturvaansa kyberhyökkäyksiin liittyen. Tutkimuksen tarkoitus on selvittää ohjaus, jota noudattamalla kyberhyökkäysten torjunta olisi voinut onnistua ja onnistuneesta hyökkäyksestä palautuminen olisi voinut olla nopeampaa tietoturvastrategiassa ja -politiikassa.

Tässä tutkimuksessa keskitytään tietoturvan tarkasteluun tietoturvastrategian ja -politiikan sekä toimijaa vastaan tehdyn kyberhyökkäyksen näkökulmasta, joten tarkastelu kohdistetaan kuntiin kohdistuvaan ohjaukseen. Kaupunki on yksi kunnan muoto, joten lakia sovelletaan myös niihin. (Kuntalaki, 2015)

Tämän luvun tarkoituksena on luoda käsitys voimassa olevasta lainsäädännöstä, ohjeista ja oppaista kokonaisuutena ja luoda käsitys, mitä kunnissa tulisi noudattaa tietoturvallisuustyön tekemisessä. Tämän lisäksi arvioidaan kuntien mahdollisuuksia ymmärtää olemassa olevaa ohjeistusta ja hyödyntää sitä tietoturvatyössä.

4.1 Kunnallinen tietoturvallisuuden järjestäminen

Yhdysvalloissa tietoturvallisuus voidaan valtionhallinnossa järjestää kahdella tavalla: keskitetysti tai organisaation sisällä hajautetusti. Keskitetyssä mallissa tietoturvallisuudesta vastaava henkilöstöresurssi, päätöksenteko ja vastuu sijoitetaan yhdeksi kokonaisuudeksi mukaan lukien sisäinen raportointi ja kehittäminen. Hajautetussa mallissa organisaatiossa voi olla koko organisaation tietoturvan johtaja, mutta muu resurssi sekä päätöksenteko on hajautettu organisaatio sisälle. Kummankin ääripään sovellutukset ovat harvinaisia. Valitun toteutustavan osalta keskeisiä tekijöitä ovat hallinnon koko, organisaation tehtävä, olemassa olevat resurssit, hallinnolliset ja

lainsäädännölliset vaatimukset, budjetti, tietoturvaa toteuttavien tahojen määrä, organisaation koko ja sijainti sekä muun organisaation päätöksentekotapa sekä hallinto. (Bowen;Hash;& Wilson, 2006)

Suomessa kuntien tietoturvan järjestäytymistä ei ohjata lailla. Kuntalaki 2015 (410/2015) tai tiedonhallintalaki 2019 (906/2019) eivät nimeä kuntien käyttöön erillistä tietoturvaan tai hallintoon käskettyä tahoa tai organisaatiota. Jokaisen kunnan osalta kuntakohtainen hallintosääntö määrittää kunnan toiminnan organisoitumisen ja tätä kautta tietoturvaorganisaation rakenteen sekä tehtävät. (Kuntalaki, 2015)

Julkisten organisaatioiden toiminnassa on kuitenkin havaittu kehittämistarpeita (Valtiovarainministeriö, 2020), joihin on reagoitu julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa 2020–2023 kohdassa 3.1 ” Kuntien käytössä olevien tietoverkkojen turvallisuus” ja 3.2 ”Kuntien yhteiset digitaalisen turvallisuuden palvelut”. Nämä ovat osa julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmaa (JUDO), jota toteuttaa JUDO-hanke. Kuntien tietoturvallisuuden organisointiin liittyen yksi hankkeen tavoitteista on yhteisten asiantuntijapalveluiden tuottaminen kunnille. (Digi- ja väestötietovirasto, 2020)

4.2 Kansallinen ohjaus

Suomessa kansallinen ohjaus on jakautunut Valtiovarainnimisteriölle, Liikenne- ja viestintäministeriölle, Ulkoministeriölle, Sisäministeriölle, Puolustusministeriölle ja valtioneuvoston kanslialle. Sisäisinä toimijoina tunnistetaan myös Digi- ja väestötietovirasto, Traficom, Kyberturvallisuuskeskus, Valtori ja Huoltovarmuuskeskus. Kehittämiseen liittyen edellä mainittujen lisäksi osallistuu turvallisuuskomitea. (Valtiovarainministeriö, 2020)

Kansallisesti on laadittu tietoturvaa ohjaavia kokonaisuuksia lakien ja asetusten lisäksi:

- Yhteiskunnan turvallisuusstrategia (YTS) – valtioneuvoston periaatepäätös 2016
    - edeltänyt vastaavat strategiat 2003, 2006 ja 2010
- Kyberturvallisuusstrategia 2019 – turvallisuuskomitea
    - edeltänyt Kyberturvallisuusstrategia 2013
- Julkisen hallinnon digitaalisen turvallisuuden ohjelma JUDO 2019
    - Sisältää JUDO-hankkeen, joka toteuttaa ohjelmaa
- Julkisen hallinnon digitaalinen turvallisuus – valtioneuvoston periaatepäätös 2020.

YTS julkaistiin neljännen kerran 2016 ja sitä on edeltänyt vastaavat julkaisut 2003, 2006 ja 2010, joista kaksi ensimmäistä nimellä ”Yhteiskunnan elintärkeiden toimintojen turvaaminen”. YTS on tunnistanut digitaalisen toimintaympäristön häiriöt riskiksi johtamiselle 2003 ja määrittänyt sähköisen viestinnän kehittämiskohteeksi. (Valtioneuvosto, 2003) Vuonna 2006 siihen lisättiin kuntien

keskeinen rooli peruspalveluiden ja elintärkeiden toimintojen järjestämisessä. Samalla tietojärjestelmiin kohdistuvia uhkia kuvataan laajemmin. (Valtioneuvosto, 2006)

Vuonna 2010 julkaistussa turvallisuusstrategiassa kuntien merkitystä korostetaan kahta edellistä enemmän toteamalla sivulla 6: ” Kuntien rooli yhteiskunnan varautumisessa ja häiriötilanteiden hallinnassa on paikallishallinnossa keskeinen, koska peruspalveluiden ja muiden yhteiskunnan elintärkeiden toimintojen järjestäminen on merkittäviltä osiltaan kuntien vastuulla. Kuntien varautumisvelvoite poikkeusoloihin perustuu valmiuslakiin mutta erityisesti normaaliolojen turvallisuuden, ja normaaliolojen häiriötilanteiden hallinta edellyttävät kuntien varautumisen kehittämistä” Julkaisu myös ottaa kantaa kuntien palveluiden ulkoistamiseen ja kuntien rooliin ulkoisten palveluntarjoajien roolien muodostamisessa ja vastuiden selkeyttämisessä. (Valtioneuvosto, 2010)

Vuoden 2017 YTS ei muuta aiempien julkaisujen keskeisiä linjauksia, mutta korostaa entisestään varautumisen merkitystä uhkien sietämisessä. (Valtioneuvosto, 2017)

Kyberturvallisuusstrategia on julkaistu vuosina 2013 ja 2019 Turvallisuuskomitean toimesta. Kyberturvallisuusstrategian tehtävä on toimia Yhteiskunnan turvallisuusstrategian toimeenpanon osana. Se kuvaa kyberturvallisuuden vision ja toimintamallin strategiset linjaukset. (Valtioneuvosto, 2013)

Kyberturvallisuusstrategia 2013 määrittelee 10 keskeistä strategista tehtävää, joilla kyberturvallisuutta parannetaan kansallisesti. Niistä seuraavat kohdat koskevat osin kuntien varautumista:

- kohta 1: ” Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.”
- Kohta 7: ” Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.”
- Kohta 8: ” Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.”
- Kohta 9: ” Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.”

Kyberturvallisuusstrategia 2019 poikkeaa edellisestä sekä rakenteellisesti että sisällöllisesti. Siinä tiivistetään strategiset tavoitteet kolmeen pääkohtaan. Kuntien tehtäviä ei käsitellä erikseen, mutta kaikki kolme kohtaa voidaan päätellä johtavan kuntien kyberpoikkeamien sietoisuuden kasvuun. (Valtioneuvosto, 2019)

Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma JUDO on julkaistu vuonna joulukuussa 2018 ja sen varsinainen toimenpidesuunnitelma vuosille 2018–2021 ja sen jatko-ohjelma ”HAUKKA”, joka kattaa vuodet 2020–2023. (Valtiovarainministeriö, 2020) Kehittämisohjelma on tehty kattamaan koko

julkinen hallinto ja se ottaa huomioon kunnat. Kehittämisohjelma on valinnut kolme keskeistä kehittämisaluetta kehitettäväksi:

1. Digitaalisen turvallisuuden ja johtamisen kehittäminen
2. Osaava henkilöstö
3. Uuden teknologian tehokas hyödyntäminen palveluiden ja digiturvallisuuden toteuttamisessa. (Valtiovarainministeriö, 2018)

Varsinainen toimenpidesuunnitelma on jaettu 5 toimenpiteeseen, joista kaikki koskevat myös kuntatasolla eri päättäjiä. Nämä ovat:

1. Digitaalisen turvallisuuden johtamisen ja riskienhallinnan kehittäminen
2. Digitaalisen turvallisuuden soveltamis- ja arviointikehikon toteuttaminen
3. Julkisen hallinnon digitaalisen turvallisuuden koulutusjärjestelmä sekä digiturvasovellus
4. Julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan raportoinnin kehittäminen
5. Digitaalisen turvallisuuden harjoitusohjelma ja sen toteuttaminen vuosina 2018–2021.

Kaikki ohjelman toimenpiteet vaikuttavat eri toimijoihin kuntatasolla ja niiden toteuttaminen on aloitettu 1/2019 alkaen. (Valtiovarainministeriö, 2018)

4.3 Julkisia toimijoita ohjaavat tietoturvaan liittyvät lait ja asetukset

Kuntien tietoturvaan tai tietosuojaan liittyviä lakeja ja asetuksia on paljon. VAHTI-ohje 4/2007 määrittää liitteessä 4 52 erilaista lakia, asetusta ja päätöstä, joissa käsitellään tietoturvallisuutta. Tutkituissa tietoturvapolitiikoissa vain Virtain kaupunki on tehnyt niistä yksityiskohtaisen luettelon. Siihen kuuluu:

- Perustuslaki (731/1999)
- Kuntalaki (410/2015)
- Hallintolaki (434/2003)
- Arkistolaki (831/1994)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki viranomaisen toiminnan julkisuudesta (621/1999)
- Henkilötietolaki (523/1999)
- Euroopan unionin yleinen tietosuoja-asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (EU 679/2016)
- Euroopan parlamentin ja neuvoston direktiivi, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai

rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta (EU 680/2016)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (617/2009)
- Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista (661/2009)
- Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)
- Laki julkisista hankinnoista ja käyttöoikeussopimuksista (1397/2016)
- Rikoslaki (39/1889)
- Työsopimuslaki (55/2001)
- Valmiuslaki (1552/2011)
- Tietoyhteiskuntakaari (917/2014)
- Tekijänoikeuslaki (404/1961)
- Lukiolaki (629/1998)
- Perusopetuslaki (628/1998)
- Oppilas- ja opiskelijahuoltolaki (1287/2013)
- Kansanterveyslaki (66/1972)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)
- Laki sosiaali- ja terveydenhuollon palvelusetelistä (569/2009)
- Laki sähköisestä lääkemääräyksestä (61/2007)
- Laki terveydenhuollon ammattihenkilöstä (559/1994)
- Sosiaalihuoltolaki (1301/2014), sosiaalihuoltolain (710/1982) 2 luku, 25, 26, 26 a, 27 d, 27 e ja 40 § sekä 5 ja 8 luku jäävät voimaan
- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista (298/2009)
- Terveydenhuoltolaki (1326/2010). (Virtain kaupunki, 2018)

Huomioitavaa on, että Virtain kaupungin luettelosta puuttuu ainakin seuraavia kokonaisuuksia:

- Laki julkisen hallinnon tiedonhallinnasta (906/2019)
- edeltänyt Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)
- Lakia 906/2019 on täydennetty Valtioneuvoston asetuksella asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)
- Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)
- Laki tietoturvallisuuden arviointilaitoksista (1405/2011)
- Laki digitaalisten palveluiden tarjoamisesta (306/2019)
- Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 571/2016.

Ensimmäinen ja toinen on julkaistu vasta Virtain kaupungin tietoturvastrategian jälkeen, joten sitä ei ole huomioitu listauksessa. Asetus tietoturvallisuudesta valtionhallinnossa (681/2010) olisi sen sijaan pitänyt kuulua listaukseen. Asetusta 681/2010 ja lakia 906/2019 käsitellään luvussa 3.3.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuuden arvioinnista olisi voitu ottaa huomioon Virtain kaupungin listauksessa. Se koskee kuitenkin tietoturvastrategiatason ohjausta, jolloin politiikkatasolla sen huomiointi olisi vaatinut esimerkiksi kansallisen turvallisuusauditointikriteeristön vaatimusten luettelointia toimenpiteitä varten.

Laki tietoturvallisuuden arviointilaitoksista liittyy samoin tietoturvastrategian muodostamiseen ja sen arviointiin. Politiikkatasolla laki olisi voitu huomioida valitsemassa soveltuva auditoinnin toteuttava yritys toteuttamaan tietoturvan auditointi.

Laki digitaalisten palveluiden tarjoamisesta (306/2019) on suunnattu edistämään viranomaisten palveluiden tarjoamista yhdenvertaisesti kaikille ja parantamaan palveluiden saatavuuden lisäksi laatua ja tietoturvaa. Laki koskee myös kuntia. Laki velvoittaa kuntia suunnittelemaan ja ylläpitämään palvelunsa huomioiden tietoturva ja tietosuoja sekä löydettävyys ja helppokäyttöisyys. Laki viittaa myös aluehallintoviraston ylläpitämään ”Digi kuuluu kaikille”-sivustoon, jossa ylläpidetään digitaalisten palveluiden saavutettavuuden toteutumisen vaatimuksia, saavutettavuusselosteita sekä palvelua, jossa voi ilmoittaa ongelmia digitaalisissa palveluissa.

Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista (571/2016) edistää samoja asioita, kuin edellä kuvattu laki digitaalisten palveluiden tarjoamisesta, mutta kohdistuu sähköisen asioinnin tukipalveluihin. Tällaisia palveluita ovat tietoa tai tietovirtoja kokoavat palvelut ja niiden sisältöä esittävät palvelut, tunnistukseen liittyvät palvelut, asiointivaltuutuspalvelut, viestintäpalvelut, maksupalvelut ja karttapalvelut.

4.4 Asetus tietoturvallisuudesta valtionhallinnossa

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) koskee pääosin asiakirjaturvallisuutta ja asetus on kumottu lailla 906/2019 1.1.2020. Kumoutunut asetus koskee kuitenkin kaikki julkisia toimijoita ja on ollut voimassa tutkimukseen valittujen kyberhyökkäysten aikaan.

Lain tarkoituksena on ohjata tietoturvan toteuttamista julkisessa hallinnossa. Määrällisesti asetus käsittelee eniten asiakirjaturvallisuutta, mutta alkuosassa se käskee keskeisiä periaatteita tietoturvan toteuttamiseksi. Pykälässä 4 annetaan tietoturvan toteuttamisen suunnittelun perusteet, jotka ovat:

- selvitykset ja arviot olemassa olevista asiakirjoista
- tallennetun tiedon merkitys
- hyvät julkisuus- ja salassapitoperusteet tietojärjestelmien toteutuksessa

- oikeat tietoturvatoimenpiteiden mitoitus käsiteltävän tiedon merkityksen ja käyttötarkoituksen mukaisesti
- asiakirjoihin ja tietojärjestelmiin kohdistuvat uhat
- tietoturvallisuuden kustannukset.

Tässä asetuksessa 681/2010 todetaan pykälässä 5, että viranomaisen on huolehdittava seuraavista asioista tietoturvaan liittyen:

1. viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan;
2. viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3. asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4. tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5. asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6. tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7. asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8. henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
9. henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10. annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Lisäksi asetuksen pykälässä 6 velvoitetaan suunnittelemaan asiakirjojen turvallisuus koko niiden elinkaaren ajan. (Valtioneuvosto, 2010)

4.4.1 Laki julkisen hallinnon tiedonhallinnasta 906/2019

Laki julkisen hallinnon tiedonhallinnasta tai tiedonhallintolain (Eduskunta, 2019) viimeisin päivitys astui voimaan 1.1.2020, eli tutkittujen kyberhyökkäysten jälkeen. Tätä lakia ei ole sisällytetty muun muassa Virtain kaupungin tietoturvapolitiikkaan, joka on muodostettu ennen lain voimaantuloa. 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. (Eduskunta, 2019)

Laki jakaa vastuun tiedonhallintayksiköille, joita ovat muun muassa kunnat. Lisäksi lain lukua 3 sovelletaan kuntiin ja kuntayhtymiin.

Laki määrittää, että tietohallintoyksikön pitää muun muassa määrittää tiedonhallinnon vastuut sekä ajantasaiset ohjeet, joihin kuuluu tietoaineiston käsittely, tietojärjestelmien käyttö, tiedonkäsittelyoikeudet, tietohallinnon vastuun toteuttaminen, tiedonsaantioikeuksien toteuttaminen, tietoturvatoimenpiteet ja poikkeusoloihin varautuminen. Laki ei suoraan käske tiedonhallintayksiköitä muodostamaan tietoturvastrategiaa tai -politiikkaa. (Eduskunta, 2019)

4.5 Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta

Oikeusministeriö on julkaissut asetuksen viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta 21.11.1999. (Oikeusministeriö, 1999) Osaa asetuksesta on muutettu 1.7.2010 asetuksella 681 ja 1101/2019. Muutokset koskevat muun muassa asiakirjojen merkintää ja luokitellun tiedon käsittelyä. Asetus tarkentaa sen asettamisen aikaan voimassa ollutta julkisuuslakia 621/1999 ja arkistolakia 831/1994.

Asetuksen tarkoituksena on kuvata ne toimenpiteet, joita viranomaisen on tehtävä yleisesti toiminnan julkisuuteen ja hyvään tiedonhallintotapaan liittyen. Tietojärjestelmiin liittyen laki velvoittaa tiedon käsittelyä suunniteltaessa huomioimaan miten seuraavat asiat toteutetaan:

1. oikeus saada tietoja viranomaisten julkisista asiakirjoista;
2. velvollisuus tuottaa ja jakaa tietoja sekä antaa tietoja keskeneräisistä asioista;
3. henkilötietojen, erityisesti arkaluonteisten tietojen, suojaaminen;
4. salassa pidettäviksi säädettyjen tietojen suojaaminen;
5. tietojen käyttötarkoituksia koskevat rajoitukset;
6. tietojen käytettävyys, eheys ja laatu viranomaisen tehtävän hoidossa ja viranomaisten yhteistyössä;
7. tietojen laatu erityisesti käytettäessä niitä yksilöitä ja yhteisöjä koskevan päätöksenteon pohjana tai oikeuksien ja velvollisuuksien osoittajina.

Asetus mainitsee luvun 1 pykälässä 1, että julkisen toimijan on tietoturvallisuuteen liittyen otettava huomioon toimenpiteet uhkien määrittämiseksi, niiden vähentämiseksi ja poistamiseksi sekä näistä toimenpiteistä aiheutuvat kustannukset ja vaikutukset. Lisäksi luvun 1 pykälässä

2 esitetään vaatimukset asiakirjojen käsittelyoikeuksien rajoittamiseen myös tietojärjestelmissä ja luvussa 2 pykälässä 5 käsky muodostaa ja ylläpitää rekisteriä muodostetuista asiakirjoista sekä niitä yhdistävistä asioista. Lisäksi varsinaisesta rekisteristä pitää pystyä seuraamaan asiakirjan tilaa, eli käsittelyn vaihe kuten asian vireille saattaminen.

Kuntien toiminnan kannalta merkittävä on luvun 2 pykälä 8, jossa käsketään ylläpitämään tietojärjestelmistä seloste. Selosteen tulee sisältää tietojärjestelmän käyttötarkoitus ja siihen tallennettavan tiedon kuvaus. Luvun 3 pykälässä 10 käsketty selosteiden muodostamiseksi määräaika on ollut 30.11.2000 ja ennen 1.12.1999 käyttöönotettujen tietojärjestelmien tietoturvallisuusjärjestelyt ja ohjeet on saatettava lain edellyttämään tasoon 30.11.2004 mennessä. (Oikeusministeriö, 1999)

4.6 Kuntalaki 410/2015

Kuntalaki (Kuntalaki, 2015) 37§ käskee kuntaa muodostamaan kuntastrategian, jonka perusteella kuntaa johdetaan. Sen hyväksyy kunnan valtuusto ja sitä toteuttaa kunnan hallitus. Kuntastrategia pitää sisällään seuraavat kokonaisuudet:

1. kunnan asukkaiden hyvinvoinnin edistäminen;
2. palvelujen järjestäminen ja tuottaminen;
3. kunnan tehtäviä koskevissa laeissa säädetyt palvelutavoitteet;
4. omistajapolitiikka;
5. henkilöstöpolitiikka;
6. kunnan asukkaiden osallistumis- ja vaikuttamismahdollisuudet;
7. elinympäristön ja alueen elinvoiman kehittäminen.

Kunnan strategian tulee perustua arvioon nykytilanteesta, Arvioon siihen kohdistuvista muutoksista sekä niiden vaikutuksista kunnan tehtäviin. Lisäksi strategia tulee ottaa kantaa strategian toteutumisen mittaamiseen ja arviointiin. (Kuntalaki, 2015)

Kuntalaki ei määrää kuntaa tekemään erikseen muita strategioita, mutta se ei myöskään estä niiden tekemistä. Se ei myöskään käske tekemään kunnalle tietoturvapolitiikkaa, mutta käskee 98§:ssa, että sähköisissä kokouksissa ja päätöksentekomenettelyssä kunnan tulee huolehtia tietoturvallisuudesta ja siitä, ettei salassa pidettävät tiedot ole ulkopuolisten saatavissa.

Kuntalaki mahdollistaa toiminnan järjestämisen itse, ulkoistamalla tai yhteistoiminnassa muiden kuntien kanssa. Ulkoistamisessa tai yhteistoiminnassa toiminnan tulee perustua sopimuksiin. Kuntien välinen yhteistyö kattaa myös viranomaistehtävien hoitamisen. (Kuntalaki, 2015)

4.7 SuomiDigi-sivusto

Digi- ja väestövirasto ylläpitää SuomiDigi-sivustoa, joka on tarkoitettu julkiselle sektorille digitaalisten palveluiden kehittämisen, tuottamisen ja päätöksen teon tukemiseksi. Sivusto on kuitenkin julkinen ja avoin, joten sitä voi hyödyntää laajemmin. Sivusto sisältää ajankohtaisten artikkeleiden ja uutisten lisäksi digitalisaatioon liittyvää lainsäädäntöä, julkisen hallinnon suosituksia (JHS) sekä valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeita ja suosituksia. (Digi- ja väestövirasto, 2021)

4.7.1 Julkisen hallinnon suositukset (JHS)

Julkisen hallinnon toteuttamiseen on valmisteltu vuosina 1992–2019 suosituksia kuntien ja valtion yhteistyönä. Suositukset on koottu verkkoon osoitteeseen https://www.suomidigi.fi/ohjeet-ja-tuki/jhs-suositukset, mutta suosituksia tuottava järjestelmä lakkautettiin 2020, kun tiedonhallintalaki 906/2019 tuli voimaan. Vuonna 2020 voimassa olleet suositukset on löydettävissä verkkosivustolta ja niitä voi edelleen hyödyntää. Sivustolla on saatavissa 62 suositusta, joista 16 on merkitty vanhentuneeksi. Kuntien tietoturvallisuuden kannalta merkityksellisiä ovat ainakin seuraavat suositukset:

- JHS176 Sähköisten asiakirjallisten tietojen käsittely, hallinta ja säilyttäminen
- JHS179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen
- JHS198 kokonaisarkkitehtuurin peruskuvaukset
- JHS156 Asiakirjojen ja tietojen rekisteröinti sähköisen asioinnin ja asiankäsittelyn tiedonhallinnassa
- JHS189 Avoimen tietoaineiston käyttölupa
- JHS190 Julkisten verkkopalveluiden suunnittelu ja kehittäminen
- JHS201 Rekisteritiedon metatiedot. (Digi- ja väestövirasto, 2021)

4.7.2 VAHTI-ohjeet

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) oli valtiovarainministeriössä toiminut työryhmä, joka kokosi tietoturvaan liittyviä ohjeita 1992–2013. Sen jälkeen työtä on jatkanut Valtionhallinnon tieto- ja kybertuvallisuuden johtoryhmä (2014–2016) ja Julkisen hallinnon turvallisuuden johtoryhmä (2017–2019). Kaikkien näiden johtoryhmien tuottamat ohjeet on koottu verkkoon osoitteeseen https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet. Osa ohjeista on vanhentuneita, mutta niitä voidaan soveltaa perusperiaatteiden osalta edelleen. Sivustolla on saatavissa voimassa olevina ohjeina 21 ohjetta/opasta ja vanhentuneina 25 ohjetta/opasta. Kaikkia ohjeita voidaan soveltaa kunnallisessa tietoturvallisuuden kehittämisessä. Keskeisiä ohjeita on vaikea erotella tietoturvastrategian ja politiikan muodostamisen

näkökulmasta, sillä ohjeisto kokonaisuudessaan on tarkoitettu julkishallinnon tietoturvatyön tukemiseksi.

4.8 Turvallisuustasot ja minivaatimukset

Suomessa tietoturvallisuuden jaottelu on toteutettu neljällä tasolla: Perustaso, korotettu taso, korkea taso ja erityistaso. Tasot yhtenevät kansalliseen turvallisuusluokitteluun TLIV (käyttö rajoitettu) – TLIII (Luottamuksellinen) – TLII(Salainen) – TLI (erittäin salainen). (Valtiovarainministeriö, 2014) Viranomaisten tietojärjestelmät on saatettava turvaluokan TLIV perustason vaatimusten tasalle 1.7.2013 mennessä. (Valtioneuvosto, 2010)

Varsinaiset perustason vaatimukset on esitelty VAHTI-ohjeen 2/2014 liitteessä 4. Seuraava on suora lainaus liitteestä 4:

”Tietoturvallisuuden toteuttamiseksi valtionhallinnon viranomaisen on huolehdittava siitä, että:

1. viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan;
2. viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään;
3. asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään;
4. tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi;
5. asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi;
6. tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä;
7. asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja;
8. henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla;
9. henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä;
10. annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.” (Valtiovarainministeriö, 2014)

Näiden vaatimusten toteuttamiseksi VAHTI-ohje 3/2012 ” Teknisen ICT-ympäristön tietoturvataso-ohje” esittelee jokaiseen kohtaan menetelmän tai

välineen vaatimuksen toteuttamiseksi. Mikäli julkinen tai yksityinen organisaatio käsittelee korotetun tason tietoa, voidaan sen tietoturvallisuuden tasoa arvioida Kansallisen auditointikriteeristön (KATAKRI) mukaisesti. KATAKRI:n ensimmäinen versio on julkaistu vuonna 2009 ja sitä on päivitetty 2011 ja 2015. Viimeisin versio on lausuntokierroksella vuonna 2020. KATAKRI ei kuitenkaan ole viranomaisvaatimus.

Kansainvälisesti tietoturvallisuuden tason luokitteluun on useita erilaisia menetelmiä, joista NIST on tuottanut Yhdysvaltojen kansalliset tietoturvallisuuden minivaatimukset julkishallinnolle "FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems". Tässä tietoturvan minimivaatimukset jaetaan 17 osa-alueeseen, jotka jaetaan lisäksi teknisiin ja hallinnollisiin keinoihin. Jokaisen osa-alueen osalta tulisi laatia sekä toiminnallisia, että hallinnollisia keinoja minimivaatimusten täyttämiseksi. Asiakirja ei määritä tapoja vaatimusten toteuttamiseksi, vaan ne kuvataan NIST dokumentissa 800-53" Recommended Security Controls for Federal Information Systems." (Stallings & Brown, 2018) & (National Institute of Standards and Technology , 2006)

Suojauskeinot valitaan käyttöön suojattavan järjestelmän tai tiedon vaikuttavuuden perusteella huomioiden kustannustehokkuus, riskianalyysi sekä mahdollinen tietoturvastrategia. Käytettävä jaottelu asiakirjassa on: alhaisen tason, keskitason ja korkean tason järjestelmät. Järjestelmien jaottelu kuuluu osaksi riskien arviointia tässä asiakirjassa. (National Institute of Standards and Technology , 2006)

4.9 Johtopäätökset

Suomessa digitaalisesta turvallisuudesta vastaavia ministeriöitä sekä virastoja on useita. Lisäksi on varsinainen lainsäädännöllinen elin eduskunta, jonka vastuulla varsinainen lainsäädäntö on. Kaikki nämä toimijat tuottavat merkittävän määrän lainsäädäntöä, asetuksia, määräyksiä ja ohjeita, joita julkisessa hallinnossa tulee noudattaa. Tutkitun materiaalin määrä on erittäin suuri ja jaettu useaan eri paikkaan. Tässä tutkimuksessa löytyi tietoturvaan liittyen 41 lakia, 62 suositusta (joista 16 vanhentunutta), 46 ohjetta/opasta (joista 25 vanhentunutta). Tutkimuksessa ei todennäköisesti löydetty kaikkia kuntien tietoturvallisuuteen liittyviä lakeja, asetuksia, ohjeita tai oppaita eikä EU-lainsäädäntöä tutkittu, sillä esimerkiksi VAHTI-ohje 2/2009 ICT-varautumisesta listaa varautumiseen liittyen 43 lakia, joista osaa ei käsitelty tämän tutkimuksen listauksessa.

Virtain kaupunki on tietoturvapolitiikassaan luetellut noudattavia asiakirjoja, mutta listauksesta puuttuu merkittäviä kokonaisuuksia. Muut tutkitut kohteet eivät ole luetelleet noudatettavia asiakirjoja osana tietoturvapolitiikkaa. Yksittäisistä tutkituista kunnista ei voi päätellä valtakunnallisen ohjauksen kokonaisuuden ymmärrettävyyttä ja selkeyttä, mutta kokonaisuudesta jää sekava vaikutelma.

Valtion ohjaus kuntien tietoturvan muodostamiselle on periaate- ja strategiatasolla lueteltu muutamassa keskeisessä asiakirjassa. Kansallisesti haasteita on tunnistettu kuntatasolla ja toimenpideohjelma on käynnistetty. Tällä työllä ei kuitenkaan ole ollut merkitystä vuoden 2019 tutkittuihin tapauksiin, sillä toimenpideohjelmat ovat käynnistyneet liian myöhään.

Kunta on toimijana itsenäinen ja päättää omasta strategiastaan itse. Sen tehtäviin kuuluu kuntalain mukaan hyvä hallinto ja hallinnon järjestäminen tietoturvallisesti. Toimintaa varten kunnan pitää resursoida oma toiminta ja päättää, millä tavoin se järjestää tietoturvaan liittyvät asiat sisäisesti tai ulkoistamalla. Vastuuta kunta ei voi ulkoistaa, vaikka kunnan digitaalisia palveluita ulkoistettaisiin.

Tietoturvaan liittyvä päätöksenteko ei poikkea muusta kunnallisesta päätöksenteosta. Tietoturvaan liittyvät esitykset valmistelee kuntakohtaisesti tietohallinto tai vastaava organisaatio. Päätökset esitellään eri toimielimissä kunnassa kuntakohtaisesti ja lopullisen päätöksen muun muassa tietoturvapolitiikan käyttöönotosta tekee kunnan hallitus.

Tietoturvatyötä kunnissa ohjaa merkittävä määrä eri lakeja, asetuksia ja ohjeita. Selkeää ohjausta muodostaa tietoturvastrategia tai -politiikka on hankala löytää. Laeista ja asetuksista ei löydy selkeästi määräystä tietoturvan tekemistavoista, riskienarvioinnista ja mittaamisesta, vaikka riskien arviointi ja kehittäminen mainitaan. Selkein kokonaisuus muodostuu VAHTI-ohjeista. Lainsäädäntöpohja on sekava ja jaettu moneen paikkaan. Tutkimuksen viitekehyksessä tämä tarkoittaa sitä, että kuntien välille syntyy eroja tietoturvapolitiikan sisällössä ja esimerkiksi mitattavuus ja vertailtavuus vaikeutuu. Lisäksi referenssin löytäminen ohjaavista asiakirjoista on hankalaa, eikä viitteitä valtakunnan laajuisesta yhteistyöstä löydy tutkitusta materiaalista tai henkilöiden haastatteluista. Yhteistyötä tehdään toki yksittäisten kuntien välillä.

Tietoturvan organisoinnista ei löydy selkeää merkintää laeista tai säädöksistä. Esimerkiksi tutkimuskohteiden kunnat järjestävät tietoturvan paikallisessa hallintosäännössä käsketyllä tavalla. Lainsäädäntö käskee kuitenkin asettamaan vastuun tietoturvallisuudesta jollekin määritetylle taholle kunnassa.

Tietoturvastrategian toteuttamiseksi tutkituista asiakirjoista löytyy kansallista ohjausta, josta joitain osia voitaisiin hyödyntää kuntien tietoturvastrategiassa. Keskeiset periaatteet, kuten riskien arviointi, koulutus, suoritustason mittaaminen ja kehittämisen menetelmät ovat samoja hallinnon tasosta riippumatta. Vain näiden periaatteiden suoritustasot ja käytettävät menetelmät vaihtuvat.

Tietoturvapolitiikan osalta tarkastellut asiakirjat muodostavat kansallisesti kattavan pohjan. Vaikka tieto on merkittävästi hajallaan, niin kunnallisen tietoturvastrategian ja -politiikan muodostamiseksi on paljon tietoa. Keskeinen tutkimustapausten aikaan voimassa ollut asetus on ollut ”Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa” sekä VAHTI-ohjeet. Keskeiset lait käskevät muun muassa rekistereiden muodostamisen ja ylläpidon sekä

tiedon luokittelun periaatteet sekä varsinaiset merkinnät. Asiakirjoissa ei kuitenkaan käsketä tietojärjestelmien elinkaaren keskeisiä periaatteita, jolloin muun muassa tietojärjestelmien dokumentaatiosta käsketään vain tietojärjestelmäselosteiden muodossa.

Asiakirjojen perusteella voidaan todeta, että kunnan tietoturvastrategian tai -politiikan tekemiseen tarvitaan runsaasti asiantuntemusta voimassa olevista laeista, asetuksista ja suosituksista. Lisäksi strategian ja politiikan muodostajan on syytä tietää ennakkoon tietoturvan kehittämisen keskeiset periaatteet, jotta tutkituista asiakirjoista voidaan poimia kuntatason ohjaukseen tarvittavat asiat ja soveltaa ne hallintotasolle sopivaksi.

5 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄT

Tämä luvun lähteenä käytetyt SFS-EN ISO/IEC 27000:2020 (jatkossa ISO27000) ja SFS EN ISO/IEC 27001:2017 (jatkossa ISO27001) on hankittu alun perin tutkijan yrityksen käyttöön ja standardien lainaukset on tehty Suomen Standardisoimisliitto SFS ry:n luvalla. Tutkijalla on käyttöoikeus lähdemateriaaliin.

Tässä luvussa tarkastellaan viitekehykseksi valittua ISO27000-standardisarjaa ja ISO27001-standardia sekä niiden soveltamista tietoturvallisuuden johtamisessa ja kehittämisessä kunnassa tietoturvallisuuden hallintajärjestelmänä. Luvun tarkoituksen on antaa yleiskuvat ISO27000-standardisarjasta sekä ISO27001 rakenteesta ja pohtia sen soveltumista julkisen organisaation käyttöön. Tarkastelu toteutetaan yleisellä tasolla, sillä soveltamista julkiseen organisaatioon on tutkittu muun muassa Tatu Suhosen pro gradu -tutkimuksessa ”ISO/IEC 27001 -sertifioinnin hankintaperusteet ja sertifiointielimen valintaperusteet” (JYU 2019) ja Tiina Virran pro gradu -tutkimuksessa ”ISO 27001 -standardiin perustuva tietoturvajohtamisen hallintamalli THL:lle” (JYU 2020).

Tämän luvun tarkoituksena on kuvata työvälineitä tietoturvallisuustyön tekemiseksi edellisessä luvussa kuvatun lainsäädännön ja ohjeiden pohjalta.

5.1 Tietoturvallisuuden hallintajärjestelmä - yleistä

Tietoturvallisuuden hallintajärjestelmä (Information Security Management System, ISMS) on formaali ja järjestelmällinen tapa lähestyä organisaation tietoturvan tai sen osan kehittämistä. Niitä voi käyttää kaiken kokoiset organisaatiot, jotka käsittelevät tietoa, pitävät tietoa merkittävänä tekijänä liiketoiminnassaan, tietoon kohdistuu uhkia ja niiden hallintaan halutaan käyttää järjestelmällisiä hallintakeinoja. Tietoturvallisuuden hallintajärjestelmän tavoitteena on riskien hallinta ja toiminnan jatkuvuuden turvaaminen. Hallintajärjestelmät voivat ottaa huomioon voimassa olevan lainsäädännön, kuten EU GDPR (European union General Data Protection Regulation). (Suomen standardisoimisliitto SFS, 2020) (Dutton, 2019) (TechTarget, 2011)

Tietoturvallisuuden hallinta on kehittynyt kansainvälisesti voimakkaasti viimeisinä vuosikymmeninä. Tiedonhallinnan suorituskyvyt, kuten tietokoneet ja tietoverkot ovat aikaansaaneet kansainvälisiä parhaita käytäntöjä, joista on muodostettu standardeja. (Stallings & Brown, 2018) Tietoturvan kasvavien vaatimusten täyttämiseksi, voidaan organisaatioissa käyttää erilaisia tietoturvastandardeja ja sertifiointeja. Tietoturvastandardit voivat olla teknologia- tai johtamispainotteisia. Teknologiapainotteiset standardit tuottavat loogisia ja fyysisiä ratkaisuja muun muassa tietojärjestelmien tietoturvaan kun

johtamispainotteiset standardit tuottavat hyvää tietojärjestelmien tietototurvan hallintaa ja menetelmiä. (Hsu, 2009) Tämän tutkimuksen kannalta johtamispainotteiset standardit ovat tutkimuksen kohteena.

Tietoturvallisuuteen on kehitetty useita johtamispainotteisia standardeja sekä viitekehyksiä, joita tarvelähtöisesti voidaan harkita eri organisaatioiden käyttöön. Suomessa ei ole valittu valtionhallinnossa yhtä tapaa toteuttaa tietoturvallisuutta, mutta esimerkiksi Yhdysvalloissa National Institute of Standards and Technology (NIST) tuottaa materiaalia julkisille organisaatioille. Suomessa liikenneministeriö on huomioinut standardisoinnin yhtenä keinona valita sopimuskumppaneita sekä julkisessa hallinnossa että yksityisellä puolella. Standardisoinnin tulee rakentua liiketoiminnan tarpeista, vaikka se usein nähdään erillisenä osana. (Liikenne- ja viestintäministeriö, 2016)

Kansainvälistä tietoturvaan liittyvää standardisointia tekee kolme organisaatiota: International Organization for Standardization (ISO), International Electrotechnical commission (IEC) ja Internation TeleCommucation Union (ITU). (Wikipedia, 2021) Kansallisesti tietoturvaan liittyviä standardeja tekee esimerkiksi Yhdysvalloissa National Institute of Standards and Technology (NIST). (National Institute of Standards and Technology, 2017)

ISO on kansallisten standardisointijärjestöjen liitto, joka laatii ja tutkii standardeja, suorituskyvyn kehittämistä ja kouluttaa standardeja, niiden soveltamista ja muun muassa auditointeihin kuuluvia henkilöitä. Liittoon kuuluu 165 maata. Kehittämistyöhön ei voi osallistua suoraan yksityiset henkilöt tai yritykset, vaan osallistuminen tapahtuu kansallisesti. Kehittämistyö tuottaa standardien lisäksi teknisiä määrityksiä, raportteja, julkisia määrityksiä, sopimuksia ja ohjeita. ISO27000-sarja on yksi ISO:n tuottama tietoturvallisuuteen liittyvä standardisarja. (International organization for Standardization, 2021)

NIST on Yhdysvaltojen kauppaministeriön alainen organisaatio, joka vastaa kansallisesti standardisoinnista. NIST on tuottanut kansalliseen käyttöön tietoturvaan liittyviä standardeja, kuten SP 800-12 ”An introduction to information security”, SP 800-181 “Workforce framework for cybersecurity”, SP 800-18 ”Guide for developing security plans for federal information systems” ja “Framework for improving critical infrastructure cybersecurity”.

Muita kansainvälisesti käytettyjä tietoturvallisuuden hallintamalleja ja viitekehyksiä ovat muun muassa Zachman Framework, TOGAF (The Open Group Architecture Framework), E2AF (Extended Enterprise Architecture Framework), GERAM (Generalized Enterprise Reference Architecture and Methodology). (Magoulas;Hadzic;Saarikko;& Pessi, 2012). Näiden lisäksi kirjallisissa lähteissä mainitaan myös EISA (Enterprise Information Security Architecture) ja SABSA (the Sherwood Applied Business Security Architecture) sekä Yhdysvalloissa on puolustusministeriön käyttöön tehty DoDAF (Deparment of Defence Architecture Framework) monimutkaisten toimintojen riippuvuuksien ja rajapintojen hallintaan.

5.2 Tietoturvan hallintajärjestelmän käyttöönotto ja saavutettavat hyödyt

Tietoturvan hallintajärjestelmän käyttöönotto on organisaation strateginen valinta. Kyseessä on prosessiin pohjautuva menetelmä tietoturvan parantamiseksi ja organisaation toiminnan jatkuvuuden varmistamiseksi. Järjestelmän onnistumista edistää muun muassa ymmärrys tietoturvan tarpeesta, vastuiden määrittely, johdon sitoutuminen ja sidosryhmien huomiointi, yhteiskunnan arvojen tukeminen, riskien arviointi, turvallisuuden sisällyttäminen tietojärjestelmien olennaiseksi osaksi, tietoturvahäiriöiden havainnointi ja ehkäisy, kattavan toimintatavan varmistaminen ja tehdyn työn uudelleen arviointi sekä jatkokehittäminen. (Suomen standardisoimisliitto SFS, 2020)

5.3 ISO27000 tietoturvan hallintajärjestelmien yleiskuvaus

Tässä standardissa esitellään ISO27000-standardisarja sekä siihen liittyvä keskeinen sanasto. Standardisarja on tarkoitettu kaiken tyyppisille organisaatioille, jotka käsittelevät tietoa, tietoon kohdistuu uhkia ja tieto on tärkeää toiminnan kannalta sekä organisaatio vastaa uhkiin toteuttamalla tietoturvan hallintakeinoja. Standardi ISO27000:2020 on viides julkaisu ja se kumoaa edellisen ISO27000:2016.

ISO on yhdistänyt useita teknisistä ja toiminnallisista tietoturvakäytännöistä standardisarjaan ISO27000, joka käsittää sarjan osat 27000–27021 (ei sisällä toistaiseksi osia 27012, 27015 ja 27020). Sarja on jaettu neljään osaan seuraavasti:

1. Sanastostandardit
2. Vaatimusstandardit
3. Ohjestandardit
4. Toimialakohtaiset standardit.

ISO27000-standardisarja on hyväksytty kansainväliseksi standardiksi ja se on hyväksytty myös Suomessa.

Siirryttäessä tietoturvastrategia ja -politiikasta toimenpiteisiin, voidaan käyttää muita sarjan osia täydentämään ja toteuttamaan muodostetussa politiikassa vaadittuja käytäntöjä. (Suomen standardisoimisliitto SFS, 2020)

Tämän tutkimuksen kannalta merkittävimmät ovat tietoturvan hallintajärjestelmää kuvaavat osat. Näitä osia ovat:

- ISO27000: Tietoturvallisuuden hallintajärjestelmät
- ISO27001: Tietoturvallisuuden hallintajärjestelmän vaatimukset.

5.4 ISO27001 tietoturvan hallintajärjestelmän vaatimukset

Tämä alaluku esittelee ISO27001 standardin yleisesti ja sitoo standardin hyödynnettävyyden julkiseen organisaatioon seuraavaa lainsäädännöllistä lukua varten. Tämä alaluku ei käsittele kaikkia yksittäisiä vaatimuksia, sillä standardin soveltaminen vaihtelee sitä soveltavan organisaation ja toimintaympäristön mukaan.

ISO27001-standardi kuuluu edellä kuvattuun ISO27000-standardisarjaan ja sen osaan vaatimusstandardit. Kyseessä on kansainvälinen standardi. ISO27001 määrittelee vaatimukset, joilla luodaan tietoturvan hallintajärjestelmä ja toteutetaan käyttöönotto, käytetään sitä, seurataan ja katselmoidaan käyttöä, suoritetaan ylläpito ja parannetaan sen käyttöä kohdeorganisaatiossa. Vaatimukset ottava huomioon liiketoiminnan riskit. Standardia voidaan soveltaa koko organisaatioon tai sen osaan eikä organisaation kokoa, toimialaa tai muita sitä määrittäviä kokonaisuuksia ole määritelty tai niillä ei ole merkitystä.

Standardin vaatimukset voidaan ottaa organisaation tietoturvallisuuden hallintajärjestelmän vaatimusten pohjaksi, mutta standardissa odotetaan, että organisaation, toimialueen, liiketoiminnan ja muut muutokset otetaan jatkuvasti huomioon hallintajärjestelmää käyttöönotettaessa ja kehitettäessä. Standardin mukaan on tärkeää, että tietoturvallisuuden hallintajärjestelmä yhdistyy organisaation muihin prosesseihin ja johtamis- sekä hallintarakenteisiin.

Standardit esittää tietoturvallisuuden liittyviä vaatimuksia yleisellä tasolla ja niitä on tarkoitus soveltaa organisaation mukaan. Vaatimukset on esitetty standardissa ISO/IEC määrittämässä rakenteessa, mutta rakenne ei muodosta vaatimusten tärkeysjärjestystä. Asiakirja jakautuu vaatimusten osalta 7 lukuun (luvut 4–10) sekä näitä tukevaan liitteeseen A ”Hallintatavoitteiden ja -keinojen viiteluettelo”.

Vaatimusten pääluvut käsittelevät seuraavia kokonaisuuksia:

- luku 4: Organisaation toimintaympäristö
- luku 5: Johtajuus
- luku 6: Suunnittelu
- luku 7: Tukitoimet
- luku 8: Toiminta
- luku 9: Suorituskyvyn arviointi
- luku 10: Parantaminen.

Pääluvut kuvaavat yleisellä tasolla tietoturvallisuuden hallintajärjestelmää käyttöönottavaan organisaatioon kohdistusvia vaatimuksia. Vaatimukset eivät ole teknisiä, vaan toiminnallisia. Ne kuvaavat sekä tietoturvallisuuden hallinnan prosesseja että organisaatioon tai sen osiin kohdistuvia vaatimuksia. Esimerkki vaatimuksesta luku 5.2 ”tietoturvapolitiikka”: ”Ylimmän johdon on laadittava tietoturvapolitiikka”.

Liitteessä A yleisen tason vaatimuksille esitetään hallintakeino taulukkomuodossa. Tarkennukset kohdistuvat päälukujen vaatimuksiin, joskaan vaatimusten numerointi ei ole päälukujen kanssa yhtenevä vaan yhtenee

ISO27002 ”Tietoturvallisuuden hallintakeinojen menettelyohjeet”-rakenteeseen. Tarkennukset on jaettu 14 pääotsikkoon ja niitä täydentäviin alakohtiin hallintakeinoineen. Alakohdat kuvaavat hallintajärjestelmään liittyvän vaatimuksen sekä siihen liittyvän hallintakeinon. Pääotsikot ovat:

- A.5: Tietoturvapolitiikat
- A.6: Tietoturvallisuuden organisointi
- A.7: Henkilöstöturvallisuus
- A.8: Suojattavan omaisuuden hallinta
- A.9: Pääsynhallinta
- A.10: Salaus
- A.11: Fyysinen turvallisuus ja ympäristön turvallisuus
- A.12: Käyttöturvallisuus
- A.13: Viestintäturvallisuus
- A.14: Järjestelmien hankkiminen, kehittäminen ja ylläpito
- A.15: Suhteet toimittajiin
- A.16: Tietoturvahäiriöiden hallinta
- A.17: Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
- A.18: Vaatimustenmukaisuus.

Esimerkki hallintatavoitteesta ja -keinosta A.5.1.1: ”Tietoturvapolitiikka: Hallintakeino. Tietoturvallisuudelle on määriteltävä joukko johdon hyväksymiä politiikkoja, jotka julkaistava henkilökunnan ja asiaankuuluvien organisaation ulkopuolisten osapuolten käyttöön ja joista tiedotetaan henkilökunnalle ja osapuolille.”

5.4.1 Referenssinä tietoturvaperiaatteet ja -käytännöt

Edellä kuvattu ISO27001-standardin rakenne on osin sama, kuin VAHTI-ohjeessa 4/2007 määritelty ”Tietoturvaperiaatteet ja -käytännöt”. Tämän dokumentin rakenne on:

1. Hallinnolliset turvallisuustoimenpiteet ja johtaminen
    - 1.1. Turvallisuuden tarkoitus ja tavoitteet
    - 1.2. Johdon hyväksymät periaatteet ja linjaukset
    - 1.3. Toteutusidea
    - 1.4. Vastuut, toiminnan organisointi ja johtaminen
    - 1.5. Turvattavat toiminnot ja järjestelmät
    - 1.6. Sopimukset
2. Tietoturvatoimenpiteet ja menettelyt
    - 2.1. Henkilöstöturvallisuus
    - 2.2. Tietoaineistoturvallisuus, varmuus- ja suojakopiointi
    - 2.3. Fyysinen turvallisuus
    - 2.4. Laitteistoturvallisuus
    - 2.5. Ohjelmistoturvallisuus
    - 2.6. Tietoliikenneturvallisuus
    - 2.7. Käyttöturvallisuus, haittaohjelmistoilta suojautuminen

3. Ulkoistettujen tietojenkäsittelytoimintojen turvallisuus
4. Keskeisten kehittämiskohteiden varmistaminen
(esimerkiksi asiointipalvelu, etätyö)
5. Tietoturvatoimenpiteiden toteuttaminen hankintojen yhteydessä
6. Tietoturvallisuuden seuranta, valvonta, tarkastus ja testaus
7. Ohjeet
8. Valmiudet ja menettelyt vahinkotilanteisiin
9. Koulutus
10. Suunnitelman päivitys ja toimenpiteiden ylläpito
11. Raportointi johdolle. (Valtiovarainministeriö, 2007)

5.5 Johtopäätökset

Tietoturvallisuuden hallintajärjestelmiä ja niihin liittyviä viitekehyksiä on useita. Eurooppalainen ISO/IEC27000-standardisarja on hyväksytty kansainväliseksi standardiksi ja useissa lähteissä sitä pidetään tietoturvallisuuden hallintajärjestelmiä määrittävänä standardisarjana. Se on hyväksytty myös Suomessa ja sitä on suositeltu käytettäväksi valtionhallinnon suosituksissa organisaatioita erottelematta. Standardisarja on kehittyvä ja tutkimuksen kirjoitushetkellä ISO27000:2020 korvaa käyttöön hyväksytyn ISO27000:2017-sarjan.

ISO27000-standardisarja kuvaa tietoturvallisuuden hallintajärjestelmän kokonaisuuden ja toimiala- tai organisaatiotyyppiriippumaton. Se soveltuu käytettäväksi julkisessa hallinnossa ja on sovellettavissa erikokoisiin organisaatioihin, esimerkiksi erikokoisiin kuntiin.

Rakenteellisesti standardisarja käsittelee tietoturvaa yleiseltä tasolta kohti yksityiskohtia. Pääasiakirjana ISO27000 käsittelee vain standardisarjaa sekä siihen liittyvää sanastoa. Standardisarjan rakenne mahdollistaa organisaatioiden osalta vain tarpeellisten standardien hankkimisen tietoturvallisuuden hallintajärjestelmän muodostamiseksi. Standardisarjaan kuuluu myös kaksi toimialakohtaista standardia energiatoimialalle ja terveydenhuoltoon. Rakenteellisesti sarja soveltuu julkiseen hallintoon kuten kuntiin.

Tutkimuksessa tarkasteltu ISO27001-standardi kuvaa tietoturvallisuuden hallintajärjestelmän vaatimukset yleisellä tasolla ja on suunnattu tietoturvallisuuden hallintajärjestelmän käyttöä suunnittelevan organisaation ylimmäksi ohjaavaksi asiakirjaksi. ISO27001 itsessään ei ole tietoturvallisuuden hallintajärjestelmä vaan kuvaus sen vaatimuksista. Standardi kuvaa vaatimukset organisaatioin ylimmän johdon sekä tietoturvapolitiikan muodostavat ja toteuttavan tason näkökulmasta. Standardi ei yksilöi tekniikoita eikä prosesseja vaan tarjoaa eri kokonaisuuksien toteuttamiseksi hallintakeinoja, eli tapoja toteuttaa vaatimukset. Näitä hallintakeino yksilöidään lisää muissa sarjan standardeissa. ISO27001 soveltuu julkisessa organisaatiossa organisaation johdon ja tietoturvaa johtavan ja toteuttavan henkilökunnan työvälineeksi, mutta

ei riitä tietoturvan hallintajärjestelmän tekemiseksi ilman kokemusta tai osaamista.

Tietoturvallisuuden hallintajärjestelmä voidaan luoda standardoidun mallin, kuten ISO27000-sarjan pohjalta. Tutkitut asiakirjat eivät kuitenkaan velvoita auditoimaan valittua järjestelmään vaan valitun mallin mukaisesti tarkastelemaan sitä määräajoin. Koska varsinainen standardointi ja standardin ylläpitäminen mielletään kalliiksi, kunnat voisivat soveltaa tietoturvanhallintajärjestelmän rakennetta sekä syklistä ylläpitoa.

ISO27001-standardin esittämä rakenne ei mukaile valtionhallinnon VAHTI-ohjeessa 4/2007 määriteltyä esimerkkirakennetta tietoturvapolitiikasta. Sen sijaan se noudattelee saman ohjeen ”tietoturvaperiaatteet ja -käytännöt” esimerkkirakennetta, joten se on hyödynnettävissä osaksi tietoturvapolitiikkaa tai siitä muodostettavia periaatteita ja käytäntöjä.

6 TUTKIMUSTAPAUKSET

Tässä luvussa käsitellään tapaustutkimuksen kohteisiksi valitut Lahden ja Kokemäen kyberhyökkäykset sekä referenssiksi valitut Espoon ja Virtain kaupungin tietoturva- ja tietosuojapolitiikat. Tapaukset käsitellään esittelemällä ennen kyberhyökkäystä käytössä ollut tietoturvapolitiikka, käsittelemällä tapahtunut kyberhyökkäys näkökulmana käytössä ollut tietoturvapolitiikka ja lopuksi esittelemällä joko tietoturvapolitiikassa tapahtuneet muutokset tai muu muutokseen liittyvä materiaali. Referenssien osalta esitellään vain voimassa ollut tietoturvapolitiikka.

Tämän luvun tarkoituksena on esitellä tutkimuksen varsinaiset tutkimustapaukset ja löytää niiden perusteella tietoturvastrategiaan ja -politiikkaan sekä tietoturvan hallintajärjestelmään liittyvät yhteydet tai niiden puutteet.

6.1 Referenssit

Tutkimuksen referenssiksi on valittu Espoon kaupungin ja Virtojen kaupungin tietoturvapolitiikat. Valinta pohjautui voimassa olevan tietoturvapolitiikan saatavuuteen ja luettavuuteen sekä kuntien kokoon. Espoon ja Lahden vertailu ei ole koon puolesta perusteltua, mutta Espoon kaupunki on vuodesta 2018 alkaen profiloitunut tietoturvatyössä ja soveltuu sen vuoksi referenssiksi. Seuraava kuntien vertailu perustuu stat.fi-sivuston vertailutietoihin, aluejakona on käytetty vuotta 2019:

	Lahti	Espoo	Kokemäki	Virrat
Väkiluku 2018	283 632	119 951	7226	6739
Työllisyysaste 2017	74,2	66,5	67,8	67,3
Vähintään toisen asteen tutkinnon suorittaneiden osuus 15 vuotta täyttäneistä, %, 2018	77	71,8	66,8	65,8
Alueella olevien työpaikkojen määrä, 2017	120 676	50 573	2308	2289

TAULUKKO 1 Tutkimuskohteiden ja referenssien vertailu

Espoo ei ole toimijana joutunut kyberhyökkäyksen onnistuneen, havaitun ja laajan kyberhyökkäyksen kohteeksi toistaiseksi. Sen tietoturvapolitiikka on

vuodelta 2018 ja se on otettu käyttöön 28.5.2018 otsikolla ”Espoon kaupunki, Tietoturva- ja tietosuojapolitiikka”.

Virrat ei ole toimijana joutunut onnistuneen laajan kyberhyökkäyksen kohteeksi toistaiseksi. Sen tietoturvapolitiikka on kaupungeista uusin ja se on otettu käyttöön 10.12.2018 otsikolla ”Virtain kaupungin tietoturva- ja tietosuojapolitiikka”. (Virtain kaupunki, 2018)

6.1.1 Espoon kaupungin tietoturvapolitiikka

Espoon kaupunki otti käyttöön viimeisimmän tietoturvapolitiikan 2018. Kyseessä on vuoden 2016 tietoturvapolitiikan päivitys. Politiikan on tarkastanut kaupungin tietoturvaryhmä 19.4.2018 ja hyväksynyt kaupunginhallitus 28.5.2018 nimellä ”Tietoturva- ja tietosuojapolitiikka”. (Espoon kaupunki, 2018)

Asiakirja on 8 sivua pitkä ja sisältää 9 lukua. Sen alussa kuvataan tietoturvan ja -suojan merkitys kaupungin toiminnalle sekä käydään läpi tietoturvan peruskäsitteistö luottamuksellisuus-eheys-käytettävyys kautta. Tietosuojan käsitteistölle on oma lukunsa, jossa luetellaan tietosuojan periaatteet. Luvuissa 4 käsitellään riskienhallinta, joka tietoturvan sekä tietosuojan rakentumisen perustana. Luvussa 5 käsitellään varautumista, luvussa 6 vaatimustenmukaisuutta ja tavoitteita ja luvussa 7 tietoturvan ja tietosuojan organisoitumista sekä vastuita. Luvussa 8 käsitellään tiedon ja tietojärjestelmien käyttö ja luvussa 9 tietoturva- ja tietosuojaosaaminen. Tämä asiakirjan on asetettu julkisesti saataville Espoon kaupungin verkkosivuille. (Espoon kaupunki, 2018)

Asiakirjan rakenne ei noudattele tutkittuja valtionhallinnon esimerkkirakenteita tai tietoturvan hallintajärjestelmien rakennetta eikä sen sisältö vastaa niitä. Asiakirja on luonteeltaan strategia, jossa otetaan kantaa tavoitteisiin, keskeisiin noudatettaviin reunaehtoihin ja vastuisiin sekä resursointiin. Asiakirja ei sisällä teknisiä tai toiminnallisia ohjeita tietoturvan tai tietosuojan toteuttamiseksi pois lukien edellä mainitut reunaehdot. Asiakirja ei sisällä tietoturvan mittaamiseen tai jatkuvaan parantamiseen liittyviä kohtia, mutta siinä mainitaan henkilökunnan perehdytys sekä jatkokoulutus.

6.1.2 Virtain kaupungin tietoturvapolitiikka

Virtain kaupunki otti käyttöön tietoturvapolitiikan 2018. Tätä politiikkaa on edeltänyt vastaava tietoturvapolitiikka 2015. Politiikan on hyväksynyt kaupunginhallitus 10.12.2018 nimellä ”Virtain kaupungin tietoturva- ja tietosuojapolitikka”. (Virtain kaupunki, 2018)

Asiakirja on 12 sivua pitkä ja se sisältää 2 liitettä. Luvussa 1 kuvataan tietoturva ja tietosuojan merkitys kaupungille sekä käydään läpi keskeisiä käsitteitä. Luvussa 2 käsitellään tietoturvan keskeisiä käsitteitä ja periaatteita ja luvussa 3 tietosuojan vastaavia asioita. Luvussa 4 käsitellään tietoturvaorganisaatiota ja siihen liittyviä vastuita. Luvussa 5 käsitellään tietoturvan ja tietosuojan toteuttamista. Luvussa 6 kuvataan tietoturvan seurantaa ja valvontaa sekä siihen liittyvää ilmoittamismenettelyä. Luvussa 7

käsitellään koulutusta ja ohjeistusta. Asiakirja on saatavilla julkisesti Virtain kaupungin verkkosivuilla. (Virtain kaupunki, 2018)

Asiakirja on sisällöltään samankaltainen kuin Espoon kaupungin tietoturvapolitiikka. Se muistuttaa sisällöltään strategiaa. Keskeisenä erona Espoon kaupungin vastaavaan asiakirjaan on liitteet. Liitteessä 1 luetellaan tietosuojaan vaikuttava lainsäädäntö ja liitteessä 2 on tietoturvaan ja -suojaan liittyvät käsitteet.

6.2 Lahden kyberhyökkäys 11.6.2019

6.2.1 Tietoturvapolitiikan rakenne ennen hyökkäystä

Lahden kaupunki otti käyttöön tietoturvapolitiikan 4.4.2011 (Lahden kaupunki, 2011) Kyseessä on kaupungin ensimmäinen virallinen tietoturvapolitiikka. Se on nimetty tietoturvanpolitiikan näkökulmasta poikkeavasti ”Tietoturvan hoidon periaatteet” kaupungin johdon käskystä. (Monni, 2020) Politiikkaa on edeltänyt ohjekoonnelma, josta osia on käytetty muun muassa kaupungin työntekijöiden perehdyttämiseen. (Monni, 2020) Politiikka on muodostettu kaupungin tietohallintojohtajan virkatyönä ja se on hyväksytty kaupungin tietohallintotiimissä 23.3.2011, kaupungin johtoryhmässä 21.3.2011 ja lopuksi kaupungin hallituksessa 4.4.2011. Tietoturvapolitiikka ei perustu kaupungin tietoturvastrategiaan tai tietoturvariskien arvioon, koska kaupungilla ei sellaisia ole. (Monni, 2020) Riskien hallinta kuitenkin mainitaan varsinaisessa politiikka osuudessa luvussa 4.

Politiikka on 7 sivua pitkä ja se koostuu 6 luvusta. Sen alussa kuvataan tietoturvan merkitys kaupungin toimintaan sekä tietoturva-käsite yleisesti tietoturvan peruskäsitteistön luottamuksellisuus-eheys-käytettävyys kautta. Tämän jälkeen luvuissa 3 ja 4 kerrotaan tietoturvallisuuden organisointi lahden kaupungissa sekä siihen liittyvät keskeiset periaatteet. Luvuissa 5 ja 6 kerrotaan asiakirjan käyttöperiaate, sen suhde muuhun ohjeistukseen sekä soveltamisala.

Politiikkaa on käytetty ohjaamaan kaupungin tietoturvaa sekä työntekijöiden perehdyttämiseen. Lisäksi perehdyttämisessä on käytetty muuta kaupungin tietohallinnon tekemää ohjeistusta.

6.2.2 Tietoturvapolitiikan sisältö ennen hyökkäystä

Tietoturvapolitiikka on muodostettu tietohallintojohtajan ja tietohallintotiimin toimesta virkatyönä. Siihen ei ole vaikuttanut muut kaupungin toimialat. (Monni, 2020) Politiikka on tiivis ja selkeä luettava. Se on sisällön osalta tarkoitettu henkilöille, joilla ei ole aikaisempaa tietoturvakoulutusta.

Politiikan alku on strategian kaltainen. Siinä kuvataan kaupungin tietoturvan toimintakenttä sekä tietoturvatyön rooli siinä ja kaupungin toiminnassa. Tietoturvatyölle annetaan tarkoitus ja tavoite. Se ei kuitenkaan rajaa

tietoturvatyötä, resursseja eikä ohjaa työn toteuttamistapoja. Strategiatasolla tämä osuus on voinut ohjata tietoturvatyötä kyberhyökkäykseltä suojautumisessa.

Asiakirja ohjaa tietoturvatyön järjestäytymisen toimijan, vastuun ja tehtävän osalta. Organisaatio on kuvattu kattavasti vastuineen. Toimijat nimetään tehtävänhoitajan virkanimikkeellä esimerkiksi ”kaupunginjohtaja”, ryhmittäin esimerkiksi ”tietoturvaryhmä” ja eri virkoihin kuuluvin lisävastuin kuten ”rekisterinpitäjä”. Varsinaiset vastuut ovat lyhyesti kuvattu esimerkiksi ”vastaa rekisterin pitäjän antamista tehtävistä”. Kuvaukset ovat osien ympäripyöreitä eivätkä anna lukijalle kuvaa vastuun todellisesta luonteesta mittareineen. Tehtävä ovat konkreettisia kuten ”hyväksyy tietoturvan hoidon periaatteet”.

Varsinaisten toimijoiden, vastuiden ja tehtävien lisäksi tietoturvaryhmän tehtävä on kuvattu tarkemmin. Kyseessä on virtuaaliorganisaatio, joka toimii tietohallintotiimin alaisuudessa. Siihen kuului noin 20 henkilöä eri kaupungin toimialoilta. Kuvattujen tehtävien osalta tämä virtuaaliorganisaatio on ollut vastuussa merkittäviltä osin tietoturvaan liittyvien asiakirjojen tuottamisesta. Tämän organisaation kuvaaminen ja tehtävien määrittäminen on voinut vaikuttaa merkittävästi kyberhyökkäyksen torjunnassa.

Varsinainen politiikka on luvussa 4. Siinä on 13 kappaletta, joista jokainen sisältää jonkin tietoturvapoliittisen linjauksen. Tarkasteltaessa sitä viitekehyksessä valitun ISO27000 tietoturvan hallintajärjestelmän rakenteen kannalta, se sisältää viittaukset tietoturvallisuuden mittaamiseen, hallinnolliseen tietoturvaan ja henkilöturvallisuuteen. Näiden lisäksi se sisältää ohjeita tietojärjestelmien kehittämisestä, tiedottamisesta sekä yhteistyöstä. Tämän luvun sisällöllä on voinut olla suurin vaikutus kyberhyökkäyksen torjunnassa.

6.2.3 Kyberhyökkäys 11.6.2019

Lahden kaupungin tietojärjestelmään kohdistettiin kyberhyökkäys 11.6.2019 alkaen. Tämän luvun tiedot perustuvat Lahden kaupungin tietohallintojohtaja Markon Monnin haastatteluun sekä erikseen viitattuihin lähteisiin. Marko Monni toimi Lahden tietohallintojohtajan jo tietoturvapolitiikan laatimisessa 2011 ja jatkaa tehtävässään edelleen. Haastattelun materiaali on tutkijan hallussa.

Lahden kaupungin tietoverkkoa käytetään kaupungin hallintoon sekä eri toimijoiden palveluiden tuottamiseen. Siinä on toimijoina lahden kaupungin konserniin kuuluvan tietohallintoyksikön lisäksi Fujitsu Oy palveluiden toteuttajana sekä DNA tietoliikenneyhteyden ja konesalipalveluiden osalta. Varsinainen palvelutuotanto on jaettu tietohallintoyksikön ja Fujitsu Oy:n välillä.

Hyökkäyksen alkaessa kaupungin tietoverkko oli muutoksen kohteena, jossa osa palveluista tuotettiin käyttäen kaupungin tietoverkkoa vain siirtotienä palvelutuotannon ja loppukäyttäjän välillä. Tällaisia toimijoita oli muun muassa terveyden huolto hyvinvointikuntayhtymässä (HYKY). Tietoverkko oli mahdollista segmentoida fyysisesti eri osiin, mutta loogista segmentointia ei ollut tehty.

Hyökkäys käynnistyi etäkäyttötyöasemalta työntekijän työmatkalla Tampereella. Työasema-arkkitehtuuri mahdollisti tilanteen, jossa työasema oli VPN-yhteydellä kaupungin tietoverkossa ja toisella yhteydellä julkisessa internetissä yhtä aikaa. Hyökkääjä hyödynsi työasemaa julkisen internetin kautta ja sai haittaohjelma siirrettyä kaupungin tietoverkkoon tämän kautta.

Päästessään kaupungin tietoverkkoon haittaohjelma levisi kaikkiin käytössä olleisiin työasemiin. Työasemien haittaohjelmatunnistus (F-secure) tunnisti haittaohjelman ja eristi sen työasemassa, josta tuli ensimmäinen ilmoitus klo 14.36. Työntekijä sai haittaohjelmasta ilmoituksen kuten myös sen eristämisestä yksittäisessä työasemassa.

Tietoverkossa haittaohjelma pyrki myös pääsemään heikosti suojattuihin palvelimiin ja palveluihin. Verkossa tietokantapalvelimen järjestelmävalvojatunnus (admin) oli jäänyt esiasetustilaan, jossa asennuksen jälkeen käyttäjätunnusta tai salasanaa ei ollut vaihdettu. Haittaohjelma pääsi tietokantapalvelimelle ja sitä kautta levisi myös muihin palvelimiin kuten käyttöoikeuksia ja työasemien käynnistysjärjestystä ohjaavaan palvelimeen (active directory, AD). Tämän vuoksi haittaohjelma pääsi muokkaamaan verkossa kiinni olleitten työasemien käynnistysjärjestystä ja jokaisen käynnistyksen yhteydessä haittaohjelma suoritettiin uudelleen tietoturvaohjelmistosta huolimatta. Toisin sanoen haittaohjelmaa ei voitu poistaa käytössä olleella tietoturvaohjelmistolla eikä sen leviämistä voitu sillä pysäyttää.

Tapahtumaan selvittämiseen osallistuneiden mukaan haittaohjelma myös mahdollisti hyökkääjän pääsyn tietoverkkoon ja palveluihin todennäköisesti raportoimalla löytämänsä heikkoudet hyökkääjälle. Hyökkääjä pääsi näin aktiivisesti vaikuttamaan tapahtumiin hyökkäyksen aikana, josta saatiin myös tieto hyökkäyksen aikana.

Hyökkäyksen takia hyvinvointikuntayhtymä irrotettiin kaupungin verkosta 11.6. klo 20.21. Tämä johti siihen, että muun muassa eri osassa sijainneet sairaanhoidon palvelut eivät toimineet loppukäyttäjällä. Palvelut palautettiin osin klo 23.26, jotta terveydenhuoltoa ei olisi vaarannettu. HYKY irrotettiin kuitenkin uudelleen 12.6. klo 22.30, koska toimintaan osallistuneet asiantuntijat havaitsivat hyökkääjän olevan edelleen aktiivinen tietoverkossa.

F-securen asiantuntijat tunnistivat haittaohjelman 12.6. aamuyöllä ja tekivät ohjelmiston, jolla haittaohjelma saadaan poistettua järjestelmästä. Lupa sovelluksen asentamiseen tietoverkkoon annettiin 12.6. klo 14.00. Varsinaiset poistotoimenpiteet aloitettiin 14.6. klo 18.00, jolloin kaupungin ulkoinen tietoliikenneyhteys suljettiin ja poisto-ohjelmisto suoritettiin koko verkossa kaikilla työasemilla ja palvelimilla. Poisto oli valmis klo 23.02. Tämän jälkeen aloitettiin tietoverkon tietoturvan parantaminen, jotta palveluiden palauttaminen voitaisiin aloittaa tietoturvallisesti. Ensimmäiset verkkopalvelut sallittiin 15.6. aikana.

Haittaohjelman poisto aiheutti hyökkäyksen kohteeksi joutuneiden palvelinten ja työasemien uudelleen asennuksen. Palvelinten uudelleen asennus aiheutti palvelukatkon kaikissa saastuneissa palveluissa. Palveluiden palautus priorisoitiin suuren työmäärän vuoksi 16.6. Loppukäyttäjien työasemat

asennettiin uudelleen ja kaikki käyttäjät pakotettiin ohjelmallisesti vaihtamaan salasanat 27.6.2019. Ensimmäiset ulkoisiin verkkoihin suunnatut yhteydet avattiin 28.6.2019.

Haittaohjelma ei suorittanut mitään aktiivisia toimenpiteitä leviämisen ja hyökkääjän palvelimille pääsyn mahdollistamisen lisäksi työasemilla ja verkossa. Tämän vuoksi voitiin selvittää tietojärjestelmän lokitiedostoista, ettei verkosta todennäköisesti siirretty arkaluontoista tietoa verkon ulkopuolelle kuin pieniä määriä tai ei ollenkaan.

Lahden kaupunki oli varautunut tietojärjestelmän poikkeustilanteisiin harjoittelemalla toimintaa. Se perusti ohjeistuksensa mukaisesti tilannehuoneen johtamaan toimintaa 11.6. klo 20.00. Tilannehuone jatkoi toimintaa 28.6. saakka ja järjesti tilanteen johdon lisäksi kaupungin sisäisen ja ulkoisen tiedottamisen. Toiminta johdettiin aluksi tasatunnein pidettävissä kokouksissa ja myöhemmin määräajoin pidettävissä kokouksissa.

Hyökkäyksen selvittämiseen osallistui ensimmäisestä havainnosta saakka kaupungin tietohallinnon lisäksi palveluntuottajan Fujitsu Oy, joka myös dokumentoi tapahtumat. Ulkoisen tietoliikenneyhteyden toimittaja DNA, keskusrikospoliisi KRP ja viestintäviraston kyberturvallisuuskeskus osallistuivat toimintaan 11.6. kuluessa ja F-securen RED-ryhmä 12.6. alkaen.

Hyökkäyksen seurauksena noin 60 % (noin 2000kpl) Lahden kaupungin omistamista ja leasing-sopimuksella käyttämistä työasemista saastui ja jouduttiin uudelleen asentamaan. Osa työasemista korvattiin elinkaarivaihtona uuteen samassa yhteydessä. Kaikki saastuneet palvelimet jouduttiin asentamaan uudelleen ja tietokannat palauttamaan varmuuskopioista. Lisäksi tietoverkon asetuksia muutetiin tietoturvallisesti sekä palvelimilla että tietoa reitittävillä laitteilla ja palomuureissa.

Hyökkäys onnistui teknisesti järjestelmän puutteellisen konfiguraation vuoksi. Tähän liittyviä yksityiskohtia olivat muun muassa loppukäyttäjien työasemien etätyöpöytäratkaisun puutteellinen konfiguraatio, käyttäjien tunnusten hallinta mukaan lukien salasanapolitiikka sekä pääsynhallinnan puutteelliset kontrollit muun muassa palvelimilla ja palomuureissa.

Tietojärjestelmän ja -verkon osalta konfiguraatioita muutettiin hyökkäyksen jälkeen muun muassa seuraavien asioiden osalta:

- Tietoteknisen ympäristön koventaminen
  - Palvelinverkkojen eriyttäminen
  - Palvelimien ja palveluiden kirjautumiskäytäntöjen muuttaminen
  - Työasemien ohjelmistomuutokset (tietoturva, työasemapalomuuri)
- Tietoliikenneverkon turvallisuuden parantaminen
  - Tietoliikenneverkon eri osien eriyttäminen
  - Tietoliikenteen salliminen ainoastaan tarpeellisiin yhteyksiin
  - Palomuurisäännöstön läpikäynti ja kriittinen tarkastelu
  - Tietoliikenteen aktiivinen valvonta
- Käyttäjien kirjautumispalveluiden muutokset
  - Salasanojen vaihdon pakotus ja salasanapolitiikan muutos
  - Pilvipalveluiden kirjautumiskäytännön muutos

- Ympäristön valvonnan tehostaminen
  - Splunk, Microsoft Advanced Threat Analytics, F-secure Countercept

Kyberhyökkäyksestä aiheutui Lahden kaupungille joulukuun 2019 alkuun mennessä noin 900 000 € kustannukset, joista noin 600 000 € koostui ulkoisten toimittajien asiantuntijapalveluista. Loput kustannukset koostuvat muun muassa infrastruktuurin uusimisesta.

6.2.4 Muut havainnot

Hyökkäyksen tutkimuksissa selvisi, että hyökkääjä oli tunkeutunut verkkoon jo aiemmin ja jatkoi toimintaansa haittaohjelman asentamisen jälkeen. Varsinainen haittaohjelman leviämisen vuoksi hyökkääjä sai laajemman pääsyn tietoverkon eri osiin ja palvelimille.

Hyökkäyksen selvittämistä ja palveluiden palauttamista hidasti puutteellinen dokumentaatio. Tämän lisäksi dokumentaatiota puuttui merkittävästi ja järjestelmää ylläpitävillä ei ollut riittäviä tietoja järjestelmän rakenteesta tai konfiguraatiosta.

Tietoverkon varmentaminen varmuuskopioinnilla oli toteutettu riittävän hyvin, jotta palveluissa olevan tiedon palauttaminen onnistui eikä tieto menetetty. Huomioitavaa on kuitenkin, ettei esimerkiksi palvelinten levykuvia voitu käyttää sellaisenaan puutteellisten tietoturvakonfiguraatioiden vuoksi.

Lahden kaupunki valitsi tiedottamislinjaksi aluksi niukan tiedottamisen, koska hyökkäys oli aktiivisesti käynnissä. Linja muutettiin sen jälkeen, kun tietoverkon ulkoiset yhteydet suljettiin. Lisäksi myöhemmin kaupunki on tiedottanut asiasta avoimesti.

Tilannejohtaminen oli suunniteltu ja harjoiteltu, jonka vuoksi toiminnan johtaminen käynnistyi nopeasti ja määrätietoisesti. Tilanteen johtajaksi käskettiin tietohallintojohtaja, jolle annettiin suoraan päätösvalta resurssien käytöstä tapahtuman selvittämisessä. Sen sijaan hyökkäyksen laajuus ja ajallinen kesto huomioiden toimintaa ei ollut suunniteltu jatkuvaksi pitkälle aikavälille. Tämä aiheutti muun muassa työuupumusta tapahtuman aikana ja sen jälkeen.

Kolmannet osapuolet saatiin mukaan haittaohjelman selvittämiseen tunneissa myös paikanpäälle. Toimenpiteet dokumentoitiin kattavasti, joka helpotti tilanteen selvittämistä jälkikäteen.

Hyökkääjän motiivi ei selvinnyt tutkimuksissa. Haittaohjelma ei suorittanut mitään saastuneilla työasemilla eikä tietoja siirretty kaupungin tietoverkon ulkopuolelle merkittävästi tai ollenkaan. Haittaohjelman tarkoitus ei selvinnyt tutkimuksissa, mutta asiantuntijoiden keskusteluissa on noussut esille esimerkiksi kiristyshaittaohjelman (engl. ransomware) mahdollisuus.

6.2.5 Tietoturvapolitiikka hyökkäyksen jälkeen

Lahden kaupungin tietoturvapolitiikka ei ole uudistettu hyökkäyksen jälkeen virallisella asiakirjalla. Kaupunki on käynnistänyt tietoturvallisuuden arvioinnit sisäisesti ja ulkoisella toimijalla, joiden seurauksena tietoturvakokonaisuus on tutkimuksen aikana uudistumassa. (Monni, 2020)

6.3 Kokemäen kyberhyökkäys 29.7.2019

6.3.1 Tietoturvapolitiikan rakenne ennen hyökkäystä

Kokemäen kaupunki otti käyttöön tietoturvapolitiikan 1.1.2016. (Kokemäki, 2016) Kyseessä oli kaupungin ensimmäinen virallinen tietoturvapolitiikka. Tätä on edeltänyt tietohallinnon kokoelma ohjeista loppukäyttäjälle sekä ylläpitäjille, jota on ylläpidetty tietohallinnossa. Politiikka on käsitelty kaupungin johdossa yhteistoimintakunnassa ja kaupungin hallituksen henkilöstöjaostossa sekä hyväksytty käyttöön kaupungin hallituksessa. Kaupungilla ei ole erillistä tietoturvastrategiaa tai riskiarviota, joka olisi ohjannut politiikan muodostumista.

Tietoturvapolitiikka on 13 sivua pitkä ja rakenteellisesti kaksiosainen. Sen liitteenä on työntekijälle suunnattu lomake, jolla työntekijä kuittaa tekstin luetuksi ja ymmärretyksi.

Ensimmäisessä osassa ”A) Tietoturvapolitiikka” kuvataan tietoturvaa yleisesti. Se on luonteeltaan esittelevä ja kertoo muun muassa Kokemäen kaupungin tietoturvaan kuuluvien vastuiden jaosta. Osassa on tietoturvastrategiaan kuuluvia piirteitä.

Toisessa osassa ”B) Tietoturvaperiaatteet” käsitellään tietoturvaa konkreettisemmin ja se sisältää varsinaisen politiikan. Osan luku 4 on jaoteltu ISO27001 mukaiseen tietoturvan hallintajärjestelmän rakenteeseen, joista jokaisessa alaluvussa käsitellään kyseiseen osa-alueeseen liittyvät kokonaisuudet. Lisäksi osassa käsitellään seuraukset tietoturvan laiminlyönneistä ja väärinkäytöksistä.

6.3.2 Kokemäen tietoturvapolitiikan sisältö ennen hyökkäystä

Tietoturvapolitiikka on muodostettu 2015 työryhmätyöskentelynä, jossa kaupungin hallintojohtajan johdolla kaupungin eri hallinnon osat ovat osallistuneet politiikan muodostamiseen. (Löfbacka, 2020) Politiikka on lyhyt ja helposti ymmärrettävä. Se ei perustu tietoturvastrategiaan tai riskiarvioon, vaikka riskien hallinta mainitaan sen ensimmäisessä luvussa.

Politiikan ensimmäinen osa on muodoltaan strategian kaltainen. Se määrittelee strategiaan kuuluvia osa-alueita, mutta varsin laveasti eikä osin tietoturvakontekstissa. Sidosta kaupungin varsinaiseen strategiaan ei synny lukijalle.

Osassa esitellyt eri toimijoiden ja osastojen roolit, vastuut ja velvollisuuden tietoturvallisuuden toteuttamisessa sekä kehittämisessä. Roolit ovat selkeät ja sitoutuvat henkilöiden tehtävänimikkeisiin. Rooleissa on päällekkäisyyttä rooleissa ”osastopäällikkö” ja ”esimies”. Rooli ”kaikkien kaupungin tietoa käsittelevä” on epäselvä ja ulottaa vastuuta epämääriseen henkilöstöryhmään.

Ensimmäinen luku voisi olla nimetty sisältönsä mukaisesti tietoturvastrategiaksi ja sisältö muokata strategian kaltaiseksi ohjaavaksi kokonaisuudeksi.

Politiikan toinen osa sisältää varsinaisen politiikan. Sen alussa kuvaillaan tietoturvaa yleisesti sekä avataan keskeisiä käsitteitä. Sen jälkeen käsitellään kaupungin tiedon ja tietojärjestelmien käyttö ja siihen liittyvät oikeudet sekä tietoturvaosaamisen ylläpito. Loppu osassa käsitellään varsinainen politiikka eli toimintaa ohjaavat ja rajaavat kokonaisuudet ISO27001 tietoturvan hallintajärjestelmän rakenteessa. Jokainen alilukuu alkaa sen kuvauksella ja sisältää alilukuun kuuluvat politiikkalinjaukset.

Toinen osa on sisällöltään sekä politiikan ja käytäntöjen sekoitus. Se selkeästi linjaa politiikkaan kuuluvia kokonaisuuksia, mutta ohjeistaa samalla loppukäyttäjää. Lopputulos voi sekoittaa erityisesti peruskäyttäjää, joille ylemmän tasoiset politiikkalinjaukset eivät konkreettisesti tarkoita mitään.

Politiikasta puuttuu seuraavia osia, joilla voi olla merkitystä tietoverkon häiriötilanteiden selvittämisessä ja palautumisessa:

- Politiikka ei käske mittareita tietoturvatason mittaamiseksi ja vertailtavuuden parantamiseksi
- Tietoturvan tason arviointia ei määritetä
- Toimintaa poikkeustilanteissa ei ohjeisteta ylläpitäjille ja loppukäyttäjille
- Palvelutuotannon tukea ei määritellä.

6.3.3 Kyberhyökkäys 29.7.2019

Tämän luvun teksti perustuu tutkijan haastatteluihin 29.9.2020 sekä erikseen viitattuihin artikkeleihin ja uutisiin. Haastateltavina olivat Aki Ketonen, joka toimii Kokemäen kaupungin tietohallintopäällikkönä sekä Mikko Löfbacka, joka toimi tapahtuma aikana Kokemäen kaupungin hallintojohtajana. Haastattelumateriaali on tutkijan hallussa.

Kokemäen kaupungin tietoverkkoa käytetään kaupungin asioiden hoitamiseen sisäisesti ja ulkoisesti. Sen käyttäjinä toimi mm. sivistystoimi, koulutoimi, terveyden huolto sekä kaupungin hallinto ja kaupungin keskeisen infrastruktuurin palvelut kuten vesilaitos. Tietoverkko oli segmentoitu vähintään kolmeen osaan ja sisäverkko oli eroteltu ulkoverkosta palomuurilla. Verkossa oli noin 200 työasemaa sekä palvelutuotantoon tarvitut palvelimet. Tietoverkon ylläpito oli toteutettu yhteistyössä 3. osapuolen kaupallisen toimijan kanssa.

Kokemäen kaupungin tietojärjestelmiin kohdistunut kyberhyökkäys havaittiin maanantaina 29.7.2019 aamulla. Ensimmäiset viitteet hyökkäyksestä teki Aki Ketonen. Hyökkäyksen kohteeksi oli joutunut verkkosegmentti, johon

kuului kaupungin hallinto sekä muun muassa vesilaitos. Hyökkäys ei levinnyt kahteen muuhun segmenttiin, joissa toimi muun muassa terveydenhuolto sekä koulutoimi.

Kyberhyökkäys toteutettiin kiristyshaittaohjelmalla. Kiristyshaittaohjelma (engl. ransomware) on haittaohjelma, joka salaa kohteen tiedostoja ja vaatii käyttäjältä lunnaita tietojen purkamisesta. (Stallings & Brown, 2018) Tämän tyyppisiä hyökkäyksiä on tehty muun muassa Windows 95 ja 98 käyttöjärjestelmiä vastaan (Chernobyl-virus) ja Ukrainassa sähköjakelujärjestelmään kohdistuneen hyökkäyksen osana. (Stallings & Brown, 2018) (Boozallen, 2016)

Hyökkäys kohdistui tietoverkossa käynnissä tai käynnistyneisiin päätelaitteisiin ja virtuaalikoneisiin salaten niiden tiedostojärjestelmän ja antamalla käyttäjälle ilmoituksen lunnaiden maksamisesta. Näiden päätelaitteiden käyttö estyi täysin. Sellaiset päätelaitteet, jotka eivät olleet käynnissä tai palvelinten tietokannat, jotka olivat ajossa eivät saastuneet. Haittaohjelma levisi saastuneessa verkkosegmentissä, mutta ei levinnyt muihin segmentteihin.

Kokemäen kaupungin tietohallinto käynnisti toimenpiteet haittaohjelman leviämisen estämiseksi. Näitä olivat muun muassa saastuneen verkon eristäminen muusta verkosta, saastuneiden työasemien kartoittaminen ja käyttäjien ohjeistaminen, jotta lisää työasemia ei käynnistetä saastuneeseen verkkoon. Työhön osallistui tietoverkon hallintaan osallistunut 3. osapuoli sekä Kyberturvallisuuskeskus sekä Porin poliisi.

Kokemäen hallintojohtaja Mikko Löfbacka toimi loma-aikana kaupunginjohtajan sijaisena ja vastasi viestinnästä sisäisesti ja ulkoisesti. Hän sai tiedon hyökkäyksestä 27.9.2019 noin kello 12 ja aloitti toimenpiteet kyberturvallisuuskeskuksen ja poliisin kanssa.

27.9.2020 illalla tietoverkon tilanne oli stabiili. Haittaohjelma ei levinnyt 29.7.2019 jälkeen uusiin kohteisiin. Saastuneita työasemia oli 10 kappaletta ja palvelimilla saastuneita tietokantoja useita. Saastuneen tietoverkkosegmentin toiminta oli pysäytetty ja haittaohjelman etsintä sekä poistaminen aloitettu.

Järjestelmän palautus aloitettiin vaiheittain 30.–31.7. ja kriittiset palvelut nostettiin takaisin palvelutuotantoon 1.–2.8. Koko verkon palvelut oli palautettu 7.8.2019 niiltä osin, kuin tieto oli saatu palautettua. Palautuksen aikana havaittiin, että tietoverkon dokumentaatio ollut ajan tasalla ja käyttöhenkilöstöllä ei ollut riittävää osaamista kaikista verkon osista.

Kyberhyökkäyksestä aiheutui suoraan noin 25 000 € kulut sekä välillisesti tietoturvan parantamiseen liittyen tapahtuman jälkeen 75 000 € kustannukset. Tämä kustannus ei ole suoraa seurausta kyberhyökkäyksestä vaan lisääntyneen ymmärryksen takia tapahtunut suunniteltu budjetin kasvattaminen.

Käytettyjen henkilöstöresurssien määrää ei ole laskettu. Arviolta 5–10 henkilöä eri organisaatioista sitoutui täydellä työajalla haittaohjelman alkuperän selvittämiseen, järjestelmän uudelleen asennuksiin ja palvelutuotantoon nostoon noin 10 työpäivän ajan. Yhteensä resursseja käytettiin siis 50–100 henkilötyöpäivää, joskin luku voi olla liian pieni.

Tietoverkkoon kytkettynä ja päällä olleista työasemista saastui 10 kappaletta. Näillä koneilla olleita tietoja ei saatu palautettua. Päätelaitteet hylättiin tapahtuman jälkeen ja tilalle hankittiin uudet, sillä laitteet olivat vanhentuneita.

Useita virtuaalipalvelimia ja niissä ajossa olleita tietokantoja saastui. Palvelimilla olleita tietoja saatiin palautettu, mutta osa varmuuskopioista oli vanhoja. Joitain viimeisimpiä tietoja esimerkiksi vesilaitoksen järjestelmästä menetettiin pysyvästi. Virtuaalikoneet jouduttiin asentamaan uudelleen, mutta fyysisiä laitteita ei jouduttu uusimaan.

Viitteitä siitä, että tietoa olisi viety tietoverkosta ei ole. Tämä ei tarkoita sitä, etteikö tietoa olisi voitu viedä, mutta sitä ei jälkikäteen voitu todeta.

Saastunut verkkosegmentti tietoineen oli pois käytöstä noin 9 työpäivää. Tämä esti osin tässä verkkosegmentissä työskennelleiden henkilöiden työn tai aiheutti siihen merkittäviä muutoksia. Muun muassa järjestelmän sähköposti oli pois käytöstä, jolloin tiedottamista hoidettiin yksityishenkilöiden omista sähköpostiosoitteista.

Tietoverkon ylläpidon näkökulmasta hyökkäys aiheutti muutoksia tietoverkon dokumentointiin, varmuuskopiointiin, käyttövaltuushallinnan dokumentointiin, loppukäyttäjän ohjeisiin sekä ylläpidon yleisiin järjestelyihin.

6.3.4 Muut havainnot ja seuraukset

Tietoverkkoon tunkeutumisreitti ei selvinnyt tutkimuksissa. Mahdollisia reittejä olivat ainakin sähköposti sekä sisä- ja ulkoverkon välinen palomuuri. Selvittämistä hankaloitti puutteellinen tai tuhoutunut lokitieto.

Saastuneen järjestelmän erottamista muusta verkosta sekä palauttamista hidasti verkon puutteellinen dokumentointi, yksilöiden rajallinen tieto verkon rakenteesta sekä yksittäisiin henkilöihin keskittynyt osaaminen. Osittain hyvällä onnella hyökkäyksen aikaan keskeisen osaamisen omaava henkilöstö oli saatavilla.

Tietoverkon varmentaminen oli toteutettu osin puutteellisesti. Kaikkia varmuuskopioita ei saatu palautettua ja osan palauttamiseen jouduttiin käyttämään poikkeavia menettelyitä, jotka eivät aiheutuneet varsinaisesta kyberhyökkäyksestä.

Hallintojohtaja Löfbacka valitsi aktiivisen ja avoimen tiedottamisen tiedottamisstrategiaksi. Tämä sitoi henkilöstöä tiedottamiseen, joka ei kuitenkaan ollut pois ongelman selvittämisestä. Tiedottaminen aloitettiin tiistaina 30.7., jolloin asiasta annettiin lehdistötiedote ja ensimmäinen toimittaja soitti hallintojohtajalle.

Tapahtuma ajoittui lomakaudelle, jolloin muun muassa kaupunginhallitus kutsuttiin koolle loma-aikana. Kaupungin tietohallintopäällikkö ja hallintojohtaja sitoutuivat tapahtuman hoitamiseen, jolla on ollut vaikutusta muun päivittäisen toiminnan johtamiseen.

Tapahtuman aikana yhteydenpito kaupungin hallinnon sisällä, kyberturvallisuuskeskuksen, poliisin ja median kanssa oli päivittäistä. Asioita

sovittiin kasvotusten, puhelimitse ja verkkotapaamisissa. Lisäksi kaupunki tiedotti asiasta sovituin määräajoin.

Hyökkäyksestä palautumiseen liittyen tehtiin riskiarvion perusteella päätös, että järjestelmä nostetaan ylös vaikka kaikkia sen osia ei ollut asennettu uudelleen. Päätös nopeutti palautumista, mutta toisaalta olisi voinut johtaa ylimääräiseen työhön.

6.3.5 Tietoturvapolitiikka kyberhyökkäyksen jälkeen

Kokemäen kaupunki päivitti tietoturvapolitiikan kyberhyökkäyksen jälkeen ja otti sen käyttöön 1.1.2020 otsikolla ”Kokemäen kaupungin ja konserniyhtiöiden tietosuoja- ja tietoturvaperiaatteet ja yleiset toimintaohjeet”. Tietoturvapolitiikka on valmisteltu kaupungin tietosuojavaltuutetun toimenpitein ja lausuttu eri toimijoilla ennen käyttöönottoa. Kaupungilla ei edelleenkään ole erillistä tietoturvastrategiaa tai riskianalyysiä, johon politiikka perustuisi.

Tietoturvapolitiikka on 30-sivuinen ja sisältää rakenteellisesti viisi lukua. Aiemmassa politiikassa liitteenä ollutta kuittauslomaketta ei ole enää sisällytetty osaksi politiikkaa.

Ensimmäinen luku on johdanto asiakirjan sisältöön. Toinen luku sisältää tietosuojan yleiset periaatteet, käsitteet ja vastuut sekä siihen liittyvän lainsäädännön. Kolmannessa osassa käsitellään tietosuojan politiikka- ja ylläpitäjä sekä loppukäyttäjäntason ohjeet. Neljäs luku on sama kuin vuoden 2016 politiikan toinen osa. Viiden luku sisältää tietoturvaan liittyvät loppukäyttäjän ohjeet. Kokonaisuudessaan varsinainen tietoturvaosuus ei ole muuttunut.

7 TULOKSET JA POHDINTA

Tässä luvussa esitellään tutkimuksen tulokset tapaustutkimusten osalta sekä pohdinta tulosten pohjalta. Tulokset esitellään vertailuna referenssikaupunkeihin sekä arviona tietoturvapolitiikan vaikuttavuudesta kohdattuihin kyberhyökkäyksiin.

7.1 Tietoturvapolitiikan vertailu referensseihin

Tutkimuksen kohteena olleet Lahti ja Kokemäki sekä referenssinä olleet Espoo ja Virrat ovat tuottaneet tietoturvan parantamiseksi tietoturvapolitiikat. Lahden kaupungin asiakirja on nimetty muista poikkeavasti, vaikka keskeinen sisältö on sama. Tutkittujen kyberhyökkäysten aikana 2019 Espoon ja Virtojen politiikka sisälsi myös tietosuojaan liittyviä osia, jotka eivät ole tämän tutkimuksen kannalta merkityksellisiä.

Kaikkien tutkittujen kaupunkien tietoturvapolitiikat muistuttavat sekä tietoturvastrategiaa, että tietoturvapolitiikka, joskin ne ovat enemmän politiikkaan painottuvia. Strategian näkökulmasta niissä esitetään löyhästi visio ja missio sekä kuvataan resurssit. Politiikan näkökulmasta niissä esitellään tietoturvan toiminta-ajatus, tavoitteet ja organisaation sitoutuminen. Tutkituissa asiakirjoissa ei kuitenkaan esitellä tietoturvan hallintajärjestelmää. Jokainen politiikka on kirjallinen ja organisaation sekä sidosryhmien julkisesti saatavilla.

Lahden ja Espoon tietoturvapolitiikat ovat keskeisiltä osilta samanlaiset, kun Espoon kaupungin politiikkaan sisältyvää tietosuojaosuutta ei huomioida. Lahden kaupungin voimassa ollut politiikka oli vuodelta 2011, joskaan se ei näy sisällössä vertailtuna Espoon vuoden 2018 politiikkaan. Molemmissa kuvataan tietoturvan merkitys kaupungin toiminnalle ja sen jatkuvuudelle. Molempien lähtökohtana on riskienhallinta ja niissä kuvataan tietoturvaan liittyvät toimijat sekä niihin liittyvät vastuut. Espoon vastuukuvaukset ovat laajempia, mutta Lahden kaupungin politiikassa vastuita luetellaan lisää luvussa 4 ”Turvallisuuden järjestämistä ohjaavat periaatteet”. Lahden kaupunkia vastaan tehdyn kyberhyökkäyksen näkökulmasta Espoon kaupungin tietoturvapolitiikka ei tarjoa merkittäviä eroja hyökkäyksen torjuntaan.

Kokemäen ja Virtain kaupungin tietoturva politiikat ovat rakenteellisesti erilaiset. Virtain kaupungin politiikka muistuttaa rakenteeltaan ja sisällöltään Lahden ja Espoon vastaavia, kun Kokemäen politiikka on karkeasti ISO27000-standardin mukaisessa rakenteessa. Samoin sisällöllisesti Kokemäen politiikka on rakenteensa vuoksi politiikkana täydellisempi tietoturvan hallintajärjestelmän näkökulmasta. Siinä on muita enemmän konkreettisia rajauksia ja linjauksia tietoturvan toteuttamiseksi. Kokemäen kaupunkia vastaan tehdyn kyberhyökkäyksen näkökulmasta Kokemäen tietoturvapolitiikka tarjoaa enemmän konkreettisia linjauksia kuin Virtain kaupungin politiikka.

7.2 Tietoturvapolitiikan vaikutus kyberhyökkäyksen torjuntaan

7.2.1 Arvio tietoturvapolitiikan vaikutuksesta kyberhyökkäyksen onnistumiseen, Lahti

Hyökkäyksen onnistumista tietoturvastrategian näkökulmasta ei voida arvioida, koska sellaista ei ollut. Tietoturvapolitiikan osalta arvio tehdään vuoden 2011 ”Tietoturvan hoidon periaatteet” asiakirjan pohjalta. Arvio on tutkimuksen viitekehyksessä ISO27000-standardin rakenteessa. Hyökkäyksen onnistumisen kannalta keskeinen syy suunnittelun tasolla oli puuttuva tietoturvastrategia ja puutteellinen tietoturvapolitiikka, jonka vuoksi tietojärjestelmän konfiguraatio ei ollut tietoturvallinen.

Kokonaisuudessaan politiikka oli yhdistelmä strategiaa, politiikkaa ja loppukäyttäjän ohjeita. Se ei kuitenkaan muodostanut selkeästi mitään näistä. Se oli kirjoitettu loppukäyttäjille, jolloin merkittävä osa sen laajuudesta koostui tietoturvaa kuvaavista ja selvittävistä osuuksista. Strategiset linjaukset olivat hajanaisia ja muun muassa tietoturvan kehittämiseen soveltuvaa mittaristoa ei käsketty. Politiikan kannalta siinä ei ollut tunnistettavissa minkään viitekehyksen rakennetta eikä tietosisältö ollut organisoitu viitekehysten mukaisesti.

Strategisten linjausten osalta kyberhyökkäystä estävinä tai hidastavina linjauksina voidaan pitää tietoturvan organisointia, tavoitteita ja tarkoitusta. Organisointia voidaan pitää myös osana resursointia.

Hallinnollisen tietoturvan osa-alueen osalta tietoturvan toimijat, vastuut ja tehtävät olivat jaettu. Tämä oli kuitenkin osin epämääräinen, jolloin suurin osa työstä oli osoitettu tietoturvaryhmälle. Tietoturvaryhmä oli kuitenkin varsin suuri ja koostui lähinnä eri toimialojen johtajista. Sen toimintakyky oli heikko eikä se tuottanut politiikan vaatimia käytännön tason ohjeita tai ylemmän tason poliittisia linjauksia. Lisäksi hallinnollisen tietoturvan linjaukset eivät kattaneet muun muassa tiedon käsittelyyn liittyviä asioita ja dokumentointia.

Politiikka ei ota kantaa fyysiseen, laitteistojen, ohjelmistojen tai tietoliikenteen tietoturvaan. Hyökkäyksen näkökulmasta muun muassa etätyöpöytäarkkitehtuuri, salasanapolitiikka ja käyttäjähallinta puuttui politiikasta. Vaikka siinä ei mainittu myöskään varmentamista, haittaohjelmistoihin ja tietoliikenteen turvallisuuteen liittyviä yksityiskohtia, ne oli hoidettu ohjeistamalla erikseen ja edistivät hyökkäyksen selvittämistä.

Tietoaineiston turvallisuudesta löytyy mainintoja muun muassa sen käsittelyn ja säilytyksen osalta. Niissä ei kuitenkaan rajata tai käsketä toteutukseen liittyviä reunaehtoja tai rajoitteita.

Henkilöturvallisuuden osalta jokainen kaupungin työntekijä tunnistetaan osaksi tietoturvaa. Poikkeustilanteiden toimintaa tai ilmoitusmenettelyitä ei kuvata, vaikka ne mainitaan. Poikkeustilanteiden toiminta on kuvattu kaupungin varautumiseen liittyvissä dokumenteissa.

Viitekehyksessä mainituista muista kokonaisuuksista voidaan todeta, ettei tietoturvan kehitystä ollut sidottu vuosittaiseen prosessiin, siitä annettavaa raportointia ei ollut määritelty vastuuorganisaatioita pidemmälle eikä tietoturvan kehittämiseen otettu kantaa.

Asiakirjan rakenne ei noudattele tutkittuja valtionhallinnon esimerkkirakenteita tai tietoturvan hallintajärjestelmien rakennetta eikä sen sisältö vastaa niitä.

7.2.2 Arvio tietoturvapolitiikan vaikutuksesta kyberhyökkäyksen onnistumiseen, Kokemäki

Hyökkäyksen onnistumista tietoturvastrategian näkökulmasta ei voida arvioida, koska sellaista ei ollut. Tietoturvapolitiikan osalta arvio tehdään vuoden 2016 ” Kokemäen kaupungin henkilöstön tietoturvapolitiikka ja -periaatteet” asiakirjan pohjalta. Arvio on tutkimuksen viitekehyksen ISO27000 mukaisessa järjestyksessä. Hyökkäyksen onnistumisen kannalta keskeinen syy puuttuva tietoturvastrategia ja puutteellinen tietoturvapolitiikka, jonka vuoksi tietojärjestelmän konfiguraatio ei ollut tietoturvallinen.

Kokonaisuudessaan politiikka oli yhdistelmä strategiaa, politiikkaa ja loppukäyttäjän ohjeita mukaan lukien kuittaussivu. Se on sisällöllisesti suunnattu loppukäyttäjille ja strategian ja politiikan tasolla kyberhyökkäyksen ehkäisyyn, torjuntaan ja siitä palautumisen liittyviä asioita on jonkin verran. Osa asioista ei ole suoraan suojautumiseen liittyviä, mutta niiden johdosta tehdyt toimenpiteet ovat joko hidastaneet hyökkäystä tai nopeuttaneet palautumista.

Strategisen varautumisen osalta tietoturvan kehittämiseen liittyviä toimenpiteitä ja mittareita ei ole käsketty. Sen sijaan tietoturva sidotaan laatuun ja työn onnistumiseen. Tietoturvaan liittyvä raportointi on käsketty ylimalkaisesti, joka on johtanut reagoivaan raportointiin. Kyberhyökkäyksen torjuntaan liittyvä strategisina linjauksina voidaan pitää myös tietoturvan tavoitteita, tarkoitus ja organisointia. Verrattuna Lahden vastaavaan organisointiin, Kokemäellä ei käsketä suoraan tehtäviä vastuullisille toimijoille.

Varsinainen politiikka on viitekehyksen ISO27001 rakenteen mukainen, jolloin sen vertailtavuus ja mitattavuus on samaa viitekehystä toteuttavien toimijoiden kanssa helppoa. Näillä on vaikutus tietoturvan kehittämiseen sekä toteuttamiseen ja välillisesti myös kyberhyökkäyksen torjuntaan ja siitä palautumiseen.

Hallinnollisen tietoturvan osalta politiikka käskee toimijat, koulutuksen, vastuut ja valvonnan sekä käyttöoikeudet. Se ottaa kantaa tiedon ja koulutusmateriaalin säilyttämiseen. Tietohallinnon osalta järjestelmään kerääntyvään tietoon tai sen seurantaan ei oteta kantaa. Tapahtuneessa hyökkäyksessä tällä olisi ollut merkitystä sekä palautumisen että tapauksen selvittämisen osalta. Näiden lisäksi järjestelmän dokumentointia ei mainita, joka on vaikuttanut hyökkäyksestä palautumiseen.

Fyysiseen tietoturvaan otetaan kantaa, mutta tässä tapauksessa fyysisellä tietoturvalla ei ole ollut merkitystä hyökkäykseen varautumisessa tai siitä

palautuessa, ellei hallinnollisessa tietoturvassa mainittua dokumentointia oteta huomioon.

Laitteiston tietoturvan osalta politiikan linjaukset ovat edesauttaneet kyberhyökkäyksen torjuntaa ja siitä palautumista. Laitteistojen päivitys mainitaan erikseen, joka toteutuessaan parantaa tietoturvaa ja auttaa kyberuhkiin varautuessa. Tutkitussa kyberhyökkäyksessä laitteistoturvallisuudella ja ohjelmistoturvallisuudella on ollut osa-alueista suurin merkitys hyökkääjälle hyökkäyksen onnistumisessa.

Ohjelmistojen tietoturvallisuuden osalta politiikka erityisesti käyttäjähallinnalla on ollut merkitystä sekä hyökkäyksen torjunnassa että siitä palautumisessa. Sen sijaan puutteelliset linjaukset vastuissa, dokumentoinnissa, seurannassa ja osaamisessa ovat aikaansaaneet hyökkääjälle mahdollisuuden hyökätä ja hidastaneet hyökkäyksen selvittämistä sekä siitä palautumista.

Tietoaineistojen käsittelyn osalta politiikassa ei ole tietovarantojen käsittelyyn liittyvää politiikkaa, johon kuuluisi muun muassa tiedon määrään, laatuun ja lokittamiseen liittyvät määritykset. Sen sijaan varmuuskopiointi on mainittu ja sillä on ollut merkittävä osuus palautumiseen kuluneen ajan käytössä. Vaikka varmentamiseen liittyen ei käsketty kuin vastuu, on vastuuseen käsketty tietohallinto toteuttanut sen riittävän laajasti palautumisen näkökulmasta suhteessa tutkittuun hyökkäykseen. Menetetyn tiedon määrä on pysynyt pienenä suhteessa onnistuneeseen kiristyshaittaohjelmahyökkäykseen.

Tietoliikenteen tietoturvaan on otettu kantaa osa-alueista vähiten. Politiikka ei ota kantaa tietoliikenteen valvontaa, lokitukseen sekä valvontaan liittyviin vastuisiin. Näillä on ollut kriittinen rooli hyökkäyksen onnistumisessa tutkitussa tapauksessa.

Henkilötietoturvaa ei osa-alueena ole erikseen vaan sen tilalla käyttöturvallisuus. Politiikassa otetaan kantaa käyttöoikeuksien hallintaan ja dokumentointiin, ulkoistamiseen muiden kuin tietojärjestelmien kehittämisen ja käyttöönottamiseen liittyvät tietoturvaelementit. Näillä on ollut positiivinen vaikutus hyökkäyksestä palautumisessa.

Muina huomioina politiikasta voidaan todeta, että tietoverkon segmentointi on merkittävästi pienentänyt hyökkäyksen eskalaatiota tietoverkossa ja mahdollistanut kaupungin palveluiden osittaisen käyttämisen myös hyökkäyksen vaikutuksen aikana. Segmentointia ei kuitenkaan erikseen mainita politiikassa.

Politiikka sisältää järjestelmän väärinkäyttöön liittyvät ohjeet sekä sanktiot ja loppukäyttäjän allekirjoituslomakkeen. Näillä ei ole ollut merkitystä tutkitussa tapauksessa.

Politiikka ei sisällä tietoturvan kehittämiseen liittyviä kokonaisuuksia, kuten mittareita, vuosikelloa tai tapaa tuoda muutokset osaksi politiikkaa. Näillä on voinut olla merkitystä kyberhyökkäyksen torjunnassa, sillä politiikka on ollut yli 3 vuotta vanha, kun varsinainen hyökkäys tapahtui. Tämä arvio ei ota huomioon tietoturvaohjeissa tapahtunutta kehitystä kyseessä olevana aikana.

7.3 Tulokset

Tutkimuksessa selvitettiin, mikä on tietoturvastrategia ja -politiikka yleisellä tasolla sekä Suomessa valtionhallinnossa. Tuloksena on, että nämä on määritelty Suomessa varsin kattavasti ja tietoturvapolitiikan osalta on luotu esimerkkirakenteita eri julkisten toimijoiden käyttöön. Nämä rakenteet noudattelevat ISO27000-standardisarjassa määriteltyä tietoturvallisuuden hallintajärjestelmän rakennetta löyhästi. Standardia voidaan siis soveltaa valtionhallinnon ohjauksen pohjalta varsin helposti rakenteiden osalta.

Suomessa tietoturvallisuuden valtiollinen ohjaus on kattava ja lainsäädäntöä, säädöksiä ja päätöksiä tietoturvallisuuden toteuttamiseen on paljon. Tietoturvallisuuden tekijöiden näkökulmasta tietoturvaan liittyviä asioita löytyy erittäin monesta asiakirjasta ja kaikkien asioiden tunnistaminen on erittäin hankalaa. Tutkimuksessa selvisi, että yhdenkään tutkitun kunnan tietoturvapolitiikassa luetellut lainsäädännölliset lähteet eivät vastaa tutkimuksessa löydettyihin asiakirjoihin tai VAHTI-ohjeiden määrittämään luetteloon. Voidaan todeta, että tietoturvapolitiikan tekijällä tulee olla merkittävästi ammattitaitoa, jotta hän pystyy ottamaan huomioon kaikki voimassa olevat laita, asetukset ja säädöksen huomioon politiikan muodostamisessa.

Tietoturvallisuuden hallintajärjestelmiä ja niihin verrattavia viitekehyksiä on useita. Tutkimuksen viitekehykseksi valittu ISO27000-standardisarja on viitekehyksenä laaja ja siitä löytyy paljon perusteita tietoturvallisuuden kehittämiseksi missä tahansa organisaatiossa. Se soveltuu käyttöön valtionhallintoon. Nykyinen valtionhallinnon ohjaus noudattelee siinä esiteltyä rakennetta ja se on sellaisenaan sovellettavissa erikokoisiin kuntiin. Standardin käyttö ei edellytä turvallisuuden auditointia, mutta ulkoisella ja sisäisellä auditoinnilla parannetaan tietoturvallisuutta syklisesti jatkuvan parantamisen periaatteilla.

Tutkimuksen varsinaisiin tutkimuskysymyksiin löydettiin vastauksia, joskin niiden kattavuutta ja yleistettävyyttä on arvioita kriittisesti. Referensseihin verrattuna vain Kokemäen tietoturvapolitiikka oli selkeästi rakenteellisesti, että sisällöllisesti erilainen kuin muiden. Silti yhdenkään tutkitun kaupungin politiikka ei vastannut valtionhallinnon esimerkkirakenteita tai ISO27000-standardisarjassa esitettyä rakennetta.

Lahden ja Kokemäen tietoturvapolitiikka vaikutti kyberhyökkäyksiin sekä positiivisesti mahdollistamalla hyökkäyksen että negatiivisesti estämällä sen laajentumista ja nopeuttamalla palautumista. Molempien kaupunkien osalta politiikassa ei ollut riittävästi pohdittu kaupunkien tietoturvallisuuden tilaa, kehitystä, resursointi, mittaamista ja resursointia suhteessa uhkaan. Sen sijaan vastuut oli määritelty hyvin ja tietoturvallisuuden tavoite ja merkitys oli selkeästi näkyvillä.

Tulosten perusteella voidaan todeta, että erityisesti Kokemäen voimassa ollut tietoturvapolitiikka vaikutti kyberhyökkäyksestä palautumiseen. Politiikka oli muodostettu osin VAHTI-ohjeen 4/2007 esimerkkirakenteiden mukaisesti ja

sillä vastattiin moniin sellaisiin yksityiskohtiin, joilla hyökkäyksestä palautuminen nopeutui. Silti tämäkään tietoturvapolitiikka ei ollut itsessään kattava.

Lahden tietoturvapolitiikka oli itsessään kuntapolitiikan tulos nimensä puolesta. Sitä ei nimetty tietoturvapolitiikaksi poliittisessa päätöksenteossa. Tällä ei ollut merkitystä lopputuloksen kannalta. Politiikka oli yleisellä tasolla määritelty ja siinä otettiin kantaa tietoturvapolitiikkaan liian pintapuolisesti hyökkäyksen torjunnan, rajaamisen ja siitä palautumisen näkökulmasta.

Espoon ja Virtain kaupungin politiikat olivat hyvin Lahden kaupungin kaltaiset. Niillä on vaikutusta kaupunkien kyberturvallisuuteen, mutta niitä ei voi vielä tutkia tässä viitekehyksessä, koska onnistunutta ja havaittua kyberhyökkäystä ei ole vielä tapahtunut.

Lahden ja Kokemäen kaupunkien tietoturvapolitiikka ei ole tutkimuksen tekohetkellä olennaisesti muuttuneet. Lahden kaupunki käynnisti laajan tietoturvallisuuden selvityksen hyökkäyksen jälkeen ja on saanut ulkopuoliselta toimijalta raportin tietoturvallisuuden tilasta. Tämä ei ole vielä vaikuttanut voimassa olevaan politiikkaan. Kokemäen tietoturvapolitiikka on uudistunut hyökkäyksen jälkeen, mutta muutokset koskevat suurimmalta osin tietosuojaa.

8 YHTEENVETO

Tutkimuksen tarkoituksena oli selvittää, onko kuntien tietoturvastrategialla ja -politiikalla merkitystä kyberhyökkäyksen torjunnassa, rajaamisessa sekä siitä palautumisessa. Tutkimuskohteeksi valittiin kaksi lähivuosina tapahtunutta onnistunutta kyberhyökkäystä, joista oli uutisoitu julkisuudessa ja niissä toiminut tietoturvahenkilöstö oli edelleen tehtävissään. Tapausten referensseiksi valittiin kaksi samankokoista kuntaa tietoturvapolitiikan osalta.

Kyberhyökkäyksiä tutkittaessa selvisi, että molempien kaupunkien tietoturvassa oli merkittäviä puutteita sekä teknisesti että toiminnallisesti. Tämä havainto ohjasi tutkimuksen kohteeksi tietoturvastrategian ja -politiikan merkityksen kyseissä kyberhyökkäysten torjunnassa. Valittu tutkimusasetelma osoittautui erittäin tutkittavaksi sekä aineiston määrän että tutkittavan materiaalin laadun vuoksi.

Tutkimuksessa oli tarkoitus selvittää, miten käytössä ollut tietoturvastrategia ja -politiikka vaikuttaa kyberhyökkäyksen torjuntaan. Asetelmassa kyberhyökkäys oli onnistunut kyberhyökkäys, sillä sen tutkimiseksi on saatavissa enemmän aineistoa. Epäonnistuneen hyökkäyksen tutkiminen olisi ollut tutkimuksen kannalta yhtä mielenkiintoista, mutta käytännössä materiaalin puuttumisen vuoksi mahdotonta. Lisäksi on huomioitava, ettei yhdelläkään tutkituista kunnista ollut tietoturvastrategiaa, jolloin tutkimus pohjautui tietoturvapolitiikan tutkimukseen.

Tietoturvastrategiaa ei ole yksiselitteisesti määritelty. Vaikka akateemisesti tällä on suuri merkitys, tietoturvallisuuden toteuttamisen kannalta asialla ei vaikuta olevan suurta merkitystä. Sen sijaan merkittävää on, ettei yksikään kohdeorganisaatio ollut tehnyt erillistä tietoturvastrategiaa ohjaamaan ja resursoimaan tietoturvan toteuttamista. Kaikissa kohdeorganisaatioissa oli päädytty ratkaisuun, jossa tietoturvapolitiikkaan oli kirjoitettu sisälle strategiatyyppiset linjaukset. Ratkaisua ei voi aineiston perusteella pitää vääränä, mutta sen edellytyksenä on, että varsinaiset politiikkaan kuuluvat linjaukset tulee myös tehtyä ja dokumentoitua. Näin ei ollut tapahtunut kuin Kokemäellä, joskaan sielläkään linjaukset eivät olleet riittävät.

Tietoturvapolitiikka voidaan tutkimuksen perusteella käsittää kunnissa sekä strategian, politiikan että käytäntöjen kaltaiseksi dokumentiksi tai näiden yhdistelmäksi. Tämä on ymmärrettävää, kun tarkastelee tietoturvasta säädettyjä lakeja ja asetuksia sekä kirjoitettuja julkishallinnon ohjeita. Konkreettista esimerkkiä ei tutkitusta materiaalista löytynyt ja tämä haastatteluiden perusteella hankaloittaa merkittävästi tietoturvasta vastaavien työtä.

Tietoturvapolitiikka muodostetaan kunnissa kuten muutkin kuntien toimintaa ohjaavat asiakirjat ja ne hyväksyy kunnan hallitus. Menettely takaa, että dokumentit tulee tehtyä mutta ei takaa niiden laatua. Pääosin dokumenttien laatu perustuu kyseisen kunnan henkilökunnan osaamiseen eikä sen arviointiin todennäköisesti riitä kunnissa ammattitaito. Kuntien välinen vertailu vaikuttaa hyvältä mutta myös samalla ainoalta keinolta parantaa tietoturvapolitiikkaa.

Lahdessa politiikassa oli kuitenkin mainittu ulkopuolinen auditointi tai tietoturvan tarkastus, mutta sitä ei ollut toteutettu. Tämä on ymmärrettävää huomioiden käytössä olleet resurssit, mutta toisaalta huomioiden seuraukset, huono päätös.

Tutkittujen kuntien tietoturvapolitiikat olivat Espoon, Lahden ja Virtojen osalta lähes samanlaiset. Niiden rakenne ja sisältö muistutti toisiaan. Kokemäen politiikka erosi näistä merkittävästi ja muistutti eniten tietoturvapolitiikkaa. Sitäkään ei voi pitää kattavana. Tutkimuksessa ei selvitetty politiikan perusteella muodostettua muuta kirjallista materiaalia ja on mahdollista, että ne kattavat varsinaisen politiikan puutteet. Haastatteluiden perusteella voi kuitenkin päätellä, ettei kattavuus ole esimerkiksi ISO27000-sarjassa määritellyt tietoturvan hallintajärjestelmän tasolla.

Tietoturvapolitiikan osalta valtionhallinnossa tulisi pohtia, pitäisikö kunnille tehdä tietoturvapolitiikasta mallipohja, jota kunnat voisivat soveltaa olosuhteet huomioiden. Pohjan rakenteena voisi käyttää esimerkiksi ISO27000-sarjassa määritettyä rakennetta. Yhtenäisen mallin etuna olisi muun muassa vertailtavuus ja arvioitavuus, vaikka sisällön osalta yksilölliset olosuhteet muokkaavat tietoturvapolitiikat yksilöllisesti. Tämän lisäksi tulisi pohtia, pitääkö valtionhallinnon tarkastaa kuntien tietoturvaa säännöllisesti vähintään strategian tai politiikan tasolla, jotta varsinaisen tietoturvan toteuttaminen olisi laadukkaasti rajattu. On muutoinkin todettava, ettei Lahden ja Kokemäen tietoturvaa ollut arvioitu ulkoisesti ennen hyökkäystä ja tällä on ollut vaikutusta hyökkäysten onnistumisessa.

Varsinaiset onnistuneet kyberhyökkäykset olivat taidokkaasti toteutettu. On todennäköistä, että niitä ei olisi voitu estää, mikäli hyökkääjällä olisi käytössään riittävästi aikaa, resursseja ja motivaatiota. Sen sijaan hyökkäysten vaikutuksia ja palautumiseen kulunutta aikaa ja resursseja olisi voitu merkittävästi pienentää onnistuneella suojautumisella.

Haastatteluita tehdessä jäi vaikutelma, ettei Lahden ja Kokemäen tietoturvapäälliköt uskoneet käytössä olleiden tietoturvapolitiikojen vaikuttaneen positiivisesti hyökkäysten torjunnassa. Tämä ei kuitenkaan pidä paikkaansa ja erityisesti Kokemäen tietoturvapolitiikka ja sen muodostamisprosessi on vaikuttanut merkittävästi hyökkäyksestä palautumiseen.

Tietoturvallisuuden henkilöstöresursointi oli tutkituissa kunnissa pieni. Tämä on varsin ymmärrettävää ja perusteltua, varsinkin ennen onnistunutta hyökkäystä. Sen sijaan onnistuneen hyökkäyksen jälkeen kuntien tulisi pohtia, onko mielekästä yhdistää tietohallinto ja tietoturvallisuus samalle henkilölle ja voitaisiinko kaikkia tietoturvallisuuteen liittyviä tehtäviä ulkoistaa kunnista koulutetuille ammattilaisille. Töiden ulkoistaminen ei ulkoista vastuuta. Lisäksi tietoturvallisuus tulisi olla organisoitu ja resursoitu suhteessa uhkaan. On varsin olennaista pohtia, riittääkö kaupungin toiminnan mahdollisesti lamauttavan asian hoitamiseen yksi henkilö.

Tutkimuksen aikana haastattelin Kokemäen kaupungin kyberhyökkäykseen liittyen Porin poliisista Marko Levosta, joka osallistui

tapauksen tutkintaan. Haastattelun tarkoituksena oli taustoittaa tapausta eikä haastattelusta ole otettu viittauksia varsinaiseen materiaaliin. Hänen kertomuksensa vahvistaa kaikkien haastateltujen näkemystä kyberhyökkäyksen selvittämisestä. Olennaisimpina nousivat esiin omien fyysisten ja loogisten verkkojen tuntemus, yhteyshenkilön merkitys sekä varautumissuunnitelma. Nämä ovat asioina suhteellisen helposti dokumentoitavia ja harjoiteltavia, joten ainakin näiden osalta kunnissa tulisi tarttua toimeen.

8.1 Tutkijan itsearvio tutkimuksesta

Tutkimuksen lopuksi tutkija suoritti itsearvion, jossa tutkimusta verrattiin Pirkko Anttilan esittämiin hyvän tutkimuksen kriteereihin: hedelmällisyys, relevanssi, objektiivisuus, verifiointi, kantavat ideat ja käytännöllisyys. (Metodix Oy, 1998)

Tutkittava aihe on ajankohtainen ja sen ajankohtaisuus jatkuu. Tietoturvahyökkäykset julkisiin ja yksityisiin tietojärjestelmiin ovat olleet ajankohtaisia koko 2000-luvun ja niiden merkitys kansantaloudelle on merkittävä sekä hinta hyökkääjälle on suhteellisen alhainen suhteessa kiinni jäämisen riskiin sekä tavoiteltavaan rikoshyötyyn. IBM on arvioinut, että keskimääräinen onnistuneen tietoturvahyökkäyksen kustannus yritykselle on 3,86 miljoona dollaria. Matalan tason tietoturvahyökkäys maksaa hyökkääjälle alkaen 30 dollarista kuukaudessa ja mahdollinen rikoshyöty on keskimäärin 25 000 dollaria. (CSO, 2020)

Tutkimuksen kohteena ovat kunnat, niiden tietoturvallisuuden fundamentit sekä niiden muodostuminen sekä tietoturvaan kohdistuva hyökkäys. Tutkittava asia on erittäin merkityksellinen kuntien palvelutuotannolle ja tutkimuksella siihen löydettävät parannukset voivat hyödyttää kuntien asukkaita merkittävästi. Tutkimusmenetelmänä tapaustutkimus soveltuu onnistuneen kyberhyökkäyksen tutkintaan varsinkin, kun tutkitaan tietoturvallisuuden muodostumista organisaatiossa. Tapaustutkimus soveltuu myös kyberhyökkäyksen tekniseen tutkintaan, mikäli lähdeaineisto on saatavilla.

Tutkimus toteutettiin asiakirjatutkimuksena ja haastatteluilla. Tutkimus ei ole kattava tai yleistettävä kaikkiin kuntiin ja niiden tietoturvaan, mutta tuloksista voidaan päätellä lisätutkimuksen tarve sekä valtakunnallisen ohjeistuksen sekavuus. Tutkimuksen objektiivisuutta olisi voitu parantaa tekemälle enemmän asiantuntijahaastatteluita esimerkiksi tapauksia tutkineiden poliisien kanssa.

Tutkimustulokset ovat toistettavissa, mutta tutkimuksen tulosten mitattavuus voisi olla parempi. Tietoturvallisuus on mittaamisen näkökulmasta hankala kokonaisuus ja sinällään onnistunut kyberhyökkäys kertoo epäonnistuneesta tietoturvasta. Tässä tutkimuksessa kohteena olleet tapaukset ovat riittävän tuoreita, jotta niiden kulkua ja merkitystä voidaan täydentää lisätutkimuksella.

Tutkimuksen kantava ajatus muuttui tutkimuksen alussa, jossa aineiston saatavuus ohjasi tutkimusta tietoturvallisuuden ylemmälle tason, eli tietoturvallisuuden ohjauksen tutkimiseen. Tutkimuksen perusajatus ei muuttunut, koska tutkittavat tapaukset sekä tutkimuskysymysten tausta ei vaihtunut. Tutkimuksen tulosten kannalta muutoksella ei ollut merkitystä, mutta jatkotutkimuksen osalta se mahdollista kyberhyökkäysten teknisen osuuden tutkimuksen sekä arvioinnin seuraaviin tutkimuksiin.

Tutkimuksen tulokset ovat luonteeltaan sellaisia, että niillä tulisi olla vaikutusta tietoturvallisuuden kehittämiseen kunnissa. Tutkimuksen tulosten perusteella on mahdollista suunnata jatkotutkimusta sekä kehittää ja ottaa käyttöön yksinkertaisia parannuksia tietoturvallisuuden ohjaamiseen julkisella sektorilla. Tutkimus on menetelmien ja teorian pohjalta laajennettavissa kuntien tutkimuksen ulkopuolelle.

8.2 Tutkimuksen rajoitteet

Tutkimukselle asetetuista rajoitteita johtuen tutkimuksen tulosten hyödynnettävyydessä on rajoitteita. Tutkimuksen tapaustutkimusten määrä ei riitä yleistettävyyteen eikä riitä kattavaan otokseen julkisten toimijoiden tietoturvastrategian ja -politiikan nykytilasta. Lisäksi tutkimus rajautui materiaalin osalta tietoturvapolitiikojen tutkimukseen eikä niistä johdettuja käytäntöjä tutkittu. Mikäli halutaan arvioida kattavasti kuntien ohjeistuksen merkitystä kyberhyökkäysten onnistumiseen tutkituissa tapauksissa, tulisi nämä dokumentit sisällyttää lähdemateriaaliin. Tällä on merkittävä vaikutus tutkimuksen laajuuteen.

Tutkimuksen lähdemateriaalina käytetyt toimijoin tietoturvastrategiat ja -politiikat ovat julkisilla toimijoilla sekä julkisia että viranomaistoiminnassa turvaluokiteltuja. Yksityisen puolen materiaali on pääosin toimijoiden salaamia. Tämä estää tutkimuksen laajentamisen julkisena tutkimuksena. Sen sijaan viitekehys ja tutkimusmenetelmä sopivat myös salatun materiaalin käsittelyyn ja tulosten saamiseen.

Tutkimuksen viitekehys ja tutkimusmenetelmä rajaavat tutkimuksen aineistoa ja tuloksia. Tietoturvallisuuden tutkimuksen kannalta liiketoimintanäkökulma on vain yksi osa kokonaisturvallisuuden viitekehystä ja muiden näkökulmien esittäminen avaa tietoturvan kehittämisen kompleksisuutta enemmän, joskin samalla monimutkaistaa tuloksia ja heikentää yleistettävyyttä. Tutkimusmenetelmänä tapaustutkimus on tutkimuksen kohde huomioiden hyvä menetelmä, mutta esimerkiksi laajempi haastattelututkimus kertoisi enemmän lähdeaineiston valmistelusta ja tietoturvastrategian ja -politiikan hyödystä kyberhyökkäyksen aikana ja siitä palautuessa.

8.3 Tutkimuksen hyödynnettävyys ja jatkotutkimus

Tutkimuksen tarkoituksena oli aluksi tutkia tapaustutkimuksen keinoin Lahteen ja Kokemäkeen kohdistuneita kyberhyökkäyksiä tekniseltä näkökulmalta. Tutkimuksen tavoite kuitenkin muuttui tutkimuksen alkuvaiheessa, jolloin kävi selväksi, ettei kyberhyökkäysten tekniselle tutkimiselle ole riittävästi lähdeaineistoa. Kyberhyökkäysten poliisitutkintaan kuuluu salassapito ja koska molemmat tapaukset ovat vielä selvittämättä, ei tutkimukseen ollut saatavilla riittävästi teknistä aineistoa. Tämä on tutkijoiden hyvä tietää tapauksia valittaessa.

Tutkimus on hyödynnettävissä erityisesti tapaustutkimuksen kohdeorganisaatioissa Kokemäen kaupungissa ja Lahdessa tietoturvatyössä sekä osin hyödynnettävissä samankokoisten julkisten toimijoiden tietoturvan kehittämisessä. Teoriaosuus antaa riittävän näkökulman liiketoiminnan näkökulmasta, jotta samassa viitekehyksessä tuloksia voidaan hyödyntää myös eri kokoisilla julkisilla toimijoilla. Yleisesti mikä tahansa harkittu tietoturvan kehittämisen viitekehys tarjoaa suurimmalle osalle toimijoista merkittäviä hyötyjä tietoturvan kehitystyössä.

Tutkimus on hyödynnettävissä jatkotutkimukseen. Tutkimusmenetelmä sopii tietoturvastrategian ja -politiikan tutkimukseen julkisessa organisaatiossa, jossa tietoturvaan liittyvät asiakirjat ovat julkisia. Tutkittavia julkisia organisaatioita on runsaasti ja esimerkiksi kyberhyökkäyksen kohteeksi joutuneita julkisia toimijoita useita. Näiden lisäksi aineistoa voidaan laajentaa horisontaalisesti kattamaan hyökkäyksen kohteeksi joutuneiden yhteistyökumppaneita ja heidän kykyään hyödyntää kohteen opit tapauksista.

Jatkotutkimuksen osalta tutkimussuuntia voisi olla ainakin:

- Tutkimuksesta olisi johdettavissa jatkotutkimusta muun muassa laajentamalla tapaustutkimusten määrää kohti yleistettävyyttä ja julkisten toimijoiden osalta kattavuutta. Jatkotutkimus voisi olla myös tarpeellinen, sillä julkisten organisaatioiden tietoturvan kehittämistä tällaisessa viitekehyksessä ei ole tutkittu Suomessa eikä tutkimustulosten pohjalta johdettua kattavaa ohjeistusta julkisille toimijoille ole saatavissa. Tämän tutkimuksen haastatteluiden osalta tarve ohjeistukselle nousi esiin useamman kerran.
- Jatkotutkimus voi selvittää julkisten organisaatioiden ohjeistusta ja velvoitteita tietoturvastrategian ja -politiikan muodostamisessa sekä laajemmin ohjeistuksella aikaan saadun strategian ja politiikan laatua suhteessa tietoturvan kehittämisen viitekehyksiin. Tässä tutkimuksessa käytetty ISO27000-sarja tarjoaa tutkimushetkellä de facto-vertailtavan viitekehyksen, mutta se ei suinkaan ole ainoa.
- Jatkotutkimus voi selvittää tietoturvapolitiikan rakennetta ja sisältöä Suomessa ja muodostaa mallipohjan, jota julkiset organisaatiot, kuten kunnat voisivat käyttää. Tällä tutkimuksessa olisi merkitystä strategisella tasolla kansallisessa tietoturvallisuudessa.

- Tutkimuksen teoriaosuus pätee sinällään sekä julkisiin että yksityisiin organisaatioihin. Kummallakin puolella suuret toimijat ovat tämän tutkimuksen tausta-aineiston perusteella hoitaneet ainakin ulkoisesti tietoturvaan liittyvän kehittämisen. Sen sijaan kummallakin puolella pienemmät toimijat kuten Pk-yritykset ovat edelleen varsin erilaisessa tilanteessa eikä velvoitteita tietoturvan kehittämiseen vaikuta olevan. Tutkimuksella voidaan selvittää ohjeistuksen ja velvoittavuuden tasoa sekä vaikutusta sellaisten yritysten toimintaan, joilla kehitystä on tehty. Tähän viitekehykseen löytyy myös useita kyberhyökkäyksen kohteeksi joutunutta yritystä.

9 Lähdeluettelo

Anderson, E.;& Choobineg, J. (3 2008). Enterprise information security strategies. *Computers & Security*, ss. 22-29.

Barton, K. A.;Gurvirender, T.;Lane, M.;& Terrell, S. (17. 2 2016). Information system security commitment: A study of external influences on senior management. *computers & security 59 (2016)*, ss. 9-25.

Beeby, N.;& Rao, S. (3 2010). Improving Organizational Information Security Strategy via Meso-Level Application of Situational Crime Prevention to the Risk Management Process. *Communications of the association for information systems*, ss. 329-358.

Boozallen. (9 2016). *Booz, Allen, Hamilton inc*. Noudettu osoitteesta https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Bowen, P.;Hash, J.;& Wilson, M. (2006). *Information Security Handbook: A Guide for Managers* . Nation institute of standards and technology.

Cole, E.;Krutz, R.;& Conley, J. (2009). *Network security bible, 2nd edition.* Wiley.

CSO. (3. 1 2020). *How much does it cost to launch a cyberattack?* Noudettu osoitteesta CSO from IDG-sivusto: https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

Digi- ja väestötietovirasto. (21. 12 2020). *JUDO-hanke*. Noudettu osoitteesta https://dvv.fi/judo

Digi- ja väestövirasto. (4. 1 2021). *JHS-suositukset*. Noudettu osoitteesta SuomiDigi: https://www.suomidigi.fi/ohjeet-ja-tuki/jhs-suositukset

Dutton, J. (4. 6 2019). *What is an ISMS? 9 reasons why you should implement one.* Noudettu osoitteesta IT Governance blog: https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one

Eduskunta. (9. 8 2019). Tiedonhallintolaki. *Laki julkisen hallinnon tiedonhallinnasta*. Helsinki: Eduskunta.

Eduskunta. (9. 8 2019). Tietohallintolaki. *Laki julkisen hallinnon tiedonhallinnasta*. Helsinki: Eduskunta.

Espoon kaupunki. (28. 5 2018). *Espoon kaupunki Tietoturva- ja tietosuojapolitiikka.* Noudettu osoitteesta Espoon kaupunki: https://www.espoo.fi/download/noname/%7BA731E826-4468-4305-AB03-98FAAA634AB0%7D/104269

Fa, S. B. (2005). *Sodankäynnin taito.* Gaudeamus.

Freedman, S. L. (2013). *Strategy: A history.* Oxford : Oxford University Press. 2013.

Horne, G.;Ahmad, A.;& Maynard, S. (2015). Information Security Strategy in Organisations: Review, Discussion and Future Research Directions. *Australasian Conference on Information Systems.* Adelade, Australia.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, ss. 140-150.

International organization for Standardization. (1 2021). *What we do*. Noudettu osoitteesta International organisation for Standardization-sivusto: International organisation for Standardization

Kaplan, R.;& Norton, S. (2004). *Strategiakartat.* Talentum.

Kokemäki, k. (1. 1 2016). Kokemäen kaupungin henkilöstön tietoturvapolitiikka ja -periaatteet. Kokemäen kaupunki.

Kotimaisten kielten keskus. (12. 10 2020). *Kielitoimiston sanakirja*. Noudettu osoitteesta https://www.kielitoimistonsanakirja.fi/#/liiketoiminta

Kuntalaki. (10. 4 2015). Suomen laki 410/2015. *Kuntalaki*. Helsinki.

Löfbacka, M. (29. 9 2020). Kokemäen kyberhyökkäys. (J. Tammelin, Haastattelija)

Lahden kaupunki. (4. 4 2011). Tietoturvan hoidon periaatteet. *Tietoturvan hoidon periaatteet*. Lahden kaupungin hallitus.

Liikenne- ja viestintäministeriö. (2016). *Maailman luotetuinta digitaalista liiketoimintaa. Suomen tietoturvallisuusstrategia.* Helsinki: Liikenne- ja viestintäministeriö.

Magoulas, T.;Hadzic, A.;Saarikko, T.;& Pessi, K. (2012). Alignment in Enterprise Architecture: A Comparative Analysis of Four Architectural Approaches. *Electronic Journal Information Systems Evaluation* , ss. 88-101.

Metodix Oy. (1998). *Pirkko Anttila: Tutkimisen taito ja tiedonhankinta*. Noudettu osoitteesta Metodix Oy:n sivusto: https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/#13.1%20Painetut%20l%C3%A4hteet%20ja%20kirjallisuus

Monni, M. (29. 10 2020). Lahden kaupungin kyberhyökkäys 2019. (J. Tammelin, Haastattelija)

National Institute of Standards and Technology . (9. 3 2006). *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems .* Noudettu osoitteesta NIST Computer security resource center: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

National Institute of Standards and Technology. (14. 6 2017). *About NIST*. Noudettu osoitteesta NIST: https://www.nist.gov/about-nist

Oikeusministeriö. (12. 11 1999). Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta. *Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta*. Oikeusministeriö.

Park, S.;& Ruighaver, T. (2008). Strategic Approach to Information Security in Organizations. *International Conference on Information Science and Security*, (ss. 26-31).

Paulsen, C.;& Byers, R. (2019). *Glossary of Key Information Security Terms, rev 3.* Nation institute of standards and technology.

Stallings, W.;& Brown, L. (2018). *Computer security - Principles and practice.* Pearson.

Suomen standardisoimisliitto SFS. (2017). *SFS-EN ISO/IEC 27001:2017.* Suomen standardisoimisliitto. Standardien lainaukset on tehty Suomen Standardisoimisliitto SFS ry:n luvalla

Suomen standardisoimisliitto SFS. (2020). *SFS-EN ISO/IEC 27000:2020.* Suomen standardisoimisliitto SFS. Standardien lainaukset on tehty Suomen Standardisoimisliitto SFS ry:n luvalla

Svechin, A. A. (1995). *Strategy.*

Sveen, F. O.;Torres, J.;& Sarriegi, J. (2009). Blind information security strategy. *ELSEVIER*, ss. 95-109.

TechTarget. (1 2011). *What is information security management system (ISMS)*. Noudettu osoitteesta WhatIs.com: https://whatis.techtarget.com/definition/information-security-management-system-ISMS

Tufano, A. A. (2014 2014). *Conflict Management for Security Professionals.* Elsevier.

Turvallisuuskomitea. (11. 3 2014). *Kansalllisen kyberturvallisuusstrategian toimeenpano-ohjelma.* Noudettu osoitteesta Turvallisuuskomitean verkkosivut: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Kyberturvallisuusstrategian-toimeenpano-ohjelma.pdf

Valtioneuvosto. (27. 11 2003). *YHTEISKUNNAN ELINTÄRKEIDEN TOIMINTOJEN TURVAAMISEN STRATEGIA*. Noudettu osoitteesta Puolustusministeriön verkkosivut: https://www.defmin.fi/files/248/2515_1687_Yhteiskunnan_elintArkeiden_toimintojen_turvaamisen_strategia_1_.pdf

Valtioneuvosto. (23. 11 2006). *Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia 2006*. Noudettu osoitteesta Puolustusministeriön verkkosivut: https://www.defmin.fi/files/815/YETT_2006.pdf

Valtioneuvosto. (1. 7 2010). Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010. Helsinki.

Valtioneuvosto. (16. 12 2010). *Yhteiskunnan turvallisuusstrategia 2010*. Noudettu osoitteesta Puolustusministeriön verkkosivusto: https://turvallisuuskomitea.fi/wp-content/uploads/2015/10/yts_2010_fi_nettiin.pdf

Valtioneuvosto. (24. 1 2013). *Suomen kyberturvallisuusstrategia (2013)*. Noudettu osoitteesta Turvallisuuskomitean verkkosivut: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Valtioneuvosto. (2. 11 2017). *Yhteiskunnan turvallisuusstrategia*. Noudettu osoitteesta Turvallisuuskomitean verkkosivut: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Valtioneuvosto. (3. 10 2019). *Kybeturvallisuusstrategia 2019*. Noudettu osoitteesta Turvallisuuskomitean verkkosivut: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Valtiovarainministeriö. (20. 4 2004). *Tietoturvallisuus ja tulosohjaus, VAHTI-ohje 4/2004*. Noudettu osoitteesta SuomiDigi-sivusto: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2004.pdf

Valtiovarainministeriö. (30. 11 2007). *Tietoturvallisuudella tuloksia, VAHTI-ohje 3/2007.* Noudettu osoitteesta SuomiDigi-sivusto: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2007.pdf

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

Valtiovarainministeriö. (8 2008). *Valtionhallinnon tietoturvasanasto*. Noudettu osoitteesta Digisuomi: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_8_2008.pdf

Valtiovarainministeriö. (8. 4 2009). *ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin.* Noudettu osoitteesta VAHTI-ohjeet: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_2_2009.pdf

Valtiovarainministeriö. (27. 11 2014). *Tietoturvallisuuden arviointiohje.* Noudettu osoitteesta VAHTI-ohjeet: https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2014_pdf_0.pdf

Valtiovarainministeriö. (12 2018). *Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma*. Noudettu osoitteesta Valtioneuvoston verkkosivut: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161218/VM_32_2018_Julkisen_hallinnon_digitaalisen_turvallisuuden_kehittamisohjelma.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö. (Helmikuu 2020). Digitaalisen turvallisuuden kansainvälinen vertailu. Helsinki, Suomi.

Valtiovarainministeriö. (8. 4 2020). Julkisen hallinnon digitaalinen turvallisuus. Helsinki.

Valtiovarainministeriö. (22. 4 2020). *Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)* . Noudettu osoitteesta Valtioneuvoston verkkosivut: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162191/VM_2020_33.pdf?sequence=1&isAllowed=y

Valtiovarainministeriö. (2020). *Tiedonhallintalautakunnan tehtävät*. Noudettu osoitteesta Tiedonhallintolautakunta: https://vm.fi/tiedonhallintalautakunnan-tehtavat

Wikipedia. (3. 1 2021). *Standards organization*. Noudettu osoitteesta Wikipedia: Standards organization

Virtain kaupunki. (10. 12 2018). Virtain kaupungin tietoturva- ja tietosuojapolitiikka. *Virtain kaupungin tietoturva- ja tietosuojapolitiikka*. Virtain kaupunki.

Woodside;& Woodside, A. G. (2017). *Title: Case Study Research : Core Skills in Using 15 Genres.* Detailed records.

Vuorinen, T. (2017). *Strategiakirja.* ALMA.

Yin, R. K. (2018). *Case study reserch desing and methods (6th edition).* California: Sage publications.

Yleisradio. (12. 6 2019). *Krp tutkii: Kyberhyökkäys Lahden verkkoon haittaa merkittävästi terveyspalveluita – sähköiset reseptit eivät toimi, verikokeissa ongelmia*. Noudettu osoitteesta YLE uutiset: https://yle.fi/uutiset/3-10827423

Yleisradio. (16. 6 2019). *Lahden troijalaishyökkäys ei tullut yllätyksenä, sillä kuntien tietoturvassa on puutteita – "Joissain kunnissa piilee vakava peiliin katsomisen paikka"*. Noudettu osoitteesta YLE uutiset: https://yle.fi/uutiset/3-10834466