Opinnäytetyö (YAMK)

Ohjelmistotekniikka ja ICT

2022

Kai Pousi

KUNTIEN KYBERTURVALLISUUS-HAASTEET JA NIIHIN VARAUTUMINEN

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (YAMK) | Tiivistelmä

Turun ammattikorkeakoulu

Ohjelmistotekniikka ja ICT

2022 | 71 sivua

Kai Pousi

KUNTIEN KYBERTURVALLISUUSHAASTEET JA NIIHIN VARAUTUMINEN

Opinnäytetyön tavoitteena on selvittää, millaisia kyberuhkakuvia Suomen kuntakenttään kohdistuu, millä tasolla kunnissa on mahdollisiin kyberhyökkäyksiin varauduttu sekä millaisia ratkaisumahdollisuuksia tilanteen parantamiseen olisi. Lisäksi tarkastellaan millaisia lisätarpeita kaupunkien yhä digitalisoituvat älykkäät verkottuneet järjestelmät sekä kriittiset palvelut asettavat kyberturvalle.

Teoreettisena viitekehyksenä työssä tarkastellaan aluksi ”kyber”-käsitettä, valtiohallinnon kyberturvallisuuden kehittämisohjelmia ja lainsäädäntöä, sekä kyberturvallisuuden uhkia ja tilannetta Suomessa ja globaalisti. Työssä analysoidaan kunnille jo tehtyjä tutkimuksia sekä toteutettiin teemahaastattelututkimus kuntien edustajille, kyberturvapalveluiden toimittajille sekä kyberturvan parissa vaikuttavalle taholle.

Tutkimus tuo esille, että Suomessa on valtionhallinnon toimesta, niin lainsäädännöllisesti kuin kehittämisohjelmien muodossa, systemaattisesti kehitetty tietoturvaa. Kyberhyökkäysten riski Suomessa ja globaalisti on kasvanut. Kyberuhkiin varautumisen taso kunnissa on parantunut, mutta kuntien välillä on eroja. Pääsääntöisesti teknisiä suojaustoimenpiteitä kuntiin on toteutettu hyvin, mutta tietoturvan johtamisessa ylemmällä tasolla on vielä kehitettävää. Kyberturva näkyy vielä heikosti kunnan strategioissa.

Asiasanat:

Kyberrikollisuus, Kyberturvallisuus, Kyberuhka, Smart City, IoT.

Master’s Thesis | Abstract

Turku University of Applied Sciences

Software technology & ICT

2022 | 71 pages

Kai Pousi

MUNICIPAL CYBER SECURITY CHALLENGES AND PREPAREDNESS FOR THEM

The aim of the thesis is to find out what kind of cyberthreats affect Finnish municipalities, at what level the municipalities are prepared for possible cyberattacks, and what kind of solution options there would be to improve the situation. In addition, the thesis examines what additional needs the cities' increasingly digitized smart networked systems and critical services place on cyber security.

As a theoretical frame of reference, the work initially examines the concept of "cyber", state government cyber security development programs and legislation, as well as cyber security threats and the situation in Finland and globally. The work analyzes the surveys already carried out for the municipalities. A themed interview study was carried out for the representatives of the municipalities, the suppliers of cyber security services and the parties involved in cyber security.

The research shows that information security has been systematically developed by the state administration in Finland, both in terms of legislation and in the form of development programs. The risk of cyber attacks in Finland and globally has increased. The level of preparedness for cyber threats in municipalities has improved, but there are differences between municipalities. As a general rule, technical security controllers have been implemented well in the municipalities, but there is still room for improvement in the management of information security at a higher level. Cyber security is still weakly reflected in the municipality's strategies.

Keywords:

Cyber crime, Cyber security, Smart City, Cyber threat, IoT

Sisältö

Kuvat

Käytetyt lyhenteet tai sanasto

Lyhenne	Lyhenteen selitys
Brute-force	Menetelmä, jossa yritetään järjestelmällisesti yrityksen ja erehdyksen kautta kokeilemalla löytää oikea salasana tai salausavain johonkin asiaan.
DVV	Digi- ja väestötietovirasto
Firmware	Tietoteknisen laitteen toimintaa ohjaava ohjelmisto tai sen osa, joka huolehtii laitteen perustoiminnoista.
Geoblokkaus	Geoblokkaus rajoittaa verkon kautta tarjottavan sisällön tai palvelun tarjoamista vain tietylle maantieteelliselle alueelle
IoT	Internet of Things - Esineiden internetillä tarkoitetaan järjestelmiä, jotka perustuvat teknisten laitteiden suorittamaan automaattiseen tiedonsiirtoon sekä kyseisten laitteiden etäseurantaan ja -ohjaukseen internet-verkon kautta.
Ubiikki	Ubiquitous computing tarkoittaa kaikkialla läsnä olevan tietotekniikan verkostoimaa yhteiskuntaa.
RDP	Remote Display Protocol. Työpöydän etäkäyttöön tarkoitettu Windowsin ohjelmisto.

1 JOHDANTO

1.1 Tutkimustavoitteet ja tutkimuskysymykset

Julkishallintoon, kuten muuhunkin yhteiskuntaan kohdistuu yhä enenevissä määrin tietoturvaloukkauksia ja kyberhyökkäyksiä, jotka samalla koskettavat myös suoraan kansalaisten turvallisuutta ja hyvinvointia. Suomi ei ole tässä suhteessa sen enempää suojassa kuin muutkaan maat, vaan joutuu varautumaan mahdollisiin kyberhyökkäyksiin yhä perusteellisimmin. Kansainvälinen tilanne on muuttunut varsin paljon tämän tutkimustyöni aloittamisen vuoden 2021 lopulta vuoden 2022 syksyyn mennessä. Tänä aikana 24.2.2022 Venäjä hyökkäsi Ukrainaan ja 18.5.2022 Suomi jätti yhdessä Ruotsin kanssa liittymishakemuksen Natoon. Nämä tapahtumat ovat osaltaan lisänneet merkittävästi kyberuhkaa sekä todennettuja kyberhyökkäyksiä Euroopassa.

Tämän tutkimuksen tavoitteena oli selvittää, millaisia kyberuhkakuvia Suomen kuntakenttään kohdistuu, miten kunnissa on mahdollisiin kyberhyökkäyksiin varauduttu sekä millaisia ratkaisumahdollisuuksia tilanteen parantamiseen olisi. Lisäksi tarkasteltiin millaisia erityistarpeita kaupunkien yhä digitalisoituvat älykkäät verkottuneet järjestelmät sekä kriittiset palvelut asettavat kyberturvalle. Työssä teoreettisena viitekehyksenä tarkastellaan kyberturvallisuuskäsitettä ja sen historiaa, valtiohallinnon kyberturvallisuuden kehittämisohjelmia ja lainsäädäntöä sekä kyberturvallisuuden uhkia ja tilannetta Suomessa ja globaalisti. Työssä analysoidaan kunnille jo tehtyjä tutkimuksia sekä toteutetaan haastattelututkimus kuntien edustajille, kyberturvapalveluiden toimittajille sekä kyberturvan parissa vaikuttavalle taholle. Näiden tulosten perusteella selvitetään, mitkä ovat keskeiset kehityskohteet kuntien kyberturvaan varautumisen kehittämiseksi.

Tutkimusongelmaa lähestyttiin seuraavien kysymysten avulla:

1) Millaisia kyberuhkia kuntakenttään kohdistuu tällä hetkellä

2) Mikä on kuntien kyberturvan varautumisaste tällä hetkellä ja mitkä ovat keskeisimmät asiat, jotka kunnissa tulisi olla kunnossa kyberuhkien torjunnassa?
3) Millaisia kyberturvavaatimuksia tulevaisuuden kaupunkien verkottuneet järjestelmät tuovat?

1.2 Tutkimusmetodi

Tutkimusmenetelmien valintaa ohjaa Hirsjärven ym. (1997, 183) mukaan yleensä se minkälaista tai mistä tietoa etsitään. Tutkimuksen empiiriset aineistonkeruumenetelmät voidaan jakaa neljään perusmenetelmään: kyselyyn, haastatteluun, havainnointiin ja dokumentteihin. Aineistonkeruussa on syytä pyrkiä ekonomiseen ja tarkoituksenmukaiseen ratkaisuun. Aina ei tarvitse kerätä aineistoa itse alusta alkaen. Valitun perusmenetelmän tulisi kuitenkin mahdollisimman hyvin soveltua tutkittavan ilmiön luonteeseen sekä tutkimuskysymyksiin (Hirsjärvi ym. 1997 ,185). Haastattelu on yleinen tapa kerätä laadullista aineistoa ja sen avulla voidaan yhtä hyvin kerätä kvantitatiivista, että kvalitatiivista aineistoa. Haastattelutyyppejä ja nimityksiä on useita. Yksinkertaisesti jaettuna löydetään neljä eri haastattelutyyppiä: strukturoitu-, puolistrukturoitu-, teema- ja avoin haastattelu (Eskola & Suoranta 2014).

Kyberturvallisuudesta kuntakentässä on tehty joitain akateemisia tutkimuksia, lähinnä opinnäytetöitä sekä valtiohallinnon tekemiä kyselytutkimuksia. Pääsääntöisesti tutkimukset ovat keskittyneet riskien hallintaan, digitaaliseen turvallisuuteen yleisesti ja palvelutarpeisiin. Tässä tutkimuksessa pyrittiin löytämään myös hieman teknisempää näkökulmaa kuntien kyberturvauhkiin varautumisessa.

Tutkimuksessa käytettiin strukturoidun ja puolistrukturoidun teemahaastattelun yhdistelmää. Osassa kysymyksissä (liitteet 1–3) oli annettuna numeeriset vastausvaihtoehdot, osa kysymyksistä oli avoimia. Numeeristen kysymysten vastauksien osalta voitiin tutkimuksessa tehdä myös määrällistä tutkimusta. Tutkimus oli siis pääasiassa kvalitatiivinen, mutta sisälsi myös kvantitatiivisia

osioita. Eskola ja Suoranta (2014, 13) toteavat, että rajat näiden tutkimusmuotojen välillä eivät aina ole selkeät. Haastatteluja voi käyttää sekä laadullisesti että määrällisesti ja vastaavasti haastatteluilla kerättyä aineistoa voidaan analysoida sekä kvalitatiivisesti että kvantitatiivisesti. Haastattelujen lisäksi tutkimuksessa hyödynnettiin tehtyjen tutkimusten ja kyselyjen tuloksia, joita tarkemmin on käsitelty kappaleessa 4 ”Julkishallinnolle tehdyt tutkimukset”.

1.3 Opinnäytetyön rakenne

Tämä opinnäytetyö koostuu johdannosta, kahdesta teorialuvusta, tehtyjen tutkimusten tarkastelukappaleesta, haastattelututkimusluvusta sekä teoriaa ja haastattelututkimusta yhdistävästä yhteenvetoluvusta, joka sisältää myös päätelmät. Tässä opinnäytetyössä tarkastellaan johdannon jälkeen perusteellisesti kyberilmiön eri alakäsitteitä, historiallista kehitystä sekä ilmiössä esiintyviä toimijoita ja uhkia. Lisäksi selvitetään olemassa olevaa kyberturvatilannetta Suomessa ja maailmalla. Toisessa teorialuvussa paneudutaan kyberturvaan liittyvään lainsäädäntöön sekä luodaan poikkileikkaus valtiohallinnon tietoturvan kehittämiseen liittyvistä ohjelmista. Teoriakappaleiden jälkeen siirrytään tarkastelemaan julkishallinnolle tehtyjä tutkimuksia ja niiden tuloksia. Näiden jälkeen esitetään varsinainen empiirinen osuus, joka toteutettiin haastatteluina. Kappaleessa analysoidaan haastattelujen tulokset. Tämän luvun jälkeen siirrytään työssä yhteenvetoon ja loppupäätelmiin.

2 KYBER-KÄSITE JA KYBERTURVATILANNE VERKOTTUNEESSA YHTEISKUNNASSA

Yhä verkottuneemmassa ja digitalisoituvammassa yhteiskunnassamme riski joutua kyberrikollisten hyökkäysten kohteeksi kasvaa. Deep Instinct julkaiseman ”2020 Cyber Threat Landscape Report” -raportin (Deep Instinct 2021) mukaan vuonna 2020 tehtiin maailmanlaajuisesti satoja miljoonia kyberhyökkäysyrityksiä joka päivä.

Kyberhyökkäykset aiheuttamat rahalliset menetykset yhteiskunnalle ovat mittavat. Maailmanlaajuisesti kyberhyökkäysten kustannusten on arvioitu olevan noin 600 miljardia dollarista (Lewis 2018, 6) aina 1500 miljardin dollariin (RiskQ 2019) riippuen tutkimuksen tekijästä.

Kaikkia kyberhyökkäysten aiheuttamia vahinkoja tai kerrannaisvaikutuksia ei pystytä jäljittämään tai muuttamaan rahaksi. On esimerkiksi vaikea arvioida tietomurron myötä menetetyn teknologisen etulyöntiaseman kustannukset tai mahdollisten menetettyjen tulevaisuuden työpaikkojen määrä, kun kasvuyritys ajautuu konkurssiin onnistuneen kyberhyökkäyksen vuoksi (Limnéll ym. 2014, 104).

Vuonna 2019 Suomessa koettiin useampi isompi kyberhyökkäys kaupunkeja kohtaan. Lahden kaupungin tietoverkkoon kesäkuussa tehtiin kyberhyökkäys jo toistamiseen puolentoista vuoden sisällä. Hyökkäyksen aiheuttamat kustannukset kaupungille nousivat useisiin satoihin tuhansiin euroihin. Kustannukset koostuivat palvelutuottajan työstä, asiantuntijapalvelujen hankinnasta sekä ohjelmistolisensseistä (Yle 2019a).

Kokemäellä havaittiin koko kaupungin verkon lamauttanut kyberhyökkäys heinäkuun 2019 lopussa. Hyökkäyksen yhteydessä osa kaupungin datasta lukittiin ja kaupungille esitettiin lunnasvaatimus tietojen vapauttamisesta (Yle 2019b).

Porin kaupunki taasen joutui tietomurron kohteeksi vain muutaman viikon sisällä Kokemäen tapauksesta elokuussa 2019. Tilanne koski noin 9000 käyttäjää opetusverkon puolella. Tietomurron mahdollisti Windows-käyttöjärjestelmässä ollut tietoturva-aukko (Yle 2019c).

Menetykset eivät monesti jää vain pelkästään rahallisiksi. Näiden päälle saattavat tulla myös mittaamattomat aineettomat menetykset kuten maineeseen tai epävarmuuteen ja turvattomuuteen liittyvät asiat, jotka yksilötasolla voivat olla varsin raskaita. Tästä hyvänä esimerkkinä psykoterapiakeskus Vastaamon tietomurron yhteydessä varastetut potilastiedot ja sitä seurannut kiristäminen, jonka tekijöitä kirjoitushetkellä ei vielä ole saatu tunnistettua. (Yle 2020)

Kunnilla on laajoja velvoitteita ja vastuuta julkisen sektorin toimijoina ja näin ollen kuntien tietoturva näyttelee erittäin tärkeää osaa suomalaisen yhteiskunnan tietoturvasta. Kuntien erilaisissa järjestelmissä on suuria määriä erilaista dataa mukaan luettuna arkaluontoisia henkilötietoja. Kunnilla on myös monia yhteiskunnan toiminnan kannalta kriittisiä järjestelmiä, joita ovat esimerkiksi sähkö-, vesi- ja energiasektori ja terveydenhuolto. Katkokset esimerkiksi sähkön jakelussa ja tuotannossa johtaisivat monien yhteiskunnan oleellisten toimintojen loppumiseen. Ilman sähköä veden pumppaus sekä tiestön valaistus loppuvat, kuten Ronikonmäki ja Sirviö (2021) toteavat.

Huolestuttavaa kyberturvarikoksissa on, että niiden paljastuminen saattaa kestää hyvinkin pitkään. Ponemon-instituutin tekemän tutkimuksen mukaan kestää keskimäärin 287 päivää ennen kuin tietomurto havaitaan. Tämä on seitsemän päivää enemmän kuin vuotta aiemmin (IBM Security 2021).

Tässä kappaleessa pyrin luomaan laajemman kuvan kyberturvallisuudesta ja sen taustoista: Mitä kyberturvallisuudella käsitetään. Millainen on kyberrikollisuuden historia. Millaisia uhkia ja toimijoita kyberrikollisuus sisältää ja mikä on kyberrikollisuuden tilanne tällä hetkellä Suomessa ja globaalisti.

2.1 Älykaupunki – ”Smart City”

Kuntien kyberturvallisuutta tarkasteltaessa yhden mielenkiintoisen näkökulman tuovat ”älykaupungit/Smart Cityt”. Jatkossa tässä opinnäytetyössä älykaupungilla ja Smart Cityllä tarkoitetaan samaa asiaa. Suomessa oli vuonna 2021 yhteensä 309 kuntaa, joista 107 käyttää itsestään kaupunki -nimitystä ja 202 kuntaa kunta -nimitystä. Yli 100 000 asukkaan kaupunkeja on yhteensä 9 ja näissä asuu yli 2,2 miljoonaa suomalaista. Suomen kunnat ovat siis melko pieniä. Keskimääräinen kunnan koko vuonna 2020 oli 17 851 asukasta (Kuntaliitto 2021a). Suomessa ”Smart Cityjä” ei ole siinä mittakaavassa kuin muualla maailmassa on olemassa. Lähimmäksi pääsee Helsinki, joka on systemaattisesti kehittänyt muun muassa Kalasataman aluetta. Sveitsiläinen tutkimuslaitos Internal Institude for Management Development and Design ja Singapore University of Technology and Design ovat yhdessä tuottaneet ”IMD Smart City report 2021” -raportin (IMD 2021) ja siinä Helsinki pääsee sijalle 6. Helsinkiä edellä ovat Singapore, Zurich, Oslo, Taipei ja Lausenne. Osalla Suomen kaupungeista on strategioissaan nostettu esille Smart City -tavoitteet, mutta nämä rajoittuvat vielä lähinnä kaupunginosahankkeisiin ja erinäisiin rajattuihin teknologisiin kokeiluihin. Yhtenä esimerkkinä on Turun kaupungin Smart&Wise kärkihanke, jossa yhdistyvät strateginen tavoite seudullisesta hiilineutraaliudesta vuonna 2029 ja Smart City -konsepti (Turun kaupunki 2021).

Tässä työssä Smart City -käsitettä käsitellään osana normaalia kaupunkia, jossa älykkäitä ratkaisua on otettu käyttöön tai suunnitellaan otettavan käyttöön. Yhä pidemmälle verkottuneet järjestelmät ja esineiden internet kaikkine sensoreineen luo omat vaatimuksensa kyberturvallisuudelle.

Verdict Media Limited (2020) on julkaisut otteen GlobalData Thematic Research tutkimusyhtiön raportista “Smart Cities – Thematic Research,2019”, jossa he kuvaavat Smart City -käsitteen käytön alkaneen 1970-luvulla, jolloin Los Angels käynnisti ensimmäisen kaupungin big data -projektin nimeltä ”A Cluster Analysis of Los Angeles”. Samaisen tutkimuksen mukaan varsinainen ensimmäinen oikea Smart City oli Amsterdam luotuaan digitaalisen virtuaalikaupungin vuonna 1994.

Sen jälkeen Smart City -aktiviteetteja olivat kiihdyttäneet eri tietotekniikkayhtiöiden erilaiset hankkeet.

Valtioneuvoston julkaisussa (Valtioneuvosto 2014) ”Älykäs kaupunki – Smart City. Katsaus fiksuihin palveluihin ja mahdollisuuksiin” todetaan, että Smart City -käsite on levinnyt laajalle kaupunkisuunnittelusta taloudelliseen ja teknologiseen ja jopa onnellisuutta koskevaan keskusteluun. Käsitteenä Smart City – Älykäs kaupunki on monimerkityksinen ja väljä. Se on ehkä enemmänkin jonkinlainen sateenvarjokäsite, jonka alla voidaan kehittää kaupunkien infrastruktuuria ja palveluita innovatiivisesti. Yhteistä kaikille Smart City -kehityshankkeille on, että ne pyrkivät parantamaan ihmisten elämänlaatua ja samalla vähentämään ympäristön kuormitusta. Yleensä keinona ovat informaatio- ja viestintäteknologian (ICT) uudet mahdollisuudet. Smart City -hankkeet voisi jakaa karkeasti kolmeen kategoriaan. Erityisesti teknologiayritysten visioissa korostuu futuristinen teknologia. Perinteisissä kaupunkien Smart City -hankkeissa on nostettu ekotehokkuus keskiöön ja aivan viimeaikaisessa kehityksessä on alettu painottaa Smart Cityjä mahdollistajina arjen toimivuuteen, hyvinvointiin ja onnellisuuteen (Valtioneuvosto 2014, 2)

Valtion teknisen tutkimuskeskuksen blogissa Smart Cityä luonnehditaan seuraavasti: *”Smart City yhdistetään käsitteenä vahvasti teknologiaan, mutta se tarkoittaa paljon muutakin. Kaupunkien on tarjottava asukkailleen elämisen helppoutta ja hyvinvointia, mahdollistettava suotuisa liiketoimintaympäristö yrityksille sekä varmistettava palvelujen joustavuus ja tehokkuus. Tämä kaikki samalla, kun huomioidaan kestävän kehityksen asettamat vaatimukset. Smart City voidaan nähdä kokonaisuutena, jossa teknologia tukee kaupunkeja pääsemään tavoitteisiinsa. Se, mitä älykäs kaupunki tai Smart City tarkalleen tarkoittaa, on syytä jättää kaupunkien ja niiden asukkaiden päätettäväksi. Koska Smart Citylle ei ole olemassa yleismaailmallista määritelmää, jokaisen kaupungin on määriteltävä älykkyys omalla tavallaan. Samalla on huolehdittava kestävän kehityksen toteutumisesta ja ratkaisujen toistettavuudesta ja skaalautuvuudesta”.* (VTT blogi 2018).

Euroopan komissio (European Comission b) on määritellyt Smart City käsitteen seuraavasti vapaasti suomennettuna:

”Älykäs kaupunki on paikka, jossa perinteisiä verkkoja ja palveluita tehostetaan digitaalisten ratkaisujen avulla asukkaiden ja elinkeinoelämän hyödyksi. Älykäs kaupunki on edelläkävijä digitaalisten teknologioiden käytössä, mikä parantaa resurssien käyttöä ja vähentää päästöjä. Se tarkoittaa älykkäämpiä kaupunkiliikenneverkkoja, uusittuja vesihuolto- ja jätehuoltolaitoksia sekä tehokkaampia tapoja valaista ja lämmittää rakennuksia. Se tarkoittaa myös vuorovaikutteisempaa ja reagoivampaa kaupunkihallintoa, turvallisempia julkisia tiloja ja ikääntyvän väestön tarpeisiin vastaamista.”

2.2 Kyberturvallisuus käsite

Vaikka kyberturvallisuus käsitteenä on laajasti käytetty, se on samalla haasteellinen, koska sille ei ole yhtä selkeää määritelmää. Graigen ym. (2014) määrittelee kyberturvallisuuskäsitteen resurssien, prosessien ja rakenteiden organisoinniksi ja kokoelmaksi, jota käytetään suojaamaan kyberavaruutta ja kyberavaruuteen perustuvia järjestelmiä tapahtumilta, jotka ovat oikeudellisesti ristiriidassa tosiasiallisten omistusoikeuksien kanssa (Craigen ym. 2014). Limnéll ym. (2014) tuovat esiin keskustelun siitä, onko kyberturvallisuus sama asia kuin tietoturvallisuus, verkkoturvallisuus tai tietokoneturvallisuus ja toteaa, että kyberille löytyy maailmalla satoja erilaisia määrittelyjä. Hänen mielestään käsitteistä voidaan keskustella loputtomiin, mutta loppujen lopuksi kyber tarkoittaa bittien maailmaa (Limnéll ym. 2014, 23).

Turvallisuuskomitea (2018) on laatinut kyberturvallisuuteen liittyviä suomenkielisiä määrityksiä. Se määrittelee muun muassa, että ”kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia”. Kybertoimintaympäristö taasen muodostuu erinäisistä digitaalisista

tietojärjestelmistä, joiden avulla varastoidaan, muokataan ja siirretään dataa viestintäverkkojen avulla.

Tietoturvalla eli tietoturvallisuudella tarkoitetaan oloja, joissa tietoturvariskit ovat hallinnassa sekä tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Toteutunut tietoturvauhka aiheuttaa kybertoimintaympäristön toiminnan häiriytymisen (Turvallisuuskomitea 2018).

Tässä yhteydessä on myös hyvä tuoda esille tietoturvan ja tietosuojan ero. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. Tietoturva on yksi tietosuojan toteuttamisen keino (Tietosuojavaltuutetun toimisto a).

2.3 Kyberrikollisuuden lyhyt historia

Käsitteen "kyberrikollisuus" todellinen alkuperä on epäselvä, mutta se näyttää nousseen esiin 1980-luvun lopulla tai 1990-luvun alussa myöhemmässä kyberpunk -tieteiskirjallisuudessa ja audiovisuaalisessa mediassa. Kyberavaruuden ja rikollisuuden välinen yhteys ilmeni jo kuitenkin William Gibsonin, Bruce Sterlingin ja Bruce Bethken varhaisissa kyberpunk-novelleissa (Jewkes & Yar 2021, 90). EU:n määritelmän mukaan kyberverkkorikollisuus koostuu rikoksista, jotka tehdään verkossa käyttämällä sähköisiä viestintäverkkoja ja tietojärjestelmiä (European Comission c).

Kyberrikollisuuden voisi sanoa saaneen alkunsa jo 1700-luvulla semaforisignaalien sieppaamisesta tai salakuuntelusta 1800-luvulla ja 1900-luvun alussa. Molemmissa tapauksissa arvokasta tietoa siepattiin ja sitten myytiin tai käytettiin muihin omiin oikeudettomiin tarkoituksiin. Varsinainen

tietoverkkorikosten synty kuitenkin sai alkunsa, kun ensimmäiset elektroniset tietokoneet valmistettiin 1940-luvulla (Jewkes & Yar 2010 ,95; Peltomäki & Norppa 2015, 32). Vaihe kesti aina 1960-luvulle asti.

Jewkes ja Yar (2010) ja Peltomäki ja Norppa (2015) kuvaavat tätä aikakautta ensimmäisen sukupolven ”matalan tason” kyberrikollisuudeksi. Tämän ajan rikoksille oli tyypillistä tietokonekeskuksissa olleiden suurikokokoisten tietokoneiden fyysinen vahingoittaminen henkilöstön toimesta sekä lisäksi keskustietokoneiden rikollinen hyödyntäminen muun muassa laittoman rahan hankkimiseen.

Toista vaihetta, joka ajoittuu 1970-luvulta 1980-luvulle, voidaan kutsua myös toisen sukupolven kyberrikosten aikakaudeksi. Tällä ajankohdalla voidaan katsoa tietokonerikosten kehittyneen. Toisen sukupolven kyberrikokset olivat verkkorikoksia kuten hakkerointi ja murtaminen. Esimerkkinä näistä Cap’n Crunchin (alias John Draperin) legendaariset hyökkäykset, joka oli saanut nimensä Cap'n Crunch -murolaatikosta hankitusta lelupillistä, jolla viheltämällä hän pystyi tuottamaan AT&T:n puhelinjärjestelmään pitkän matkan valintaäänen. Näihin aikoihin tulivat markkinoille myös ensimmäiset henkilökohtaiset tietokoneet, jotka voitiin yhdistää puhelinverkkoihin. Sen aikaiset hakkerit testasivat järjestelmiä ja jakoivat tietonsa hakkeroinneistaan ilmoitustaulupalveluissa. Näistä ilmoitustaulupalveluista kehittyivät varhaiset virtuaaliset kauppapaikat, joissa tietopalvelut ja tavarat olivat myynnissä ja samalla loivat myös mahdollisuuksia rikolliselle toiminnalle. Tässä vaiheessa lainsäätäjätkin heräsivät ongelmaan ja tietokonerikoksista ryhdyttiin säätämään omia pykäliä. (Jewkes & Yar 2010 ,96; Peltomäki & Norppa 2015, 32)

Peltomäki ja Norppa (2015) jakavat Jewkesin ja Yarin (2010) toisen sukupolven jälkimmäisen kauden vielä kolmanneksi vaiheeksi, joka sijoittuu 1990-luvulle. Tänä aikana Internet yleistyi ja TCP/IP-protokolla hyväksyttiin standardiksi. Vielä 1980-luvun puoliväliin saakka Internet oli ollut Yhdysvaltain armeijan suojattu hyökkäyksen kestävä viestintäjärjestelmä ja se avattiin aluksi valtion ja akateemisen yhteisön käyttöön ennen kuin se lopulta tuli julkisesti saataville. Internet mahdollisti entistä monipuolisemmat tavat tehdä kyberrikoksia. Aluksi

rikokset olivat lähinnä roskapostiviestejä ja harrastelijoiden hakkerointikokeiluja. Kasvava rikollisuus aiheutti kuitenkin paineita lainsäätäjille kriminalisoida verkkorikoksia tehokkaammin. Suomessa rikoslakia muutettiin ja sen 38 luvusta tuli ”tieto- ja viestintärikokset” -luku (Peltomäki & Norppa 2015, 32).

Viimeisin vaihe on alkanut vuoden 2000 tienoilla. Tätä Jewkes ja Yar (2010) kuvaavat kolmanneksi ja korkean tason kyberrikollisuuden sukupolveksi. Tälle tunnusomaista on sen hajautettu ja automatisoitu luonne ja tietokonerikollisuus on jo jokapäiväistä. Kuten edellisessä kappaleessa todettiin, verkkorikoksentekijän ja uhrin välinen vuorovaikutus tapahtui alkuvaiheessa roskapostin kautta, jonka avulla levitettiin vastaanottajan koneen haltuun ottavia haittaohjelmia, jota sitten käytettiin roskapostien edelleen lähettämiseen. Järjestäytynyt rikollisuus ja valtiolliset toimijat tulivat nopeasti perässä. Harrastelijaviruskirjoittajia ei enää paljoa nähdä (Peltomäki & Norppa 2015, 32).

Lainsäädännön näkökulmasta kyberrikollisuuden nopea kasvu ja monimuotoisuus aiheuttaa suuria haasteita. Kyberrikollisuus tuntuu kulkevan koko ajan askeleen edellä lainsäädäntöä. Teot saattavat olla hyvinkin vahingollisia, vaikka lainsäädäntö ei olisi vielä ehtinyt säätää niitä rangaistaviksi. (Peltomäki & Norppa 2015, 7). Limnéll ym. (2014) mainitsee kirjassaan, että kahdessa kolmasosassa valtioista kyberrikoksia ei tunnisteta kunnolla tai ei lainkaan ja vain alle puolet valtioista pitää tämänhetkistä lainsäädäntöä riittävänä.

2.4 Kyberrikollisuuden uhat ja toimijat

Kyberrikollisuuden luonne on muuttunut internetin alkuajoista, jolloin asian harrastajat halusivat kokeilla kykyjään tai näyttää muille, että pystyvät murtautumaan johonkin järjestelmään. Toki edelleen näitä yksittäisiä, ”hyväntahtoisia” hakkereita järjestelmien kimpusta löytyy, mutta entistä enemmän kyseessä ovat rikolliset tarkoitusperät rahan tai vahingonteon vuoksi. Kyberrikollisuuden pelikenttä on laaja, Peltomäki ja Norppa (2015) jakavat sen viiteen osa-alueeseen: kyberaktivismi (kybervandalismi, haktivismi), kyberrikollisuus, kybervakoilu, kyberterrorismi ja kyberoperaatiot. Samalla tavalla

edelleen voidaan myös kategorisoida mahdolliset toimijat: yksittäiset hakkerit, ideologiset hakkerit, rikollisryhmittymät, kyberterroristit ja valtiolliset tahot.

Kybervandalismi

Kybervandalismilla ja haktivismilla (hacktivism) tarkoitetaan tietoverkossa tapahtuvaa aktivismia eli toimintaa, jolla halutaan saada aikaan huomiota tai muutosta johonkin tiettyyn asiaan. Haktivismi terminä koostuu sanoista hakkeri ja aktivismi. Käytännössä kyse kansalaisvaikuttamisesta verkossa, jossa toimijoita voidaan kutsua ideologisiksi hakkereiksi. Usein haktivismilla viitataankin yhteiskunnallisiin liikkeisiin, jotka hyödyntävät tietoverkkojen mahdollisuuksia keinovalikoimassaan joko omatoimisesti tai hakkerien avustamina. Tietoteknologialla nähdään tällöin olevan vain välineellinen rooli. Haktivismin ja fyysisen maailman aktivismin muodot menevätkin usein päällekkäin kuten esimerkiksi Anonymouksen skientologiaa vastustamat joukkomielenosoitukset, jotka laajenivat kybermaailman toimesta ympäri maailmaa (Peltomäki & Norppa 2015; Limnéll ym. 2014)

Peltomäen ja Norpan (2015) mukaan haktivismia on esimerkiksi www-palveluun murtautuminen ja sen sotkeminen. Yleensä haktivistit iskevät palvelunestohyökkäyksellä, jossa sivustoa kuormitetaan niin massiivisella liikennemäärällä, että se kaatuu. Ryhmät myös varastavat palvelimilta asiakasrekisterejä ja kävijätietoja.

Kyberrikollisuus

Kyberrikollisuuden määrä kasvaa nopeasti, ja sen kohteeksi voi joutua lähes jokainen. YK:n tilastojen mukaan päivittäin noin miljoona ihmistä on tavalla tai toisella verkossa tapahtuvan rikollisuuden kohteena. Tarkka tilastointi on kuitenkin vaikeaa, sillä tilastointikäytännöt vaihtelevat maittain eikä isoa osaa verkkorikoksista ilmoiteta, kyetä selvittämään tai tilastoida. Verkkorikollisuuden on muuttunut liiketoiminnaksi ja motiivina ovatkin merkittävät taloudelliset intressit. Pelkästään Euroopan osalta puhutaan vuositasolla miljardeista euroista (Peltomäki & Norppa 2015)

Sisäministeriö määrittelee verkkosivullaan kyberrikollisuuden seuraavasti ”Kyberrikollisuus eli tietotekniikkarikollisuus tarkoittaa tietotekniikkaan tai tietoverkkoihin kohdistuvia rikoksia tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen tehtäviä rikoksia” (Sisäministeriö a).

Kyberrikosten tekijät koostuvat hyvin moninaisista ryhmistä alkaen yksittäisistä hakkereista ja aktivistiryhmistä, sekä rikollisryhmittymistä aina valtioiden suorittamaan tai tukemaan vakoiluun. Kohteiksi voivat joutua kaikki fyysisen maailman ilmentymät yksittäisistä henkilöistä aina kaiken kokoisiin yrityksiin, tuotantolaitoksiin ja julkisiin organisaatioihin. (Limnéll ym. 2014, 101).

ENISA (2021) tuo raportissaan kyberrikollisten sarjaan vielä niin kutsutut vuokrarikolliset ”Hacker-for-hire”. Näillä toimijoilla asiakkaat ovat yleensä valtioita, mutta myös yrityksiä ja yksittäisiä henkilöitä. Heidän tekemisiään on hyvin vaikea ennakoida. He eivät ole keskittyneet mihinkään erityisesti, joten mikä tahansa taho voi olla kohde. He ovat hyvin suojautuneita, joten puolustajien on hyvin vaikea selvittää, kuka on ollut heidän sponsorinsa tai mikä tarkoitus heillä on ollut.

Kybervakoilu

Fyysisen maailman vakoiluvastine bittien maailmassa on kybervakoilu. Kybervakoilussa on kyse taloudellisista tai poliittisista intresseistä.

Peltomäki ym. (2015) jakaa kybervakoilun teollisuusvakoiluun ja taloudelliseen tiedusteluun. Limnéll ym. (2015) lisäävät tähän vielä sotilaallisen ulottuvuuden. Verkon yli innovaatioiden varastamisen uhka on lisääntynyt sekä taloudellisen tiedustelun (tiedustelupalveluiden toimesta), että teollisuusvakoilun (yksityiset toimijat) näkökulmasta. Motiivina ovat merkittävät kansalliset intressit teollisuuspuolella.

Teollisuusvakoilun näkökulmasta koko EU-alueen kansantaloudessa merkittävä pääoma on kiinni aineettomassa pääomassa (intellectual property), mikä liittyy

mm. tuotekehitykseen. Taloudellinen verkkotiedustelu liittyy ulko- ja turvallisuuspoliittisen päätöksenteon kysymyksiin. (Peltomäki & Norppa 2015)

Vakoilua tekevät yritysten omat tai heidän palkkaamat hakkerit sekä valtiolliset tahot. Limnéll ym. (2015) toteavat, että kybervakoilua on pidettävä tänä päivänä yhtenä vakavimmista kyberuhkista, jonka seuraukset saattavat eskaloituessaan olla pahimmillaan hyvinkin vakavia.

Kyberterrorismi

Kyberterrorismissa käytetään tietoverkkoja hyökkäyksiin kriittisiä informaatiojärjestelmiä vastaan ja niiden kontrollointiin. Hyökkäysten tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen. Uhkaajana on yleensä henkilö tai ryhmittymä tai jopa valtio. Hyökkäykset ovat etukäteen suunniteltuja, tavoitteiltaan poliittisia, sosiaalisia, uskonnollisia tai ideologisia (Peltomäki & Norppa 2015; Limnéll ym. 2014).

Limnéll ym. (2015) mukaan hyökkäysten kohteina voivat olla tietojärjestelmät ja -verkot tai yleinen tietoliikenneinfrastruktuuri. Kyberterrorismin todennäköisempiä kohteita ovat järjestelmät, jotka kontrolloivat kansallisen puolustuksen ja kriittisen infrastruktuurin toiminnan

Perinteisesti on ajateltu, että suljetut tietojärjestelmät ovat turvassa hyökkäyksiltä. Suljetulla tietojärjestelmällä tarkoitetaan järjestelmää, joka ei ole verkon kautta yhteydessä ulkopuoliseen maailmaan. Tällaisia ovat esimerkiksi teollisuuden automaatiojärjestelmät ja voimalaitosten (Supervisory Control and Data Acquisition, SCADA) ohjausjärjestelmät. Suljettu tietojärjestelmäkin on kuitenkin haavoittuvainen, jos siihen yhdistetään haittaohjelman sisältävä muistitikku tai langaton reititin, joka mahdollistaa järjestelmään kytkeytymisen etänä (Peltomäki & Norppa 2015).

Valtiolla ja kunnilla onkin suuri vastuu suojata yhteiskunnan kriittistä, automatisoitua infrastruktuuria, kuten vesilaitoksia, tietoverkkoja sekä sähkön tuotantoa ja jakelua.

Kyberoperaatiot

Kybersota-käsitettä käytetään hyvinkin laajasti kuvaamaan tapahtumia ja toimia digitaalisessa kybermaailmassa. Toisille kybersota on sotaa virtuaalimaailmassa, toisille se on vastakohta konventionaaliselle sodankäynnille. Tutkijoiden mukaan kybersodankäynnin määrittelyn tulisi perustua sodan tavoitteisiin ja motiiveihin, ei niinkään kyberoperaatioiden muotoihin. Kaikki aktivistien suorittamat isotkin palvelunestohyökkäykset tai verkkovakoilu eivät ole kybersotaa vaan pikemminkin rikollista toimintaa. (Peltomäki & Norppa 2015)

Viimeisten kymmenen vuoden aikana valtiot ovat alkaneet suhtautua kybermaailmaan strategisena ulottuvuutena, jossa niiden täytyy uskottavuutensa vuoksi olla vahvoja toimijoita. Tämä on saanut valtiot resursoimaan mittavia summia erilaisten kyberkyvykkyyksien kehittämiseen. Monen maan asevoimissa kybermaailmasta puhutaan jo sodankäynnin viidentenä ulottuvuutena maan, meren, ilman ja avaruuden ohella. Tällöin valtiolla on uskottavuutensa nimissä oltava vahva puolustus-, tiedustelu- ja hyökkäyskyky kybermaailmassa – aivan kuten muissakin sodankäynnin ulottuvuuksissa. (Limnéll ym. 2014). Nato-huippukokouksessa Madridissa kesäkuussa 2022 tehdyn kyberturvallisuus linjauksen johdosta vakava kyberisku voisi johtaa liiton perustamissopimuksen artikla 5:n aktivointiin, arvioi Limnéll. ”Jotta artikla 5 aktivoitaisiin, hyökkäyksen tulisi johtaa ihmisten kuolemiin. Tässä tapauksessa hyökkäys voisi kohdistua esimerkiksi terveydenhuoltoon, jossa potilasjärjestelmistä katoaisi tietoja ja hoitolaitteita lamautuisi” (Tivi 2022a).

Kirjoitushetkellä, kuten johdannossa mainitsin, Euroopan turvallisuustilanne on kiristynyt. Ukrainaa vastaan kohdistetun konventionaalisen hyökkäyksen lisäksi heidän järjestelmiinsä on kohdistettu laajamittaisia kyberhyökkäyksiä. Tilanteesta tekee poikkeuksellisen myös siksi, että Anonymous on julistanut kybersodan Venäjää vastaan ja kutsunut tukijoitaan mukaan operaatioon (Ilta-Sanomat 2022). Hyvin todennäköisesti tulemme jatkossakin maailmalla näkemään eri yhteyksissä eriasteista kybervaikuttamista: kybervakoilua, aktivismia ja hakkerointia osana fyysisiä selkkauksia.

2.5 Kyberturvatilanne Suomessa ja maailmalla

Kyberturvayhtiön Deep Instinctin (2021) julkaiseman ”2020 Cyber Threat Landscape Report” -raportin mukaan vuonna 2020 todistettiin malware- ja ransomware-hyökkäysten merkittävää kasvua. Vuodesta 2019 vuoteen 2020 malware-hyökkäykset lisääntyivät 358 % ja ransomware-hyökkäykset 435 %.

Tätä kirjoittaessa on juuri paljastunut erittäin paha Apache Log4j kirjaston nollapäivähaavoittuvuus. Yhdysvaltain kyberviraston johtaja Jen Easterly varoitti, että log4j-haavoittuvuudelle saattaa olla alttiina satoja miljoonia laitteita ympäri maailmaa. Easterly kuvailee haavoittuvuutta erääksi uransa pahimmista, ellei jopa pahimmaksi (Tivi 2021a). Sen lisäksi, että kyseinen komponentti on käytössä lukemattomissa järjestelmissä, sen hyväksikäyttö on myös erittäin helppoa ja onnistuu muutamalla rivillä koodia. Suomen Kyberturvakeskus kertoo varoituksessaan, että Log4j haavoittuvuuden hyväksikäyttöyritysten määrä on kasvanut räjähdysmäisesti ja suosittelee päivittämään järjestelmät pikaisesti. (Kyberturvakeskus 2021).

Vuosia 2020–2021 leimaa erityisesti COVID-19-pandemia ja sen tuomat lisähaasteet muutoinkin kasvavalle kyberhyökkäyksien määrälle. Pandemian johdosta yritykset ja julkiset toimijat joutuivat nopeasti siirtämään työtekijänsä etätöihin kotitoimistoihin. Suomessa kunnille ja monille yrityksille pandemia vaati verrattain suuren digiloikan tekemisen erittäin nopealla aikataululla ja organisaatiot kovassa kiireessä muun muassa siirsivät järjestelmiään pilveen. Kuitenkin kiireestä ja huonosti saatavilla olevien pilviasiantuntijoiden johdosta, moniin järjestelmiin on jäänyt ei-vihamielisiä uhkia: konfigurointivirheitä ja inhimillisiä erehdyksiä. Näitä haavoittuvuuksia kyberrikolliset ja sekä myös valtioiden tukemat ryhmät ovat alkaneet maailmalla hyödyntää. Pilvipalveluiden osalta raportointijaksolla havaittiinkin piikki tietoturvatapahtumien osalta (ENISA 2021).

COVID-19 loi myös otollisen maaperän huijauksille, disinformaatiolle ja haittaohjelma-hyökkäyksille. Deep Instinct (2021) mainitsee raportissaan, että Google keräsi jopa yli 18 miljoonaa uuteen koronavirukseen liittyvää

haittaohjelmaa ja tietojenkalasteluviestiä palvelussaan päivittäin huhtikuussa 2020.

HP Wolf Security:n (2021) ”Blurred lines and blindspots” -raportin mukaan etätyöskentely-ympäristö on turvallisuuden kannalta erilainen, jossa työntekijät ottavat enemmän riskejä kuin normaalissa toimistossa. Etänä työskentelevät saattavat käyttää turvattomia laitteita, antavat perheenjäsenten käyttää työnantajan välineitä ja muutenkin käyttävät niitä yksityiselämän tarpeisiin.

Saman havainnon on ENISA (2021) tuonut raportissaan esille. Etätyöntekijät ovat hajallaan, heitä ei suojaa yrityksen palomuuri, eikä suojattuja VPN (Virtual Private Network) yhteyksiä ole kaikilla käytössä. Uusi hyvinkin monimuotoinen ja hallitsematon työympäristö laajensi hyökkäyspinta-alaa varsin merkittävästi, jota kyberrikolliset eivät jätä hyödyntämättä.

Useat tietoturvayhtiöt julkaisevat vuosittain kyberuhkaraportteja kuten Deep Instinct ja aiemmin mainittu EU:n kyberturvallisuusvirasto ENISA (European Network and Information Security Agency). Näiden tuottamien raporttien pohjalta on mahdollista luoda hyvä kokonaiskuva uhkista, joihin tulisi varautua.

Kuten Deep Instinctin raportin, niin myös ENISA (2021) raportin mukaan kiristyshaittaohjelma -hyökkäykset on todettu vuosien 2020–2021 suurimmaksi uhaksi. Kyberrikollisia motivoi entistä enemmän rahan teko, jossa kiristysohjelmien osuus tulee esille. Kiristysohjelmahyökkäykset ovat tulleet monivaiheisimmiksi. Pelkän tiedon kryptaamisen lisäksi lunnasvaatimuksia vahvistetaan arkaluonteisen tiedon julkistamispelotteella ja jopa osittaisella julkistamisella. Kalastelusähköpostit ja brute-force menetelmät RDP-ympäristöissä ovat yleisemmät tavata saastuttaa kohde kiristysohjelmilla.

ENISA:n raportin (2021) suurimmat uhat ovat:

- Kiristyshaittaohjelma (Ransomware), joka salaa tiedostot tai lukitsee laitteen kokonaan.
- Haittaohjelma (Malware)
- Kryptokaappaus (Cryptojacking)

- Sähköpostiin liittyvät uhat (E-mail related threats)
- Tietovarkaudet (Threats against data)
- Tiedon saatavuuteen ja eheyteen liittyvät uhat (Threats against availability and integrity)
- Disinformaatio – Väärän tiedon jakaminen (Disinformation – misinformation)
- Ei-vihamieliset uhat (Non-malicious threats)
- Toimitusketjuhyökkäys (Supply-chain attacks)

Rikolliset ovat alkaneet tehdä myös enemmän yhteistyötä keskenään ja erilaiset palvelut rikollisten välillä ovat alkaneet yleistyä. Näistä hyviä esimerkkejä ovat:

- Phishing-as-a-Service (PhaaS) - Tietojen kalastelua palveluna.
- Ransomware-as-a-Service (RaaS) - Kiristysohjelmia palveluna.
- Disinformation-as-a-Service (DaaS). Misinformaatio ja disinformaatio ovat kyberrikollisuuden aktiviteettien ydintä ja jotka COVID-19 vaikutuksesta kasvoivat merkittävästi.

Raportin mukaan perinteiset palvelunestohyökkäykset (Distributed Denial of Service) hyökkäykset ovat siirtymässä mobiiliverkkoon ja IoT-järjestelmiä vastaan. Tämä on huolestuttava havainto, joka koskee muun muassa älykaupunkien verkottuneita järjestelmiä.

ENISA on nostanut listalle myös toimitusketjuhyökkäykset. Näiden kohteena ovat erityisesti erilaisia käyttöpalveluita (managed services) tarjoavat toimijat. Esimerkkeinä ENISA mainitsee näistä muun muassa SolarWinds-ohjelmistoyrityksen toimitusketjuun kohdistuneen hyökkäyksen sekä Codecovin hakkerointi ja Kaseya-hyökkäyksen (Check Point 2021). Toimijoita ovat erityisesti valtioiden tukemat ryhmittymät.

Suomessa Liikenne- ja viestintävirastoon alainen Kyberturvallisuuskeskus seuraa maailmalla tapahtuvia ja Suomessa vaikuttavia kyberuhkia. Kyberturvallisuuskeskus kehittää ja valvoo viestintäpalveluiden turvallisuutta sekä tuottaa kyberuhan tilannekuvaa muun muassa kuukausittaisilla ”kybersäätiedotteilla”. Kuluneen vuoden aikana Suomessa on todettu varsin

mittavaa puhelinsoittokampanjaa, jossa Microsoftin IT-tueksi esittäytyneet huijarit yrittävät saada uhrejaan asentamaan koneelleen etäkäyttöohjelmia sekä näitä hyödyntäen varastettua pankkitunnuksia yms. Lisäksi uutena on noussut esiin venäjänkielisiä huijauspuheluita, joista keskusrikospoliisin Kyberkeskus varoittaa (Tivi 2021b). Kyberturvakeskuksen mukaan Log4j- komponentin haavoittuvuuden sekä huijaussoittojen lisäksi meneillään on myös tekstiviestitse leviä Flubot-haittaohjelma (Kyberturvakeskus 2022), joissa ilmoitetaan vastaanottajan saaneen esimerkiksi uuden ääniviestin tai MMS-viestin. Viestissä olevaa linkkiä painamalla haittaohjelma pyritään asentamaan vastaanottajan suostumuksella.

Kyberrikollisuus on piilorikollisuutta ja esille tulevat tapaukset ovat vain pieni osa kokonaisuudesta. Vaikka Suomessa kokonaisrikollisuus on ollut laskussa vuodesta 1990 jälkeen, viimeisen kymmenen vuoden aikana poliisiin tietoon tulleet rikokset tietoverkkoja kohtaan ovat tasaisesti kasvaneet (Sisäministeriö b), kuten alla olevasta taulukosta nähdään.

Rikokset ja häiriöt tietoverkkoja kohtaan

Ilmoitettu (kpl)	2010	2015	2016	2017	2018	2019	2020	2021
Salassapitorikos	29	48	46	58	75	58	73	49
Tietoliikenteen häirintä	25	85	71	65	34	46	77	116
Henkilörekisteririkos	36	122	114	103	111	32	9	1
Viestintäsalaisuuden loukkaus	295	298	437	378	340	268	331	249
Tietomurto	292	347	439	442	530	822	1132	1555

Kuva 1. Rikokset ja häiriöt tietoverkkoja kohtaan (Sisäministeriö b).

3 TIETOTURVAAN LIITTYVÄ LAINSÄÄDÄNTÖ JA JULKISEN HALLINNON TIETOTURVAOHJELMAT

Julkishallinnon toimintaympäristöt, joita myös Smart Cityt edustavat, ovat voimakkaassa murroksessa digitalisaation myötä. Tietoturvaan liittyy Suomessa joukko lainsäädännöllisiä velvoitteita ja suosituksia kunnille, kuten tietosuoja-asetus, tiedonhallintalaki ja NIS-direktiivi, jotka tulee huomioida toimintaympäristöjä kehitettäessä ja niitä ylläpidettäessä. Julkinen hallinto on myös viimeisen kymmenen vuoden aikana järjestelmällisesti toteuttanut uusia tietoturvan parantamiseen liittyviä ohjelmia. Seuraavissa kappaleissa käsitellään vaikuttavia lakeja ja tehdään poikkileikkaus viime vuosikymmenen julkisen hallinnon tietoturvan kehittämisohjelmista.

3.1 Laki sähköisen viestinnän palveluista

Tietoyhteiskuntakaari (Tietoyhteiskuntakaari 917/2014) tuli voimaan 1.1.2015. Lailla kumottiin muun muassa sähköisen viestinnän tietosuojalaki (Sähköisen viestinnän tietosuojalaki 516/2004). Tietoyhteiskuntakaareen on koottu keskeiset sähköistä viestintää koskevat säädökset, kuten sähköisen viestinnän tietosuojalaki ja viestintämarkkinalaki. Tietoyhteiskuntakaari selkeyttää sääntelyä ja poistaa siinä olleita päällekkäisyyksiä. Tietosuoja-asioiden ja tietosuojavaltuutetun tehtävien osalta tietoyhteiskuntakaaren sisältämä sääntely on pitkälti samaa, kuin mitä sähköisen viestinnän tietosuojalaissa on aiemmin säädetty. Tietoyhteiskuntakaaren tavoitteena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä sekä varmistaa, että viestintäverkkoja ja viestintäpalveluja on kohtuullisin ehdoin jokaisen saatavilla koko maassa. Tavoitteena on lisäksi turvata radiotaajuuksien tehokas ja häiriötön käyttö sekä edistää kilpailua. Niin ikään tarkoitus on varmistaa, että viestintäverkot ja -palvelut ovat teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja, turvallisia sekä hinnaltaan edullisia. Lain tavoitteena on myös turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen.

Sittemmin nimike Tietoyhteiskuntakaari on muutettu (Valtioneuvosto 2018b) 1.6.2018 voimaan tulleella lailla muotoon ”Laki sähköisen viestinnän palveluista”. Laki (Laki sähköisen viestinnän palveluista 7.11.2014/917) siis pääsiassa käsittelee, kuten sen nimestä voi päätellä, sähköiseen viestintään liittyviä asioita.

3.2 Laki yksityisyyden suojasta työelämässä

Liittyen työntekijän oikeuksiin suojata yksityisyyttään ja toisaalta työnantajan tarvetta kerätä ja säilyttää henkilötietoja työntekijöistään, on säädetty laki yksityisyyden suojasta työelämässä (yksityisyyden suoja 759/2004). Laki säätää, miten yksityisyyden suojaa toteutetaan työelämässä. Se sovittaa yhteen työntekijän oikeuden suojata yksityisyyttään ja työnantajan tarpeen saada näitä tietoja käyttöönsä. Laki yksityisyydensuojasta työelämässä täydentää henkilötietolain säännöksiä henkilötietojen käsittelystä.

Tässä laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta.

3.3 EU:n tietosuoja-asetus (GDPR) ja Suomen täydentävä tietosuojalaki

EU:n yleisen tietosuoja-asetuksen soveltaminen alkoi 25.5.2018 kaikissa EU:n jäsenmaissa. Tietosuoja-asetusta (GDPR) sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Tietosuoja-asetus asettaa tietosuojaa ja henkilötietojen käsittelyä koskevia velvoitteita, joihin rekisterinpitäjien ja henkilötietojen käsittelijöiden on valmistauduttava.

Keskeistä tietosuoja-asetuksessa on muun muassa riskiperusteinen lähestymistapa ja rekisterinpitäjän osoitusvelvollisuus. Rekisterinpitäjän velvollisuudet kasvavat sitä mukaa, mitä korkeampia riskejä henkilötietojen käsittelyyn liittyy. Rekisterinpitäjän on myös pystyttävä osoittamaan, että se

noudattaa tietosuoja-asetusta. Henkilötietojen käsittely on suunniteltava ja dokumentoitava.

Rekisterinpitäjän on huolehdittava siitä, että tietosuoja-asetuksessa määriteltyjä tietosuojaperiaatteita noudatetaan kaikissa henkilötietojen käsittelyvaiheissa.

GDPR tuo suoraan vaatimuksia tietojärjestelmien tietoturvalle. Peruslähtökohta asetuksessa on, että järjestelmässä on ”sisäänrakennettu ja oletusarvoinen tietosuoja”. Järjestelmään täytyy sisältyä tarvittavat suojatoimet tietojen suojaamiseen sekä oletusarvoisesti käsiteltävä vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Asetus tuo mukanaan vaatimuksen, että henkilöllä on oikeus poistaa itsestään tiedot eli ”oikeus tulla unohdetuksi” (OpiTietosuojaa.fi).

Tietosuojaperiaatteiden mukaan henkilötietoja on

- Käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- Käsiteltävä luottamuksellisesti ja turvallisesti
- Kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
    - rekisteröidyn henkilön suostumuksen kerättävään tietoon on oltava ”yksiselitteinen”.
- Kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- Päivitettävä aina tarvittaessa – epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymät
- Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot jäsennellyssä ja koneellisesti luettavassa muodossa ja oikeus toimittaa kyseiset tiedot toiselle rekisterinpitäjälle
- Säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten.

Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa

sen ilmitulosta toimivaltaiselle valvontaviranomaiselle. (Tietosuojavaltuutetun toimisto).

3.3.1 Tietosuojalaki

Suomessa henkilötietojen käsittelyä koskeva uusi tietosuojalaki (Tietosuojalaki 5.12.2018/1050) tuli voimaan 1.1.2019. Lailla täydennetään EU:n yleistä tietosuoja-asetusta. Yleisen tietosuoja-asetuksen mukaiset viranomaistehtävät on keskitetty tietosuojavaltuutetulle. Säännösten rikkomuksista voidaan määrätä varsin merkittäviä sanktioita. Tietosuojavaltuutettu voi asettaa yritykselle, yhteisölle tai viranomaiselle uhkasakon tietojen luovuttamista koskevan määräyksensä tehosteeksi. Tietosuojavaltuutetun ja apulaistietosuoja-valtuutettujen yhdessä muodostama kolmijäseninen seuraamuskollegio voi määrätä säännösten rikkomisesta hallinnollisen seuraamusmaksun. Sen määrä voi olla lievemmissä rikkomuksissa enintään 10 miljoonaa euroa tai 2 % yrityksen kokonaisliikevaihdosta ja vakavammissa rikkomuksissa enintään 20 miljoonaa euroa tai 4 % yrityksen kokonaisliikevaihdosta (Tietosuojavaltuutetun toimisto b).

3.3.2 Tiedonhallintalaki

Vuoden 2020 alussa astui voimaan laki julkisen hallinnon tiedonhallinnasta (Laki julkisen hallinnon tiedonhallinnasta (906/2019)). Laki edistää tiedonhallinnan yhdenmukaistamista, tietoturvallisuutta ja digitalisointia viranomaistoiminnassa. Laissa julkisen hallinnon tiedonhallinnasta säädetään julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa.

Laissa säädetään uudesta kuvausvelvoitteesta, tiedonhallintamallista. Tiedonhallintamalli on hallinnon sisäinen määräys ja sen tulee olla selkeä kuvaus kunnan laajennetusta tiedonhallinnasta. Mallissa tulee kuvata myös sitä minkälaisia tietojärjestelmiin ja tietovarantoihin liittyviä kytköksiä kunnalla on muihin toimijoihin, esimerkiksi väestörekisterikeskukseen. Mallissa kuvataan minimissään toimintaprosessit, tietovarannot, tietoaineistot, tietojärjestelmät

sekä tietoturvajärjestelyt. Kunnat on velvoitettu toteuttamaan tiedonhallintalain mukaiset tietoturvallisuuden vähimmäisvaatimukset vuoden 2023 loppuun mennessä (Kuntaliitto 2019).

3.3.3 NIS direktiivi

EU:n verkko- ja tietoturvadirektiivi (The Directive on Security of Network in Information Systems (NIS)) oli ensimmäinen EU:n laajuinen yleinen tietoturvasäädös, jossa annettiin velvoite kriittisen infrastruktuurin sektoreille (Energia, Terveydenhuolto, Finanssiala, Liikenne, Vesihuolto ja Digitaalinen infrastruktuuri) raportoida tietoturvapoikkeamista ja -uhkista. Direktiivi tuli voimaan 1.8.2016 ja se tuli implementoida kansallisesti 9.5.2018 mennessä. (European Comission a). Suomessa velvoitteiden noudattamista valvovat toimialakohtaiset viranomaiset; Viestintävirasto, Energiavirasto, Valvira, Finanssivalvonta, Traficom ja ELY-keskukset.

3.3.4 Toimialakohtaisia lakeja ja suosituksia

Kunnilla on toimialoja, joihin saattaa kohdistua toimialakohtaisia lakeja ja suosituksia. Yksi keskeinen toimiala on terveydenhuolto, johon tämän opinnäytetyön kirjoitushetkellä liittyvät vastuut kunnille ovat muotoutumassa uudelleen Sosiaali- ja terveydenhuollon ja pelastustoimen uudistuksen (Sote uudistus) myötä. Uudistuksen myötä siirtymävaiheen jälkeen vuoden 2023 alusta kunnista ja valtiosta erillinen julkisoikeudellinen yhteisö, hyvinvointialue, järjestää jatkossa sosiaali- ja terveydenhuollon ja pelastustoimen palvelut. Hyvinvointialueita on yhteensä 21. Lisäksi Helsingin kaupunki vastaa sosiaali- ja terveydenhuollon sekä pelastustoimen järjestämisestä alueellaan. Terveydenhuoltoon liittyviä lakeja ovat Laki terveydenhuollon ammattihenkilöistä ja Laki yksityisestä terveydenhuollosta, jotka muun muassa sisältävät potilastietoja koskevaa salassapitovelvollisuutta. Potilaslaki, joka sisältää ehtoja, miten potilastietoja voidaan käsitellä. Potilasasiakirja-asetus, jota sovelletaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettävien asiakirjojen

laatimiseen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämiseen. Terveydenhuollon asiakastietolaki, jossa säädetään julkisten ja yksityisten sosiaali- ja terveyspalveluiden asiakastietojen sähköisestä käsittelystä ja valtakunnallisista tietojärjestelmäpalveluista. Laissa on säädökset muun muassa tietojen salassapidosta, luovutuksesta ja arkistoinnista.

3.4 Valtiohallinnon tietoturvan kehittämiseen liittyvät ohjelmat

Suomessa on tehty systemaattisesti työtä valtiohallinnon tasolla kyberturvallisuuden eteen viimeisen kymmenen - viidentoista vuoden aikana. Kyberturvallisuus oli esillä jo vuoden 2010 yhteiskunnan turvallisuusstrategiassa (Puolustusministeriö 2010). Kyberuhat tunnistettiin yhdeksi mahdolliseksi uhaksi ja tietojärjestelmiin tunkeutumisen todettiin tietyissä olosuhteissa voivan täyttää jopa sotilaallisen voimankäytön tunnusmerkit.

Suomen ensimmäinen kyberturvallisuusstrategia julkaistiin 24.1.2013. Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset sekä määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus (Valtioneuvosto 2013). Strategian toimeenpano käynnistettiin toimeenpano-ohjelmalla 11.3.2014 (Turvallisuuskomitea 2014), jonka keskeisiä kehityskohtia olivat kyberturvallisuuskeskus, valtion ympärivuorokautinen tietoturvatoiminta, salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke (SATU), poliisin toimintakyky kyberrikollisuuden torjunnassa, kybertoimintaympäristöön ja kyberturvallisuuteen liittyvän lainsäädännön kehittäminen sekä tutkimus- ja koulutusohjelmat ja muu osaamisen vahvistaminen. Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista ja luovutti mietintönsä puolustusministeriölle 14.1.2015 (Puolustusministeriö 2015).

EU:n verkko- ja tietoturvadirektiivin (NIS) mukaisesti kunkin jäsenvaltion tulee laatia kansallinen strategia, jossa määritellään puitteet, visio, tavoitteet ja

painopisteet verkko- ja tietoturvallisuudesta. Tätä kansallista strategiaa varten asetettiin 28.9.2015 tietoturvallisen liiketoiminnan kehittämisryhmä. Työryhmä luovutti ehdotuksensa tietoturvastrategiaksi liikenne- ja viestintäministerille 10. helmikuuta 2016, jonka sisällön ministeri hyväksyi työryhmän ehdotuksen mukaisena 10. maaliskuuta 2016. Strategian visiona on ”Maailman luotetuin digitaalinen liiketoiminta tulee Suomesta” (Liikenne- ja viestintäministeriön julkaisuja 7/2016).

Yhteiskunnan turvallisuusstrategia sai neljännen päivityksen 2.11.2017 (Valtioneuvosto 2017). Strategia keskittyy yhteisten ja yleisten varautumisten periaatteisiin, jossa myös kyberuhkat on otettu huomioon elintärkeissä toiminnoissa.

Osana valtioneuvoston vuoden 2016 selvitys- ja tutkimussuunnitelman toimeenpanoa toteutettiin tutkimus ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (Valtioneuvoston kanslia 2017). Tässä tutkimuksessa tavoitteena oli selvittää kuinka vuoden 2013 kyberturvastrategiassa asetettu tavoite Suomen osalta olla maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa sekä niiden aiheuttaminen häiriötilanteiden hallinnassa on saavutettu. Tämä tutkimus oli osaltaan pohjana seuraavalle Suomen kyberturvallisuusstrategian toimeenpano-ohjelmalle 2017–2021 (Turvallisuuskomitea 2017). Tässä toimeenpano-ohjelmassa tarkasteltiin kyberturvallisuuden kehittämistä niin valtion, maakuntien, kuntien, yritystoiminnan ja kolmannen sektorin muodostamassa palvelukokonaisuudessa.

Valtiontalouden tarkastusvirasto teki suunnitelmiinsa sisältyneen kybersuojauksen järjestämistä koskeneen tarkastuksen, joka toteutettiin ajalla 22.9.2016–4.9.2017 (Valtiontalouden tarkastusvirasto 2017). Tässä tarkastuksessa tavoitteena oli selvittää, onko valtiohallinnon kybersuojaus järjestetty taloudellisesti, mutta kuitenkin vaikuttavasti ja tarkoituksenmukaisella tavalla.

Huoltovarmuuskeskus käynnisti vuonna 2016 Kyber2020 ohjelman, jonka tavoitteena oli parantaa suomalaisen yhteiskunnan kykyä torjua kyberuhkia sekä toipua mahdollisista vaurioista. Ohjelmaan kuului konkreettisia toimenpiteitä, jotka parantavat huoltovarmuusorganisaation kriittisten yritysten kyberturvallisuutta. Ohjelma sisälsi seitsemän keskeistä teemaa: ohjelman ohjaus ja seuranta, luottamus kyberriskien hallintaan, kyberosaaminen ja kyvykkyydet, kansallinen havainnointikyky, viestintä, tilannekuva ja tiedonvaihto, kansainvälinen yhteistyö sekä tulevaisuuden huomioiminen. Ohjelman loppuraportti ”Kyber2020” (Huoltovarmuuskeskus 2020) julkaistiin vuonna 2021. Huoltovarmuuskeskus on tämän jälkeen käynnistänyt viisivuotisen ohjelman ”Digitaalinen turvallisuus 2030” (Huoltovarmuuskeskus 2021), jonka tarkoituksena on kehittää yhteiskunnan sietokykyä kyberhäiriöitä vastaan.

Valtioneuvoston vuoden 2017 selvitys- tutkimussuunnitelman toimeenpanossa toteutettiin ”Kyberturvallisuuden strateginen johtaminen Suomessa” -selvityshanke (Valtioneuvosto 2018a), jossa laadittiin muun muassa toimenpide-ehdotuksia yhteiskunnan ja julkisen hallinnon strategisen kyberturvallisuuden johtamiseen, mittaamiseen ja varautumiseen sekä kybertoimintaympäristöä koskevan häiriötilanteiden hallintaan.

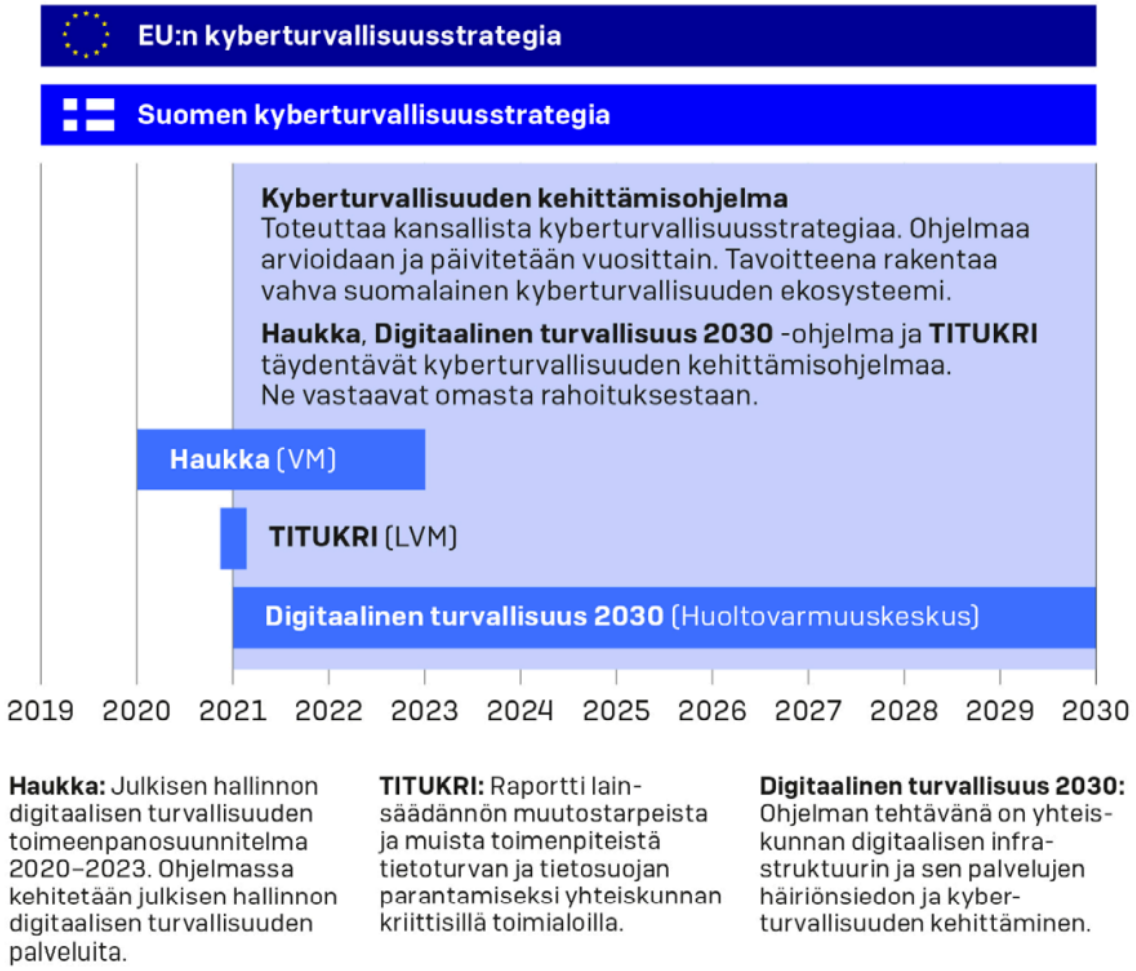
Toistaiseksi viimeisin päivitetty Suomen kyberturvallisuusstrategia julkaistiin 2019 (Valtioneuvosto 2019). Tässä kyberturvallisuusstrategiassa asetetaan Suomen keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi. Keskeisenä tavoitteena on, että Suomi on edelleen kansainvälisesti kyberturvallisuuden kärkiosaajien joukossa. Strategia on myös osa EU:n kyberturvallisuusstrategian toimeenpanoa. Strategia kulminoituu kolmeen pääkohtaan: kansainvälinen yhteistyö, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä osaamisen kehittäminen. Suomen on tehtävä tiivistä yhteistyötä kansainvälisten toimijoiden kanssa monenvälisesti, alueellisesti ja kahdenvälisesti. Kyberturvallisuuden kehittäminen taasen asettaa julkiselle hallinnolle osaamisvaatimuksia ja yhteistyövelvoitteita. Tämän johdosta kaikkien kriittisistä toiminnoista vastaavien

viranomaisten kyberturvallisuuden osaamista on parannettava kaikilla hallinnon aloilla ja tasoilla. Johtamisen osalta toteutetaan hallituskausien yli ulottuva kansallisia linjauksia konkretisoiva kyberturvallisuuden kehittämisohjelma.

Valtioneuvoston periaatepäätöksessä 8.4.2020 ”Julkisen hallinnon digitaalinen turvallisuus” määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä (Valtiovarainministeriö 2020b).

Periaatepäätöstä toteuttamaan luotiin ”Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023” -Haukka-toimeenpanosuunnitelma (Valtiovarainministeriö 2020a). Kyseessä olevassa suunnitelmassa otetaan vahvasti esille myös kunnat sekä kansalaiset, yhteisöt ja muu yhteiskunta. Tämä toimeenpanosuunnitelma on ollut myös tukena kyberturvallisuusstrategian 2019 kehittämisohjelman (LVV 2021) valmistelussa. Kehittämisohjelma on laadittu vuosille 2021–2030 ja se kuvaa kyberturvallisuuden kehittämisen lyhyen ja pitkän aikavälin tavoitteita ja painopistealueita. Kehittämisohjelmassa keskitytään neljään pääteemaan, joita ovat: huippuluokan osaaminen, kiinteä yhteistyö, vahva kotimainen kyberturvateollisuus ja tehokkaat kansalliset kyberturvakyvykkyydet.

Kyberturvallisuuden kehittämisohjelma keskeisine ohjelmineen on kuvattuna alla olevassa kuvassa (kuva 2).



Kuva 2: Kyberturvallisuuden kehittämisohjelma sen keskeiset ohjelmat (Valtioneuvosto 2021)

Kuntien ja julkisenhallinnon kannalta oleellinen hanke on vuosina 2019–2023 toteutettava Digi- ja väestötietoviraston JUDO-hanke (DVV 2019), joka kehittää julkisen hallinnon digiturvan johtamista ja hallintaa, henkilöstön digiturvaosaamista sekä tarjoaa tukea turvallisempien palveluiden kehittämiseksi. Hanke perustuu aiemmin mainittuihin ”Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmaan” sekä valtioneuvoston 8.4.2020 hyväksymään ”Julkisen hallinnon digitaalinen turvallisuus -periaatepäätökseen” ja sen toimeenpanosuunnitelmaan (Valtiovarainministeriö 2020a).

Hankkeessa on kehitetty riskien hallintaa, suosituksia tiedonhallintalain ja turvallisuusluokitusasetuksen toteuttamisen tueksi, tarjottu digitaalisen,

turvallisuuden koulutusta, luotu palvelu, jolla voidaan seurata hallinnollisen digiturvallisuuden kokonaiskuvan osa-alueiden kehittymistä ja selvitetty digitaalisen turvallisuuden harjoitustoiminnan kehittämistä. Hankkeessa on myös toteutettu muutama tutkimus kuntien digiturvapalveluiden kehittämistarpeista ja nykytilan kuvauksesta. Näiden tutkimusten tuloksia käsittelen tässä myöhemmin.

Smart City kontekstissa mielenkiintoinen on Liikenne- ja viestintäministeriön ”Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla” -selvitystyö (Liikenne- ja viestintäministeriö 2021), jossa selvitettiin tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla, erityisesti terveydenhuollon, rahoitusmarkkinoiden, energiahuollon, vesihuollon, liikenne ja digitaalisen infrastruktuurin sekä viestintäverkkojen osalta. Raportissa todetaan muun muassa, että julkisen sektorin tietoturvan tasoa selvitellyssä valtiovarainministeriön Haukka-ohjelmassa todettiin, että digitaalisen turvallisuuden tilanne on kunnissa pääosin heikompi kuin valtiotasolla. Vastaava havainto tuli esille työryhmän järjestämissä kuulemisissa, joissa kiinnitettiin huomiota siihen, että esimerkiksi terveydenhuollon, energiahuollon ja vesihuollon kriittisistä toiminnoista merkittävä osa on kuntien vastuulla.

4 JULKISHALLINNOLLE TEHDYT TUTKIMUKSET

Kuten edellä olevassa kappaleessa todettiin, valtioneuvosto hyväksyi 8.4.2020 ”Julkisen hallinnon digitaalinen turvallisuus” -periaatepäätöksen ja sen toimeenpanemiseksi käynnistettiin Haukka-toimeenpanosuunnitelma (Valtiovarainministeriö 2020a). Haukka-hankkeessa ja sen puitteissa käynnistetyssä Digi- ja väestötietoviraston JUDO-hankkeessa (DVV 2019) toteutettiin vuosina 2020 ja 2021 kyberturvallisuuden tilaa koskevia kyselyitä ja tutkimuksia. Lisäksi Kuntaliitto toteutti yhden tutkimuksen keväällä 2021. Tässä kappaleessa tarkastelen näitä julkishallinnolle tehtyjä kyberturvallisuuteen liittyvien kyselyiden tuloksia.

4.1 Digitaalisen turvallisuuden kustannusvaikuttavuusarviointi julkisessa hallinnossa.

Valtiovarainministeriö teetti selvityksen digitaalisen turvallisuuden kustannus-vaikuttavuusarvioinnin julkisessa hallinnossa (Valtiovarainministeriö 2020c). Kyseinen selvitystyö toteutettiin kirjallisuuskatsauksena sekä julkisen hallinnon organisaatioiden edustajien haastatteluiden kautta. Selvityksen tavoitteena oli kartoittaa digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arvioinnin nykytilaa julkisessa hallinnossa, sekä laatia haastatteluiden ja aiempien tutkimusten pohjalta digitaalisen turvallisuuden kustannus-vaikuttavuusmalliehdotus. Raportissa esitetään ehdotus digitaalisen turvallisuuden kustannusten ja vaikuttavuuden arvioinnin kehittämiseksi julkisessa hallinnossa.

Selvityksen mukaan haastatteluissa nousi esille, että julkisen hallinnon organisaatioilla on tarve yhtenäiselle ja selkeälle tavalle tunnistaa, luokitella ja arvioida digitaaliseen turvallisuuteen liittyviä riskejä, turvaamiseen liittyvien suojaustoimenpiteiden kustannuksia, sekä tehdyistä toimenpiteistä saavutettavia hyötyjä. Tämän pohjalta selvityksessä suositellaan, että julkisen hallinnon organisaatioiden tulisi arvioida organisaation digitaalisen turvallisuuden

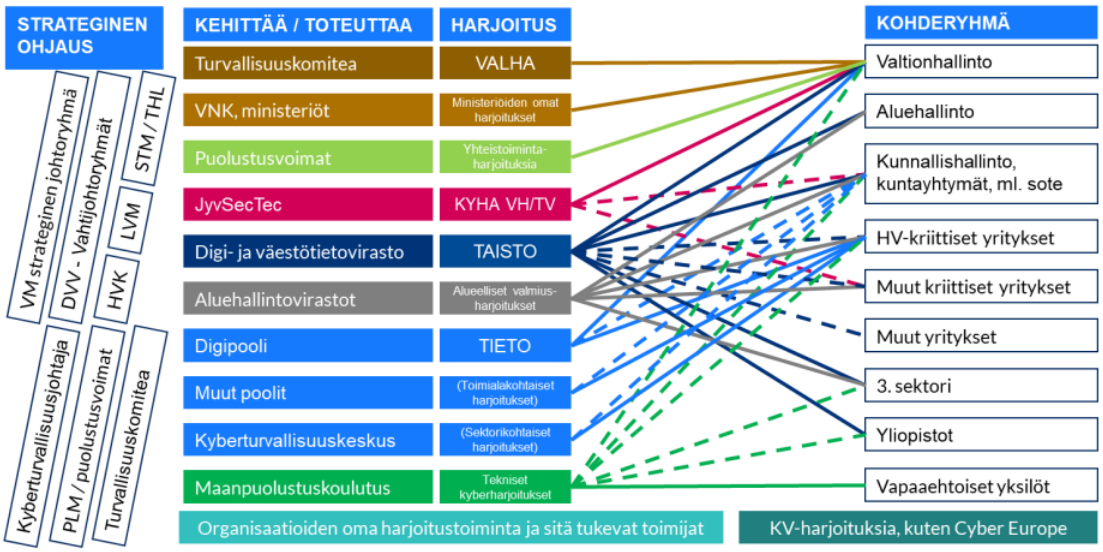
vaikuttavuutta säännöllisesti. Arvioinnissa tulisi tunnistaa organisaation toimintaan kohdistuvat riskit, sekä kohteet, joita riskeiltä halutaan suojella. Lisäksi tulisi tunnistaa myös vuosittainen odotusarvo riskien realisoitumisesta aiheutuville kustannuksille, mikäli suojattaville kohteille ei toteuteta lainkaan digitaalisen turvallisuuden suojaustoimenpiteitä.

Turvattavien kohteiden, joita ovat esimerkiksi tiedonhallintalain tarkoittaman tiedonhallintayksikön merkittävimmät tietovarannot, sekä keskeiset palvelut, arvo tulisi arvioida, sekä merkittävimmät riskit tulisi tunnistaa ja laskea rahamääräinen suuruusluokka perustuen riskin realisoitumisen todennäköisyyteen ja realisoitumisen potentiaalisesti aiheuttamiin kustannuksiin. Myös vaikuttavuutta potentiaalisilta menetyksiltä suojaavien toimenpiteiden osalta tulisi arvioida. Loppujen lopuksi toteutettavien suojaustoimenpiteiden tarkoituksena on pienentää suojattaviin kohteisiin kohdistuvien riskien aiheuttamien kustannusten odotusarvoa ja saattaa jäännösriski hyväksytylle tasolle.

4.2 Julkishallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan nykytilan kuvaus (Judo-hanke)

Digi- ja väestötietoviraston toteuttaman Judo-hankkeen projekti 5:n tehtävänä toteutettiin selvitys julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan tilasta (DVV 2020b) Tässä selvitystyössä harjoitustoiminnan nykytilaa tarkasteltiin neljästä eri näkökulmasta: lainsäädäntö, rahoitus ja ohjaus, toimijat sekä harjoitukset.

Selvityksessä tunnistetut, harjoitustoiminnan kannalta keskeiset toimijat (strateginen ohjaus, harjoitusten toteuttajat ja kehittäjät sekä harjoitusten kohderyhmät) ja harjoitukset, on kuvattu alla olevassa kuvassa 3. Kuvassa harjoituksen järjestämisen päävastuutaho on samalla rivillä kuin nimetty harjoitus.



Kuva 3. Julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan toimijoita (DVV 2020b).

Selvityksessä ilmeni, että lainsäädäntö ei tunnista harjoitustoimintaa. Poikkeuksena on valtioneuvoston asetus julkisen hallinnon turvallisuus-verkkotoiminnasta, jossa palveluntuottajalle on velvoite osallistua harjoitustoimintaan osana varautumista.

Rahoituksen osalta työryhmä nosti esille, että harjoitustoiminnan rahoitukseen ei ole suunnattu erillistä jatkuvaluonteista rahoitusta, eikä yhteistä rahoituksen koordinaatiota.

Keskeisimmiksi harjoituksiksi tunnistettiin DVV:n kerran vuodessa pidettävä TAISTO-harjoitus, Digipoolin yhdessä Kyberturvallisuuskeskuksen ja valittujen viranomaisten kanssa kerran kahdessa vuodessa TIETO-harjoitus, sekä JyvSecTec:n cyber-rangella vuosittain toteutettavat teknistoiminnalliset KYHA-harjoitukset; yksi valtionhallinnolle ja yksi turvallisuusviranomaisille. Lisäksi puolustusvoimat järjestää omalle organisaatiolleen jatkuvasti kyberturvallisuusharjoituksia. Vuodesta 2022 eteenpäin KYHA-harjoituksia järjestetään myös kunnille.

Tutkimuksessa havaittiin, että julkishallinnossa ei ole yhteisesti määriteltyä ja hyväksyttyä kansallista digitaalisen turvallisuuden harjoitusohjelmaa. Harjoitustoiminnan toimijakenttä on hajanainen ja pistemäinen, vaikkakin osa-alueittain kyvykäs. Harjoitustoimintaa ei ole myöskään kehitetty kansallisen kokonaisuuden näkökulmasta. Harjoituksia ja toimijoita on useita ja keskinäiset suhteen ovat osittain epäselviä tai määrittämättä. Yhteinen tahtotilan määritys puuttuu, raportissa korostetaan.

Digitaalisen turvallisuuden kansallisen harjoitustoiminnan nykytilan kuvauksen pohjalta on sittemmin laadittu Julkisen hallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan lyhyen ja pitkäntähtäimen tavoitteet ja toimenpiteet (DVV 2021b).

4.3 Kuntien digitaalisen turvallisuuden riskikyselyn tulokset syksyllä 2020 sekä syksyllä 2021

Valtiovarainministeriö toteutti kyselyn syksyllä 2020 kuntien digitaalisen turvallisuuden merkittävimmistä riskeistä (Valtiovarainministeriö 2021a), sekä uudestaan syksyllä yhdessä DVV:n kanssa julkishallinnon digitaalisen turvallisuuden merkittävimmiksi arvioiduista riskeistä (Valtiovarainministeriö 2021b). Syksyn 2020 kyselyssä pyydettiin arvioimaan riskiväittämiä neljästä näkökulmasta: toteutumisen todennäköisyys sekä vaikutus kunnan talouteen, maineeseen ja palveluiden saatavuuteen. Tähän selvitykseen vastasi 73 kuntaa. Syksyn 2021 kyselyssä pohjana olivat syksyn 2020 toteutetun riskikyselyn väittämät, joita oli täydennetty kyselystä saadun palautteen perusteella. Syksyn kyselyssä vastaajia oli 139, joista kuntia ja kuntayhtymiä oli 58kpl (46 %).

Syksyn 2020 vastausten perusteella merkittävimmiksi digitaalisen turvallisuuden riskeiksi nousivat laajojen tietoturvaloukkausten hallinta ja niiden johdosta mahdollisesti toteutuvaan henkilötietojen vuotamiseen. Syksyn 2021 kyselyssä vastaavan aiheisesti nousivat päällimmäisiksi riskeiksi viranomaisten toimintaan ja palveluihin kohdistuvat tahalliset vakavat tietoturvahyökkäykset, kriittiseen fyysiseen infrastruktuuriin ja tietoverkkoihin kohdistuvat vakavat väärinkäytökset,

haitanteot, sabotaasit tai tietoturvahyökkäykset, sekä kiireestä ja resursointivajeesta johtuvat tietovarantojen tietoturvan merkittävä vaarantuminen. Lisäksi riskinä nähtiin, ettei pilvipalvelujen riskejä tunneta riittävästi, jolloin niiden hallintatoimet ovat epäselviä ja tilannekuva puutteellinen.

Molemmissa kyselyissä nousi riskinä myös, ettei toimialasta vastaava johto joko ymmärrä digitaalista turvallisuutta, arvosta tai huomioi toiminnan suunnittelussa ja edelleen välttämättä toteuta riskienhallinnan kautta tunnistettuja riskienhallintatoimenpiteitä.

Syksyn 2020 kyselyssä vaikutuksiltaan suurimmiksi riskeiksi arvioitiin häiriötilanteiden jälkeisen tietojen palauttamiseen, häiriötilanteiden harjoittelemattomuuteen, sekä kriittisten tietovarantojen tietojen käsittelyyn ja siirtoon liittyvät turvallisuusriskit. Selvityksessä parantavina toimenpiteinä on esitetty kuntien toimialajohdon ja palveluita hankkivien henkilöiden digitaaliseen turvallisuuteen liittyvän osaamisen kasvattaminen ja keskitetyn osaamisen tarjoamista kunnille häiriötilanteissa. Lisäksi merkittävänä asiana nähtiin harjoitustoiminnan parantaminen sekä kriittisten tietovarantojen hallintatoimenpiteiden sekä häiriötilanteista toipumisessa tarvittavan tietojen palauttamisen hallinnan kehittäminen.

4.4 Kuntien digitaalisen turvallisuuden selvitys

Osana Digi- ja väestötietoviraston JUDO-hanketta toteutettiin kunnille kysely digitaalisesta turvallisuudesta (Valtiovarainministeriö 2020c). Kyselyssä oli tavoitteena selvittää kuntien digitaalisen turvallisuuden nykytilaa ja siihen liittyviä palvelutarpeita. Kyselyn pohjalta on laadittu Kuntien digitaalisen turvallisuuden selvitys raportti (DVV 2021a). Vastaajia oli yhteensä 98. Raportissa esitetään edelläkävijöiksi kunnat, joiden vastaustuloksista löytyi onnistumisia yhdellä tai useammalta osa-alueelta. Edelläkävijät kuvailivat itseään uudistumis- tai muutoshalukkaina ja kertoivat kaikki (100 %) osallistuvansa vuosittain TAISTO-harjoituksiin. Edelläkävijöistä jokainen käytti useampaa ulkoistettua joko kuntayhtymien ICT-toimijoiden tai kaupallisten toimijoiden palvelua.

Yksi merkittävä havainto kyselyiden mukaan oli ylimmän johdon sitoutumisen ja ymmärryksen puute tietoturvaan liittyvissä aisoissa. Tietohallinnon tai tietoturvan edustajat eivät kuulu johtoryhmään, ja näin ollen säännöllinen näkyvyys oikealla tasolla on rajallista.

Toinen merkittävä havainto raportin mukaan oli resurssien puute: Kaikki (100 %) edelläkävijöistä vastasivat, että heillä ei ole riittäviä resursseja ja 80 % vastasi, että heillä ei ole riittävää osaamista. Kokoaikaisesti tietoturvan parissa työskenteleviä asiantuntijoita ei ollut ollenkaan tai niitä oli vain muutamia. Erityisesti kaivattiin asiantuntijoita, joilla olisi kokemusta kuntasektorilta, sekä osaamista tietoturva-alalta, Microsoft 365 -palveluista ja pilviympäristöstä.

4.5 Yhdeksän digiturvaan liittyvää haastetta kuntajohdolta

Kuntaliitto toteutti keväällä 2021 kuntajohdolle suunnattuja ryhmähaastatteluja, joissa selvitettiin kuntien haasteita digitaalisten turvallisuuden alueella. Haastatteluihin osallistui kuntien ylintä johtoa ja sekä kuntien digitaalisen turvallisuuden ja riskienhallinnan johtajia. Haastattelujen pohjalta Kuntaliitto julkaisi ”9 digiturvaan liittyvää haastetta kuntajohdolta, loppuraportti” -raportin (Kuntaliitto 2021). Haastattelussa oli mukana 10 henkilöä yhdeksästä kunnasta eripuolilta Suomea. Raportin listaamat haasteet kuntajohdolle ovat aiempien valtiojohdon selvitysten kanssa samassa linjassa. Selvityksen mukaan kuntien digiturvamalli on epäselvä ja osaaminen on monesti yksilöiden varassa. Vastuuttaminen on puutteellisesta eikä digiturvan roolia ja tärkeyttä ymmärretä kuntaorganisaatiossa. Digiturvaa ei koeta koko organisaation yhteiseksi asiaksi ja vastuu digiturvasta jää usein yksilöiden käsiin, esimerkiksi turvallisuusjohtajan tai tietohallinnon henkilöille. Asiantuntijat hallitsevat digiturvakeskusteluja, josta yleisjohtaja jää herkästi sivuun. Digiturva nähdään myös helposti jarruna. Yleisjohtajat tuovat esiin, ettei digiturva saa ajaa muiden asioiden yli. Digiturvan vaatimukset asetetaan usein vastakkain sujuvuuden ja käytettävyyden vaatimusten kanssa. Lisäksi koetaan, ettei vertaistukea ole saatavilla ja johtaja saattaa jäädä vaille riittävää tukea.

5 HAASTATTELUTUTKIMUS

5.1 Haastateltavat tahot

Haastattelututkimukseen osallistui yhteensä yksitoista tahoa, joista neljä edusti kaupunkia ja yksi kaupungin energialaitosta. Viisi haastateltavaa edusti kyberturvapalveluita tarjoavia yrityksiä ja yksi valtiohallintoa. Haastattelutulokset raportoidaan anonyymisti. Kaupungeista yksi oli kooltaan yli 200 000 asukasta, yksi 100000–150000 asukasta, yksi 50 000–100 000 asukkaan kokoluokassa ja yksi alle 50000 asukasta. Energiayhtiö kuului 50 000–100 000 asukkaan kaupungille. Haastateltavat työskentelivät edustamiensa tahojen tietoturva- tai tietohallintopäällikköinä. Kaupunkien, eikä heidän edustajien nimiä tuoda esiin tietojen sensitiivisyyden vuoksi. Yritysten osalta on lupa kertoa osallistuneiden yritysten nimet, jotka olivat: Insta Advance Oy, Nixu, Fujitsu, Innofactor ja ”suuri kansainvälinen tietotekniikkayritys”. Yritysten osalta haastateltavat olivat kyberliiketoiminnasta tai -myynnistä vastaavia. Valtiohallinnon tahon haastateltava oli kyberturvallisuuden asiantuntija Digi- ja väestötietovirastosta. Jatkossa kyberturvatoimittajista ja DVV:stä puhutaan yhteisesti ”kyberturvatoimijoista”.

5.2 Aineiston kuvaus

Haastattelut suoritettiin puolistrukturoituna teemahaastatteluina, joissa muutamat kysymykset (liitteet 1–3) poikkesivat toisistaan vastaajan edustamasta tahosta riippuen. Kysymykset 1–3 olivat kaikille samoja ja näihin sisältyi myös numeraalinen arviointi. Kyberturvatoimijoiden haastattelut tehtiin ensin (liitteet 1 ja 3) ja heille esitettiin kysymys 10: ”Jos saisit esittää kunnille heidän kyberturvatilanteeseensa liittyvän yhden kysymyksen, mitä kysyisit?”. Näistä vastauksista valittiin kaksi kysymystä kuntien edustajille esitettäväksi, jotka löytyvät heidän kysymyslistastaan (liite 2) kohdista 9. ja 10. Toimittajille esitettyä kysymystä 9, jossa kysytään heidän tietoturvatarjonnastansa kunnille, ei tässä tutkimuksessa käsitellä sen enempää.

Haastattelut suoritettiin Teams-haastatteluina ja ne tallennettiin haastateltavien luvalla. Haastatteluja varten varattiin aikaa yksi tunti. Haastattelukysymykset lähetettiin etukäteen sähköpostitse tutustumista varten.

5.3 Kuntien kyberturvan varautumisaste

Haastatteluiden ensimmäisessä osiossa haettiin kuntien omaa näkemystä heihin kohdistuvista ulkoisista kyberturvauhkista, kehitysnäkymistä, mahdollisesta pahimmista katastrofista ja subjektiivista näkemystä omasta kyberturvatasosta. Tähän osioon on liitetty myös kysymys kyberjohtamisen strategiasta. Toisaalta tietoturvatoimijoilta kysyttiin, miten he näkevät omalta puoleltaan kuntiin kohdistuvat uhat. Tähän teemaan liittyen kysyttiin kunnilta myös millaisia tietoturvakontrolleja ja hallinnollisia tietoturvakäytäntöjä heillä pääpiirteittäin on.

5.3.1 Kuntiin kohdistuvat kyberturvauhat

Päällimmäisinä uhkina kunnat nostivat esille sähköpostitse tapahtuvat tietojen kalasteluviestit, joiden avulla rikolliset saavat käyttöoikeuksien kautta pääsyn joko sähköpostijärjestelmään tai riippuen käyttäjätunnuksen käyttäjäoikeuksista, jopa syvemmälle eri järjestelmiin. Näiden avulla pystytään asentamaan ja levittämään esimerkiksi kiristyshaittaohjelmia tai varastamaan tietoja. Kalasteluviestin määrät koetaan lisääntyneen merkittävästä. Palvelunestohyökkäykset ovat uhkana lähinnä haittoina, mutta niitä on ollut ja ovat opetuspuolen palveluissa etenkin riesana. Lisäksi uhkiin varautumiseen liittyvänä haasteena nähtiin näkyvyyden puute. Mikäli ei ole palvelua, jolla havaitsee hyökkääjän, niin murtautuminen saattaa jäädä huomaamatta hyvinkin pitkäksi ajaksi. Myös tietoturvaosaamisen puute nostettiin esille niin hallinnan kuin normaalin henkilöstön osalta. Yhtenä nostona oli myös se, että kunnat ostavat ulkomaisia pilvipalveluja, jonne viedään kriittisiä palveluja. Ulkomaan yhteyksien katkeaminen, esimerkiksi sabotaasin johdosta, voisi pahimmillaan merkitä hyvinkin pitkiä palvelukatkoja.

Kuntien edustajat kokevat kuitenkin, että kunnat ovat harvoin suoranainen kohde, mutta enemminkin kohdistamattomien sivuosumien uhreja. Energiapuoli on kuitenkin eri asia. Siellä kohdistettu ja valtiollinen hyökkäys koetaan riskinä.

Kunnat arvioivat kyberuhkien riskit yleisesti hieman keskikokoista suuremmaksi tasolle 3,4 (asteikoilla 1 pieni, 3 keskikokoinen, 5 suuri).

Kyberturvatoimijoiden näkemykset uhkista olivat kuntien kanssa samansuuntaisia, mutta sillä erotuksella päinvastoin kuin kunnat itse näkevät, erityisen kiinnostavina suorina kohteina. Ulkoisiksi uhiksi nostettiin kalasteluviestit ja kiristyshaittaohjelmat ja palvelunestohyökkäykset. Toimijoina nähtiin niin valtiolliset tahot kuin verkkorikollisetkin. Kuntien nähtiin olevan myös merkittäviä hybridivaikuttamisen kohteita etenkin nyt vallitsevan kansainvälisen tilanteen johdosta. Kriittiseen infraan, kuten energia- ja vesilaitoksiin kohdistuvaa uhkaa, pidettiin kohonneena. Esiin nousi myös mahdollinen puute tunnistaa ja havaita kyberhyökkäykset ja niihin liittyvä reagointikyky, sekä mahdollinen resurssipula ja osaamisen puute.

Kyberturvatoimijat arvioivat kyberuhkien riskit kuntien omaa arviointia suuremmaksi tasolle 3,75 (asteikoilla 1 pieni, 3 keskikokoinen, 5 suuri).

5.3.2 Kyberturvauhkien kehittyminen

Kyberuhkien kehittymisen osalta kunnat olivat varsin yksimielisiä siitä, että uhat kasvavat lähitulevaisuudessa. Vastaajat pohtivat, että uhkien kasvamisen nopeuteen vaikuttaa muun muassa palvelujen digitalisoitumisen kasvu (potentiaalinen hyökkäyspinta-ala kasvaa), rahallisten hyötyjen lisääntyminen ja hyökkääjien omien resurssien kasvaminen. Suomen Nato-hakemuksen jättämisen arvioitiin myös kasvattavan kyberhyökkäyksien määrää. Samalla kuitenkin toivottiin, että saturaatiopiste uhkien kasvamiseen saavutettaisiin jo pikkuhiljaa uusien kehittyvien turvaominaisuuksien ja -palveluiden myötä.

Kunnat arvioivat kyberuhkien kehitysnäkymät kasvavaksi tasolle 3,8 (1 vähenee - 3 pysyy samana - 5 kasvaa merkittävästi).

Kyberturvatoimijat olivat pääosin samoilla linjoilla kuin kuntien edustajat, eli kyberuhkat kasvavat. Yksi toimijoista poikkesi vastauksessaan ja ennusti jopa uhkien hieman vähenevän lähitulevaisuudessa. Tämän toimijan mielestä uhkien kehitys lähitulevaisuudessa riippuu pääasiassa Suomen valitsemasta turvallisuusstrategiasta; ”Mikäli päädytään Natoon, niin tullaan myös Naton kybersuojasateenvarjon alle. Meistä tulee silloin myös kohde, joita valtiolliset tahot alkavat enemmän kiusaamaan ja kunnan utiliteetit tulevat kohteeksi, mutta samalla meidän kapasiteettimme havaita ja torjua näitä paranee”. Lisäksi kyseinen kyberturvatoimija korosti, että jatkuvasti tulee uusia keinoja, joilla torjutaan uhkia. Kun järkevästi investoidaan tietoturvaan ja palvelut kehittyvät, niin riski haastateltavan mielestä alenee.

Muiden toimijoiden osalta nähtiin yhtenäisemmin, että itsessään uhkia on jatkossa yhä enemmän ja ne ovat yhä moninaisempia. Samalla myös puolustettava ympäristö monimutkaistuu ja tulee vaikeammin suojattavaksi. Huomion arvoista on huomata, että maailma kehittyy melkoisella vauhdilla teknologisesti ja tietyt kyberuhkat muutaman vuoden päästä ovat myöskin sellaisia, mitä tällä hetkellä ei vielä ole. Lisäksi koska kyberturvahyökkäyksistä on tullut liiketoimintaa, niin motivaatio tämän kasvattamiseen on suuri. Tulevaisuudenkuvana eräs toimija visioi, että ”*Parinkymmenen vuoden päästä ollaan saatu automatisoitua torjunta*.”

Kyberturvatoimijat arvioivat kyberuhkien kehitysnäkymät kasvavaksi samalla tasolle kuin kunnatkin 3,8 (1 vähenee - 3 pysyy samana - 5 kasvaa merkittävästi).

5.3.3 Mahdollisten äärimmäisten vahinkojen skenaariot

Kuntien näkemys äärimmäisestä vahingosta kyberuhkien toteutumisessa oli varsin yksimielinen. Yleisesti nähtiin lakisääteisten palvelujen toiminnan estyminen. Varsinaisena äärimmäisenä mahdollisuutena, vaikkakaan ei kovin todennäköisenä, sote-puolen potilastietojärjestelmien toimimattomuus, joka pahimmillaan voisi johtaa ihmishenkien menetykseen. Lisäksi vesilaitosten

automaatiojärjestelmien manipulointi voisi aiheuttaa suuriakin ongelmia. Pääsääntöisesti hallinnon järjestelmien toimimattomuutta ei nähty kovinkaan pahana ongelmana.

Kunnat arvioivat äärimmäisen vahingon mahdollisuutta tasolle 3,1 (1 pieni - 3 keskikokoinen - 5 suuri).

Tietoturvatoimijat nostivat myös sote-puolen ja vesilaitosten järjestelmien toimimattomuuden pahimmiksi vahinkoskenaarioiksi, joissa ihmishenkiä voisi olla vaarassa. Lisäksi nostettiin esille luottamuksen rapautuminen, joka aiheutuisi luottamuksellisten tietojen laajamittaisesta vuodosta tai tietojen manipuloinnista, jolloin tietojen oikeellisuus ja eheys menetetään.

Kyberturvatoimijat arvioivat äärimmäisen vahingon mahdollisuutta tasolle 3,3 (1 pieni - 3 keskikokoinen - 5 suuri).

5.3.4 Tietoturvakontrollit ja hallinnolliset käytännöt kunnissa

Haastateltavat kunnat kertoivat, että viimevuosien aikana tietoturvan parantamiseen on tehty paljon töitä. Perinteiset asiat kuten palomuurit, laitteiden virustorjunnat ja järjestelmien ajantasaisuus ovat perusjuttuja, jotka ovat ja tulee olla kunnossa. Tietoliikennetasolla verkot on segmentoitu. Pääsynhallintaa ja tunnusvaltuutusta on parannettu ja pääkäyttäjäoikeuksia on rajattu. Kaikilla haastateltavilla kunnilla oli myös ulkoistettuna palveluna lokien hallinta (SIEM) ja turvavalvomopalvelu (SOC). Jokainen kunta on myös suorittanut penetraatiotestauksia joko sisä- tai ulkoverkkoon tai molempiin. Testaukset on hankittu joko kaupalliselta toimijalta tai Kyberturvallisuuskeskukselta. Kaikilla oli myös käytössä monivaiheinen tunnistus (MFA) hallinnon puolella. Kuntien tapauksessa opetuspuolella haasteena on alakouluikäiset koululaiset, joilla kaikilla ei ole puhelinta käytössä ja näin ollen ei voida edellyttää heiltä monivaiheisen tunnistuksen käyttöä. Opettajilla se sen sijaan on käytössä hallintoverkon puolella. Yksittäisinä mainintoina eri kuntien osalta nostettiin esille myös erikseen palvelunestohyökkäyksien varalta hankittu palvelu, geoblokkaus ja pilviympäristön varmuuskopiointi pilvipalveluna.

Hallinnollisten tietoturvakäytäntöjen osalta esiin nousi tietoturvapolitiikkojen ja ohjeistuksien suhteen menossa oleva kehitystyö. Kaikki haastateltavat tunnistavat tietoturvapolitiikan olemassaolon, mutta vain yksi toteaa, että tietoturvapolitiikka on ajan tasalla ja tietoturvallisuuden hallintajärjestelmässä asiat ovat vastuutettu ja vastuut ovat selkeitä ja aitoja. Muilla tietoturvapolitiikat ovat enemmän tai vähemmän uudistuksen alla. Kysyttäessä löytyykö ”kyberturvallisuuden johtamisen strategiaa”, niin kukaan haastateltavista ei tällaista tunnista. Vain yksi haastateltavista kertoo, että kyberturvan osalta heillä on käytössään vuosikellotyyppinen ratkaisu, josta puhutaan strategiana. Osalta haastateltavien edustamista organisaatioista löytyy muun muassa ”digitalisaatiostrategia” ja yhdessä kunnan strategiasta löytyy maininta ”digiturva”. Kaikki haastateltavat totesivat, että strategiatasolla kyberturvasta puhutaan liian vähän ja ehdottomasti tarvittaisiin kyberjohtamisen strategia kunnan tasolle, joko omana dokumenttina tai osana kunnan kokonaisstrategiaa tai digitalisaatiostrategiaa.

Koulutuksen ja harjoittelun merkitystä korostivat kaikki haastateltavat. Henkilöstön jatkuva ja säännöllinen kehittäminen koetaan tärkeäksi ja kustannustehokkaaksi tavaksi lisätä tietoturvaa. Kunnilla on hieman eri käytäntöjä koulutuksien suhteen. Osalla on koulutuskalenteri, jossa on vuoden aikana varattu tietyt aikaikkunat ajankohtaisille tietoturvakoulutuksille. Osalla koulutuksia pidetään enemmän adhoc-tyyppisesti. Myös intrassa on saatavilla erilaisia tietoturvakoulutuksia. Taisto-harjoituksiin olivat kaikkien haastateltavien kunnat osallistuneet ja yksi taho oli järjestänyt omia harjoituksia. Haasteena harjoituksissa nähtiin vaikeus irrottautua tarvittavaksi ajaksi töistä sekä se, että harjoittelu osuu yleensä vain ylempään johtoon, eikä koko henkilöstön laajuista harjoittelua pystytä järjestämään.

5.3.5 Haastateltavien arviot oman kunnan kyberturvallisuuden tasosta.

Arviot oman kunnan kyberturvallisuuden tasosta vaihtelivat tasolta 2 tasolle 4, keskiarvon ollessa hyvää keskitasoa 3,3. (1 huono - 3 hyvää keskitasoa - 5 erittäin hyvä). Matalimman arvosanan antaja perusti arvionsa ulkopuolisen

auditoinnin tuloksena saatuun arvosanaan. Tosin henkilökohtaisesti haastattelija piti arviota kuitenkin liian alhaisena suhteessa heillä panostettuihin tietoturvahankkeisiin. Loput haastateltavat asettivat kuntansa kyberturvallisuuden tason hyvälle keskitasolle tai hieman sen yli. Perusteina oli joko ulkopuolisen suorittama auditointi, systemaattisesti tehty kehitystyö tai käyttöön otettujen mittareiden hyödyntäminen esimerkiksi Kyberturvakeskukselta. DVV:n edustaja totesi, että kuntien tietoturvatason mittaaminen tuli mukaan vuonna 2018 ja kuntien puolella on tapahtunut selvää parantumista vuosien aikana. Sote-puoli on todettu ykköseksi. Kokonaisuutena DVV:n edustaja asetti kuntien kyberturvan tasolle 3.

Haastateltavilta kysyttiin myös mikä heidän mielestään on suurin este kuntien tietoturvan toteuttamiselle, kun jätetään pois kaksi vastausta: raha ja osaajapula? Vastauksena tähän nähtiin muun muassa johtamiskulttuuri ja ymmärryksen puute tietoturva-asioissa johtotasolla. Kokonaisuuden hallinta ei ole kunnossa johtoryhmällä, jonka pitäisi viedä strategiaa ja asioita eteenpäin. Toisaalta myöskin käyttäjien vastustus, koska tietoturvan kiristäminen koetaan vaikeuttavan käyttäjien työtä.

5.4 Keskeisimmät asiat, jotka kunnissa tulisi olla kunnossa kyberuhkien torjunnassa?

Kyberturvatoimijoilta kysyttiin heidän näkemystään millaisia kyberturvakontrolleja ja hallinnollisia käytäntöjä kunnilla tulisi vähintään olla. Lisäksi millaisia lisäsuojauksia olisi hyvä harkita. Heidän mielestään vähimmäisvaatimuksena tulisi huolehtia, että kaikki tietoturvapäivitykset ovat ajan tasalla ja oletussalasanat on vaihdettu. Vanhentuneet ohjelmistot, joiden ylläpito on päättynyt, täytyisi päivittää ajantasaisiin versioihin. Virustorjunnat, palomuurit ja verkkosegmentointi ovat perusasioita. Monivaiheinen tunnistus tulisi kytkeä päälle kaikkiin niihin palveluihin, jotka ovat saavutettavissa internetin kautta. Jos henkilöille annetaan korkeampia valtuuksia (esimerkiksi pääkäyttäjätunnuksia), niin niiden voimassaoloajalle olisi hyvä asettaa automaattinen päättymisaika. On myös hyvä miettiä, onko kaikki tieto samanarvoista. Olisiko tarvetta esimerkiksi

salata tietokannat ja palvelimien levyt. Tietoliikenneyhteydet tulee olla varmennetut. Koskaan palvelut eivät saisi olla yhden kaapelin tai yhteyden päässä. Varmuuskopiot tulee olla kunnolla hoidettu ja myöskin niiden palauttamista on harjoiteltava. Osittain vähimmäisvaatimuksena nähdään myös havainnointikyky ja siihen reagoiminen. Omasta ympäristöstä tulisi olla hyvä kokonaiskuva, että pystytään havainnoimaan kaikki verkossa olevat omat laitteet, identiteetit ja tiedostot sekä saadaan signaalit joka paikasta ja lisäksi pystytään tulkitsemaan monimuotoiset uhat. Ja jos mahdollista, niin reagoimaan automaattisesti meneillään oleviin uhkiin. Hallinnollisella puolella, riippumatta minkä kokoisesta kunnasta on kyse, niin toimintatavat ja politiikat pitää olla kunnossa ja ymmärrystä, miten toimia turvallisesti. Henkilökunnan koulutus ja sitä kautta riittävä osaamisen taso ja ymmärrys tietoturvasta kuuluu vähimmäisvaatimuksiin. Jatkuva poikkeustilanteiden harjoittelu on myös yksi kouluttautumisen muoto. Yksi haastateltava nosti tärkeänä asiana ohjeistuksien ymmärrettävyyden, että ”arkijärjellä” pystytään ymmärtämään miten pitää toimia poikkeustilanteessa. Tällöin niihin pystytään myös sitoutumaan. Suositeltavina lisäpalveluina esitettiin haavoittuvuuksien hallintaa ja verkkojen skannauksia.

5.5 Kyberturvavaatimukset tulevaisuuden kaupungeille

Älykaupungeista keskusteltaessa on huomioitava, että älykaupunki-termille ei ole yhtä selkeää määritelmää, kuten aiemmin olen todennut. Toisille se on hyvinkin teknologista, toisille kestävää kehitystä ja vihreitä arvoa. Osalle jotain näiden väliltä. Haastatteluissa pyydettiin vastaajia miettimään asiaa teknologisesta, voimakkaasti digitalisoituvan kaupungin näkökulmasta.

5.5.1 Älykaupunkien (Smart City) kyberturvahaasteet.

Kuntien haastateltavat näkivät, ettei lähtökohtaisesti niin sanotulla normaalikaupungilla ja älykaupungilla pitäisi olla eroa kyberturvahaasteissa. Älykaupunkiin haastateltavat liittävät erilaiset sensorit, IoT-laitteet, massiiviset tiedonsiirtotarpeet ja digitaaliset palvelut. Toisaalta normaalikaupunkien

digitaaliset palvelut lisääntyvät. Mitä enemmän erilaisia digitaalisia järjestelmiä ja -palveluita älykaupungissa on, sen suuremmaksi kasvaa mahdollinen hyökkäyspinta-ala, aivan samoin kuin normaalikaupungissakin. Sen sijaan haasteena nähdään tapa hankkia digitaalisia palveluita ohi tietohallinnon. Toimialat pilotoivat mielellään uusia älykkäitä ratkaisuja ja pelkona on, että kyseiset pilotit jäävätkin tuotantoon, vaikka eivät mahdollisesti täytä kaikkia tietoturvavaatimuksia. Olisi tärkeää, ettei älykaupunkiratkaisuja tehdä millään epämääräisillä virityksillä. Iso riski on, että tietoturvan osalta oikaistaan ja onnistunut demo siirretään sellaisenaan suoraan tuotantokäyttöön. Toimittajia on paljon ja osa melko pieniä. Järjestelmiä ei päivitetä ja mahdollisesti sopimuksissa ei edes vaadita toimittajilta ylläpitoa. Kun tietohallinto on jätetty hankinnassa sivuun, heillä ei ole edes tietoa mitä on hankittu. Järjestelmät saattavat jäädä tietoturvakontrollien ulkopuolelle, jolloin mahdollisia tietoturvaloukkauksia ei pystytä havaitsemaan. Energialaitoksilla älyä viedään yhä enemmän energiavirtojen hallintaa, joka lisää haavoittuvuutta. Haastateltava kertoi kuitenkin, että jokainen sähköverkkoyhtiö pystyy auttavasti toimimaan myös manuaalisesti irrottamalla sähköverkon ohjauksen internetistä ja ohjaamalla sähkönsiirtoa käsikytkimillä. Kriittinen paikka toki voisi olla, jos joku pääsisi sulkemaan Suomen kaikki etäluettavat sähkömittarit.

Kyberturvatoimijat näkevät älykaupunkien osalta haasteena erityisesti verkossa olevien mitä moninaisempien IoT-laitteiden ja sensoreiden määrien lisääntymisen. Kun hyökkäyspinta-ala kasvaa, niin uhkavektoritkin lisääntyvät. Nämä pitää huomioida perinteisessä suunnittelussa, kuten ohjelmistoprojekteissa ja palvelumuotoilussa. Tietoturvan tulee olla sisään rakennettuna Secure by Design -ajattelumallilla. Ja kun ympäristö monimutkaistuu hyvinkin paljon, niin iso kysymys on, miten kokonaisuutta pystytään kunnolla ylläpitämään. Mahdollinen hybridivaikuttaminen nousi vastauksissa myös esille. Esimerkiksi mahdollisen kyberhyökkäyksen kautta infotauluihin ja vastaaviin pääsisi hyökkäävä taho levittämään omaa disinformaatiota ja massatapahtumissa mahdollisesti aiheuttamaan kaaosta.

Eräs vastaaja näki kyberturvallisuuden, fyysisen turvallisuuden, dataturvallisuuden ja tietosuojaan liittyvät asiat yhdistyvän yhä vahvemmin yhdeksi kokonaisuudeksi. Hänen mielestään olisi jossain määrin jopa vähän keinotekoista erotella, mikä on kyberjuttua ja mikä muuta turvallisuutta ja mikä on tietosuojaa. Se on kaikki tietyllä tapaa samaa kokonaisuutta ja se pakottaa pohtimaan näitä asioita yhä holistisemmin. Oli nyt sitten älykaupunki tai älyliikenne, niin vastaajan mielestä olemme matkalla yhä enemmän maailmaan, jossa tämä teknologia on ubiikkia eli on läsnä kaikkialla ja silloin se ikään kuin integroituu melkein mihin vaan.

Yhtenä mahdollisena haasteena nähtiin myös tilanne, jossa tulevaisuuden älykaupungin eri järjestelmät tuotetaan samalta älykkäältä alustalta, jonka kautta sisään päässyt hyökkääjä voisi sammuttaa koko kaupungin.

5.5.2 IoT- järjestelmien kyberturvasuojauksia

Kuntien edustajilta kysyttiin, miten he ovat suojanneet IoT-järjestelmänsä. Kyberturvatoimijoilta kysyttiin, millaisia suosituksia he antaisivat IoT-järjestelmien suojaamiseen. Kaikki haastateltavat olivat hämmästyttävän yhtä mieltä siitä, että IoT tulee olemaan suuri tietoturvauhka lähitulevaisuudessa. Järjestelmiä on jo paljon käytössä ja erityisen ongelmallisia niistä tekee, kuten aiemmassa kappaleessa kerrottiin, että niitä hankitaan ohi tietohallinnon. Eräs haastateltava toteaa muun muassa, että ”*järjestelmät ovat monesti hyvinkin heikon pääsynhallinnan takana ja varsinkin talotekniikkaan liittyvissä logiikoissa on laajalti tunnettuja tietoturva-aukkoja, joita ei todennäköisesti koskaan tulla päivittämään, koska talonmiehet ja vastaavat, jotka hoitavat näitä laitteita, eivät koe tarpeellisiksi ylläpitää niitä. Monia laitteita ajetaan niin vanhalla firmwarella, että ne ovat hakkeroitavissa helposti*”.

Haastateltavat toteavat myös, että IoT-järjestelmät ja etenkin erilaiset sensorit ovat laskentateholtaan niin heikkoja, ettei niihin voida asentaa mitään tietoturvaohjelmistoa. Tähän liittyen varsin yksiselitteisesti haastateltavat toteavat, että tehokkain keino on huolehtia verkkosegmentoinnista, jossa

taloautomaatio- ja muut IoT-laitteet kytketään niin sanottuun tekniikkaverkkoon, joka on eristetty muista hallinto- ja sisäverkoista. Toisena tärkeä asiana nähtiin mekanismi, joka mahdollistaisi näiden laitteiden päivittämisen, haavoittuvuuden skannaukset ja havainnoinnin.

Esille nostettiin isojen valmistajien järjestelmiä, joilla on kyvykkyys ottaa IoT-laitteet mukaan samoihin hallintajärjestelmiin, kuin muutkin verkon laitteet. Erikoispiirteenä IoT-laitteissa on, että niissä on lukematon määrä erilaisia protokollia ja hallintajärjestelmien tulisi pystyä tukemaan niitä. Esimerkkinä on hallintajärjestelmä, jossa yksittäisten IoT-laitteiden verkkoliikennettä voidaan seurata kytkimeltä. Kytkinportti, johon IoT-laite on kytketty, peilataan kytkimen sisällä ja näin nähdään mihin sillä liikennöidään ja mitä se tekee.

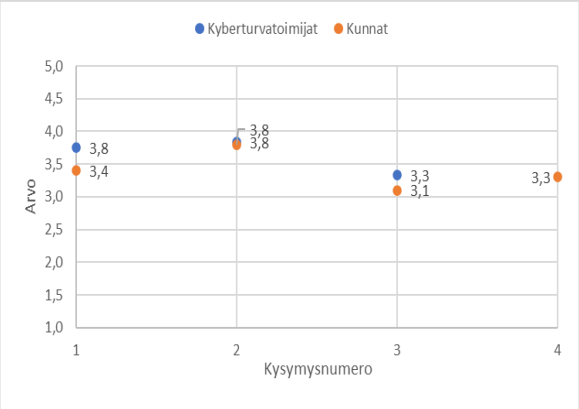
Lisäksi hallinnollisesti on erityisen tärkeää varmistaa, että jokaisella järjestelmällä on nimetty vastuuhenkilö, joka huolehtii niistä. Hankintaprosessi nähtiin myös kriittisenä pisteenä. Hankinnassa tulee varmistaa, että laitteita hankitaan vastuullisilta toimittajilta, joilla jatkossa on sekä halukkuus, että kyvykkyys ylläpitää laitteita ja ohjelmistoa.

Yllä olevien vastauksien pohjalta on koottu seuraavalla sivulle oleva hieman mukaeltu SWOT-taulukko, joka tiivistää haastatteluvastaukset.

Vahvuudet (haastateltavien kuntien osalta)	Heikkoudet (kunnissa yleisemmin)
• Jatkuva tietoturvan parantamisen kulttuuri. • Palomuurit, laitteiden virustorjunnat ja järjestelmien ajantasaisuus (tietoturvapäivitykset ja ohjelmistoversiot) ovat kunnossa. • Varmuuskopioinnit kunnossa. • Tietoliikenneverkot on segmentoitu. • Pääsynhallintaa ja tunnusvaltuutusta on parannettu ja pääkäyttäjäoikeuksia on rajattu. • Lokien hallinta (SIEM) ja turvavalvomopalvelu (SOC) käytössä. • Jokainen kunta on myös suorittanut penetraatiotestauksia. • Monivaiheinen tunnistus (MFA) hallinnon puolella käytössä. • Palvelunestohyökkäyksien estopalvelu, geoblokkaus ja pilviympäristön varmuuskopiointi. • Henkilöstön jatkuva ja säännöllinen kehittäminen. • Arviot oman kunnan kyberturvallisuuden tasosta hyvää keskitasoa. • Kunnat ovat harvoin kyberhyökkäyksien suoranainen kohde	• Puute tunnistaa ja havaita kyberhyökkäykset yleisesti. • Tietoturvaosaamisen taso henkilöstön osalta. • Puolustettava kyberympäristö entistä monimutkaisempi. • Tietoturvapolitiikat ja ohjeistukset ovat enemmän tai vähemmän vielä uudistuksen alla. • Kyberturvallisuuden johtamisen strategiaa ei varsinaisesti ole. • Tietoturvan johtamiskulttuuri ja ymmärrys johdon tasolla puutteellista. • (Äly)kaupunkien haasteena toimialojen tapa hankkia digitaalisia palveluita ohi tietohallinnon. • Loppukäyttäjien vastustus tietoturvavaatimuksia kohtaan, koska tietoturvan kiristäminen koetaan vaikeuttavan käyttäjien työtä. • Raha ja resurssit
Mahdollisuudet (parantaa kuntien tietoturvaa ja resilienssiä)	**Uhat (kunnissa yleisemmin)**
• Huolehtimalla ”Vahvuudet” nelikentässä olevat perusasiat kuntoon. • Varmuuskopioiden palautuksen testaus. • Tietokantojen ja palvelimien levyjen salaus. • Kyberjohtamisen strategia kunnan tasolle, joko omana dokumenttina tai osana kunnan kokonaisstrategiaa tai digitalisaatiostrategiaa. • Jatkuva henkilökunnan koulutus ja poikkeustilanteiden harjoittelu. • (Äly)kaupunkien digitaalijärjestelmien verkkosegmentointi, jossa taloautomaatio- ja muut IoT-laitteet kytketään niin sanottuun tekniikkaverkkoon irti hallinto- ja muusta verkosta. • IoT -laitteiden hallintajärjestelmät, jotka mahdollistavat näiden laitteiden päivittämisen, haavoittuvuuden skannaukset ja havainnoinnin. • Hankintaprosessi, joka varmistaa, että IoT-laitteita ja muitakin järjestelmiä hankitaan vastuullisilta toimittajilta ja joilla jatkossa on sekä halukkuus, että kyvykkyys päivittää laitteita. • Jokaiselle verkkoon asennettavan järjestelmän ylläpidon ja tietoturvan osalta tulee tulee nimetä vastuuhenkilö.	• Sähköpostitse tapahtuvat tietojen kalasteluviestit. • Kiristyshaittaohjelmat ja palvelunestohyökkäykset. • Uhat kasvavat lähitulevaisuudessa digitalisoitumisen kasvun, rahallisten hyötyjen lisääntymisen ja hyökkääjien omien resurssien kasvamisen johdosta • Hybridivaikuttamisen lisääntyminen ja kriittiseen infraan kohdistuvien hyökkäysten riski koholla kansainvälisen tilanteen johdosta. • Uhat monimuotoistuvat ja teknologian kehittymisen myötä aivan uusia vielä tunnistamattomia uhkia tulee ilmenemään. • Ulkomaiset pilvipalvelut, johon viedään kunnan kriittisiä palveluja. • Lakisääteisten palvelujen toiminnan estyminen ja sote-puolen potilastietojärjestelmien toimimattomuus ovat pahimmat skenaariot. • Kansalaisten luottamuksen rapautuminen luottamuksellisten tietojen laajamittaisen vuotojen seurauksena tai tietojen manipuloinnin johdosta. • (Äly)kaupunkien lisääntyvät IoT-järjestelmät ja niiden huonot tietoturvaominaisuudet ja näistä johtuva hyökkäyspinta-alan kasvu.

Kuva 4. SWOT taulukko haastatteluvastauksista.

Kuvassa 5 on esitetty keskiarvot numeraalisista vastauksista neljän ensimmäisen kysymyksen osalta:



1. Mitkä ovat mielestäsi merkittävimpiä kyberuhkia suomalaisille kunnille yleisesti ja miten suurena riskinä pidät näitä kyberuhkia suomalaisten kuntien näkökulmasta tällä hetkellä asteikolla 1-5 (1 pieni - 3 keskikokoinen - 5 suuri)?

2. Miten arvioisit kyberuhkien kehitysnäkymiä suomalaisten kuntien osalta asteikolla 1-5 ? (1 vähenee - 3 pysyy samana - 5 kasvaa merkittävästi)?

3. Millaisena pidät mahdollista äärimmäistä vahinkoa, joka voisi kunnalle kyberuhan kohteeksi joutumisesta syntyä ja kuinka mahdollisena pidät kyseistä katastrofivahinkoa kuntien näkökulmasta tällä hetkellä asteikolla 1-5 (1 pieni - 3 keskikokoinen - 5 suuri)?

4. (esitetty vain kunnille) Millaisena pidät teidän kunnan kyberturvallisuuden tasoa asteikolla 1-5 (1 huono - 3 hyvää keskitasoa - 5 erittäin hyvä)?

Kuva 5: Vastauksien keskiarvot

6 YHTEENVETO

Tämän tutkimuksen tavoitteena oli selvittää, millaisia kyberuhkakuvia Suomen kuntakenttään kohdistuu, miten kunnissa mahdollisiin kyberhyökkäyksiin on varauduttu, sekä millaisia ratkaisumahdollisuuksia tilanteen parantamiseen on tarjolla. Lisäksi tarkasteltiin millaisia lisähaasteita tulevaisuuden älykaupungit mahdollisesti tuovat kyberturvauhkien torjumiseen.

Tutkimuksessa selvitettiin aluksi kyber-käsitettä ja sen historiaa laaja-alaisesti monesta eri näkökulmasta. Näin saatiin luotua pohja, mistä tutkimusaihepiirissä on kysymys. Kyberrikollisuuden uhat ja toimijat tuodaan esille seikkaperäisesti hyödyntäen muun muassa Jewkes ja Yar (2010), Peltomäki ja Norppa (2015) ja Limnéll ym. (2014) julkaisuja, sekä Ponemon instituutin (IBM Security 2021), ENISA:n (2021), Deep Instinctin (2021) ja poliisin (Sisäministeriö 2021) raportteja.

Tietoturvaan liittyvää lainsäädäntöä sekä julkisen hallinnon tietoturvan kehittämisohjelmia tarkasteltiin omana kokonaisuutena. Yhteenvetona näistä voidaan todeta, että Suomessa on tehty systemaattisesti työtä valtiohallinnon tasolla kyberturvallisuuden eteen viimeisen kymmenen - viidentoista vuoden aikana. Kyberturvallisuus oli esillä jo vuoden 2010 yhteiskunnan turvallisuusstrategiassa (Puolustusministeriö 2010). Haasteena lainsäädännön näkökulmasta on kyberrikollisuuden nopea kasvu ja monimuotoisuus. Kyberrikollisuus koetaan kulkevan koko ajan askeleen edellä lainsäädäntöä.

Julkishallinnolle tehdyt tutkimukset ja niiden tulokset muodostivat oman teoreettisen tarkastelupohjan. Haukka hankkeessa (Valtiovarainministeriö 2020a) ja sen puitteissa käynnistetyssä Digi- ja väestötietoviraston JUDO-hankkeessa (DVV 2019) toteutettiin vuosina 2020 ja 2021 kyberturvallisuuden tilaa koskevia kyselyitä ja tutkimuksia. Lisäksi Kuntaliitto toteutti yhden tutkimuksen keväällä 2021 (Kuntaliitto 2021).

Tutkimuksen empiirinen osuus toteutettiin puolistrukturoituna teemahaastatteluina, jossa vastaajina olivat kuntien tietohallinnosta tai -turvasta

vastaavat henkilöt. Lisäksi haastateltiin tietoturvatoimittajien sekä DVV:n edustajia.

Tutkielman ensimmäisessä tutkimuskysymyksessä paneuduttiin kuntakenttään kohdistuviin kyberuhkiin. Selvityksen perusteella kyberrikollisuuden toimijat voidaan jakaa viiteen kategoriaan; kybervandalismiin, kyberrikollisuuteen, kybervakoiluun, kyberterrorismiin sekä kyberoperaatioihin. Samalla tavalla voidaan myös kategorisoida mahdolliset toimijat: yksittäiset hakkerit, ideologiset hakkerit, rikollisryhmittymät, kyberterroristit ja valtiolliset tahot. Tutkimuksessa selviää, että kyberturvatilanne on Suomessa ja maailmalla raporttien mukaan huonontunut. Kyberturvayhtiön Deep Instinctin (2021) julkaiseman ”2020 Cyber Threat Landscape Report” -raportin mukaan vuonna 2020 todistettiin malware ja ransomware hyökkäysten merkittävää kasvua. Vuodesta 2019 vuoteen 2020 malware hyökkäykset lisääntyivät 358 % ja ransomware hyökkäykset 435 %.

Haastateltavien mielestä kyberturvauhat ovat edelleen kasvava trendi. Uhkan kasvuun nähtiin vaikuttavan kansainvälinen kiristynyt tilanne, kyberrikollisuuden muuttuminen selvästi liiketoiminnaksi ja kyberrikollisten resurssien ja teknologian kehittyminen.

Päällimmäisinä ulkopuolisina uhkina kunnat nostivat esille sähköpostitse tapahtuvat tietojen kalasteluviestit, joiden avulla pystytään asentamaan ja levittämään esimerkiksi kiristyshaittaohjelmia tai varastamaan tietoja. Tätä näkemystä tukee myös ENISA:n raportti (2021), jossa suurimpina uhkina mainitaan muun muassa kiristyshaittaohjelmat, kryptokaappaus, sähköpostiin liittyvät uhat sekä disinformaatio. Muina merkittävinä uhkina nähdään havainnoinnin puute, resurssipula sekä osaaminen. Lisäksi kuntien digitaalisen turvallisuuden riskikyselyissä (Valtiovarainministeriö 2021a) ja (Valtiovarainministeriö 2021b) merkittävimmiksi riskeiksi nousivat laajojen tietoturvaloukkausten hallinta ja niiden johdosta mahdollisesti toteutuvan henkilötietojen vuotamisen. Myös kriittiseen infrastruktuuriin kohdistuvat hyökkäykset nostettiin esille.

Organisaation sisältä vaikuttavaan kyberturvallisuuteen nousi esille ylimmän johdon sitoutumisen sekä ymmärryksen puute tietoturvaan liittyvissä aisoissa (Valtiovarainministeriö 2021b). Tietohallinnon tai tietoturvan edustajat eivät kuulu johtoryhmään ja näin ollen säännöllinen näkyvyys oikealla tasolla on rajallista. Kuntaliiton 2021 kuntajohdolle toteuttamassa haastattelussa (Kuntaliitto 2021) kuntien digiturvamalli koettiin epäselväksi. Vastuuttaminen on puutteellisesta, eikä digiturvan roolia ja tärkeyttä ymmärretä kuntaorganisaatiossa. Digiturvaa ei koettu koko organisaation yhteiseksi asiaksi ja vastuu digiturvasta jää usein yksilöiden käsiin, esimerkiksi turvallisuusjohtajan tai tietohallinnon henkilöille.

Mahdollisen kyberuhkan toteutuessa pahimmiksi skenaarioiksi koettiin yleisesti lakisääteisten palvelujen toiminnan estyminen sekä sote-puolen potilastietojärjestelmien toimimattomuus että vesilaitosten automaatiojärjestelmien mahdollinen manipulointi.

Toisena kysymysaiheena oli selvittää kuntien kyberturvan varautumisastetta ja mitkä ovat keskeisimmät asiat, jotka kunnissa tulisi olla kunnossa kyberuhkien torjunnassa.

Haastateltavat kunnat olivat pääsääntöisesti tehneet paljon töitä tietoturvan parantamiseen ja perusasiat kuten palomuurit, laitteiden virustorjunnat ja järjestelmien ajantasaisuus olivat kunnossa. Tietoliikennetasolla verkot on segmentoitu. Pääsynhallintaa ja tunnusvaltuutusta on parannettu ja pääkäyttäjäoikeuksia on rajattu. Kaikilla haastateltavilla kunnilla oli myös ulkoistettuna palveluna lokien hallinta (SIEM) ja turvavalvomopalvelu (SOC). Monivaiheinen tunnistus oli myös otettu käyttöön. Nämä asiat olivat myös kyberturvatoimijoiden esille nostamia vähimmäisvaatimuksia. Lisäksi korostettiin, että kaikki oletussalasanat tulee vaihtaa. Vanhentuneet ohjelmistot, joiden ylläpito on päättynyt, täytyisi päivittää ajantasaisiin versioihin. Jos henkilöille annetaan korkeampia valtuuksia (esimerkiksi pääkäyttäjätunnuksia), niiden voimassaoloajalle olisi hyvä asettaa automaattinen päättymisaika. On myös hyvä miettiä, onko kaikki tieto samanarvoista. Olisiko tarvetta esimerkiksi salata tietokannat ja palvelimien levyt. Tietoliikenneyhteydet tulee olla varmennetut. Jatkuvuuden varmistamiseksi palvelut eivät koskaan saisi olla yhden kaapelin tai

yhteyden päässä. Varmuuskopiot tulee olla asianmukaisesti hoidettu ja niiden palauttamista on harjoiteltava. Suositeltavina lisäpalveluina esitettiin haavoittuvuuksien hallintaa ja verkkojen skannauksia.

Henkilökunnan jatkuva koulutus ja sitä kautta riittävä osaamisen taso ja ymmärrys tietoturvasta kuuluu myös vähimmäisvaatimuksiin. Jatkuva poikkeustilanteiden harjoittelu on myös erittäin tärkeää.

Kehityskohteena nousi esille hallinnolliset tietoturvakäytännöt liittyen tietoturvapolitiikkojen ja ohjeistuksien päivityksiin sekä mahdollisen kyberturvallisuuden johtamisen strategian laadinta. Myös kyberturvan johtamiskulttuuria ja ymmärryksen lisäämistä johtotasolla haluttaisiin kehittää. Samoilla linjoilla olivat myös haastatellut kyberturvatoimijat sekä DVV:n kuntien digitaalisen turvallisuuden selvitykseen vastanneet tahot.

Digitaalisen turvallisuuden kustannusvaikutusarviointikyselyssä (Valtiovarainministeriö 2020c) esiin nousseiden asioiden johdosta selvityksessä suositellaan, että julkisen hallinnon organisaatioiden tulisi arvioida organisaation digitaalisen turvallisuuden vaikuttavuutta säännöllisesti ja tunnistaa organisaation toimintaan kohdistuvat riskit, sekä kohteet, joita riskeiltä halutaan suojella.

Haastatteluun osallistuneiden kuntien edustajat pitivät omien kuntien kyberturvauhkiin varautumisen tasoa ylipäänsä hyvänä.

Kolmantena osa-alueena tarkasteltiin millaisia lisähaasteita tulevaisuuden älykaupungit tuovat kyberturvauhkien torjumiseen. Tässä työssä ”älykaupunki” -käsitettä käsiteltiin osana normaalia kaupunkia, jossa älykkäitä digitaalisia ratkaisua on otettu käyttöön tai suunnitellaan otettavan käyttöön.

Älykaupunkien kyberturvahaasteiden osalta haastateltavat näkivät, ettei lähtökohtaisesti niin sanotulla normaalikaupungilla ja älykaupungilla pitäisi olla eroa. Älykaupungeissa korostuu erilaisten digitaalisten järjestelmien määrä ja toisaalta myös normaalikaupunkien digitaaliset palvelut lisääntyvät. Tämä kasvattaa mahdollista hyökkäyspinta-alaa. Älykaupunkien haasteena nähdään

erityisesti tapa hankkia digitaalisia palveluita ohi tietohallinnon. Isona riskinä nähdään, että tietoturvan osalta oikaistaan, kun hankinnassa ei ole mukana tietoturvan ammattilaisia. Kun tietohallinto jätetään hankinnassa sivuun, heillä ei ole tietoa mitä on hankittu, eikä siten myöskään näkyvyyttä mahdollisiin tietoturvaloukkauksiin. Yhä enenevässä määrin käyttöönotettavia IoT-järjestelmiä pidettiin suurena tietoturvauhkana lähitulevaisuudessa. Tähän liittyen varsin yksiselitteisesti haastateltavat totesivat, että tehokkain keino tällä hetkellä on huolehtia verkkosegmentoinnista, jossa taloautomaatio- ja muut IoT-laitteet kytketään niin sanottuun tekniikkaverkkoon, joka on eristetty muista hallinto- ja sisäverkoista. Lisäksi hallinnollisesti on erityisen tärkeää varmistaa, että jokaisella järjestelmällä on nimetty vastuuhenkilö, joka huolehtii niistä. Hankintaprosessissa tulee myös varmistaa, että laitteita hankitaan vastuullisilta toimittajilta, joilla jatkossa on sekä halukkuus, että kyvykkyys ylläpitää laitteita ja ohjelmistoa.

Tutkimustuloksien perusteella kunnissa on tehty paljon työtä kyberuhkiin varautumiseen. Haastateltujen kuntien osalta tilanne oli varsin hyvä, mutta kehitettävääkin riittää. Tutkimus ei kuitenkaan ole aukoton ja tilanne monissa pienissä kunnissa ei välttämättä ole näin hyvällä tasolla. Suositukset kyberturvan parantamiseksi pätevät kuitenkin kaikille kunnille. Tutkimuksen validiteettia parantaa myös se, että tutkimuksessa hyödynnettiin varsin laaja-alaisesti saatavilla olevia kyberturvaraportteja, kunnallishallintoon tehtyä tutkimuksia sekä usean kunnan ja kyberturvatoimijan haastattelu.

Tulevaisuudessa tämän tutkimuksen voisi toteuttaa kattavammin valitsemalla tutkimusmenetelmään lisäksi verkkopohjaisen kyselyn, joka lähetetään kaikille kunnille. Tässä kyselyssä voitaisiin kysyä tarkemmalla tasolla rasti ruutuun menetelmällä, mitä tietoturvakontrolleja kunkin vastaajan kunnassa on käytössä. Näin ollen tutkimus yleistyisi vielä paremmin kaikkiin suomalaisiin kuntiin.

Lähteet

Check Point 2021. Kyberhyökkäykset ovat yleistyneet 29 % viime vuoden alkupuoliskoon verrattuna. Viitattu 14.2.2022 https://www.epressi.com/tiedotteet/tietotekniikka/kyberhyokkaykset-ovat-yleistyneet-29-viime-vuoden-alkupuoliskoon-verrattuna.html

Craigen, D.; Diakun-Thibault, N. & Purse, R. 2014. Technology Innovation Management Review. Defining cybersecurity. Viitattu 20.11.2021 https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014

Deep instinct 2021. 2020 Cyber threat Landscape Report. Viitattu 19.11.2021 2020 Cyber Threat Report (deepinstinct.com)

DVV 2019. Viitattu 22.12.2021 JUDO-hanke | Digi- ja väestötietovirasto | Digi- ja väestötietovirasto (dvv.fi)

DVV 2020b. Julkishallinnon digitaalisen turvallisuuden kansallisen harjoitustoiminnan nykytilan kuvaus. Viitattu 31.1.2022 https://dvv.fi/documents/16079645/0/Julkishallinnon+digitaalisen+turvallisuuden+harjoitustoiminnan_nykytilakuvaus.pdf/

DVV 2021a. Kuntien digitaalisen turvallisuuden selvitys. Viitattu 12.11.2021 https://dvv.fi/documents/16079645/17634906/Raportti%20-%20Kuntien%20digitaalisen%20turvallisuuden%20selvitys.pdf/ede8c7c4-9509-8977-92c8-9127a0fd091e/Raportti%20-%20Kuntien%20digitaalisen%20turvallisuuden%20selvitys.pdf?t=1616745436358

DVV 2021b. Viitattu 31.1.2021 https://dvv.fi/documents/16079645/17634906/Digitaalisen+turvallisuuden+harjoitustoiminnan+tavoitetilakuvaus_2021.pdf/

Enisa 2021. Threat Landscape 2021. Viitattu 14.1.2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Eskola, J & Suoranta, J. 2014. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino

European Comission a, NIS Directive. Viitattu 27.12.2021 NIS Directive | Shaping Europe's digital future (europa.eu)

European Comission b. Smart City. Viitattu 14.1.2022 https://ec.europa.eu/info/eu-regional-and-urban-development/topics/cities-and-urban-development/city-initiatives/smart-cities_en

European Comission c. Cybercrime. Viitattu 20.12.2020 https://ec.europa.eu/home-affairs/what-we-do/cybercrime_en

GDPR. Euroopan parlamentin ja neuvoston asetus (eu) 2016/679. Viitattu 8.2.2022 https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Hirsjärvi, S; Remes, P & Sajavaara, P. 1997. Tutki ja kirjoita. Tampere: Tammer-Paino Oy

HP wolf Security 2021. Blurred lines and blindspots. Viitattu 12.12.2021 https://press.hp.com/content/dam/sites/garage-press/press/press-releases/2021/wolf-security-and-flexworker/2021_HP_Wolf_Security_Blurred_Lines_Report.pdf

Huoltovarmuuskeskus 2020, Kyber2020-ohjelma. Viitattu 5.11.2021 2.kyber-2020-loppuraportti.pdf (huoltovarmuuskeskus.fi)

Huoltovarmuuskeskus 2021. Digitaalinen turvallisuus 2030. Viitattu 31.12.2021 Digitaalinen turvallisuus 2030 - Huoltovarmuuskeskus

IBM Security 2021. Cost of a Data Breach Report 2021. Viitattu 21.11.2021 https://www.ibm.com/security/data-breach

Ilta-Sanomat 2022. Hakkerikollektiivi julistaa ”kyber-sodan” Venäjää vastaan. Viitattu 18.5.2022 https://www.is.fi/digitoday/tietoturva/art-2000008642757.html

IMD 2021. IMD Smart City report 2021. Viitattu 5.2.2022 Documents of Smart City Index (imd.org)

Jewkes, Y. & Yar M. 2010. Handbook of Internet Crime. Cullompton, UK; Portland, Or.: Willan

Kuntaliitto 2019. Tiedonhallintalaki. Viitattu 27.12.2021 Tiedonhallintalaki astuu voimaan vuodenvaihteessa - mitä se tarkoittaa kuntasektorille? | Kuntaliitto.fi

Kuntaliitto 2021. 9 digiturvaan liittyvää haastetta kuntajohdolta, loppuraportti. Viitattu 31.1.2022 https://www.kuntaliitto.fi/sites/default/files/media/file/9%20digiturvaan%20liittyv%C3%A4%C3%A4%20haastetta%20kuntajohdolta%20-loppuraportti.pdf

Kuntaliitto 2021a. Kaupunkien ja kuntien lukumäärät ja väestötiedot. Viitattu 8.2.2022 https://www.kuntaliitto.fi/tietotuotteet-ja-palvelut/kaupunkien-ja-kuntien-lukumaarat-ja-vaestotiedot

Kyberturvakeskus 2021. Varoitus 5/2021. Viitattu 8.2.2022 Log4j-komponentin haavoittuvuus on aktiivisen hyväksikäytön kohteena - päivitä välittömästi! | Kyberturvallisuuskeskus

Kyberturvakeskus 2022. Varoitus 1/2022 - FluBot-haittaohjelmaa levitetään jälleen tekstiviestitse. Viitattu 18.5.2022 https://www.kyberturvallisuuskeskus.fi/fi/varoitus_1/2022

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Viitattu 27.12.2021 https://www.finlex.fi/fi/laki/alkup/2019/20190906

Laki sähköisen viestinnän palveluista 7.11.2014/917. Viitattu 8.2.2022 https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#L20

Lewis, J. 2018. McAfee. Economic Impact of Cybercrime - No Slowing Down. Viitattu 19.11.2021 https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf

Liikenne- ja viestintäministeriön julkaisuja 7/2016. Suomen tietoturvallisuusstrategia. Viitattu 31.12.2021 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/78106/Julkaisuja_7-2016.pdf

Liikenne- ja viestintäministeriö 2021. Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Viitattu 8.2.2022 https://julkaisut.valtioneuvosto.fi/handle/10024/162783

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

LVV 2021. Kyberturvallisuuden kehittämisohjelma. Viitattu 5.11.2021 Kyberturvallisuuden kehittämisohjelma - Valto (valtioneuvosto.fi)

Opitietosuojaa.fi. Viitattu 27.12.2021 EU:n yleinen tietosuoja-asetus (GDPR) muuttaa kansalliset käytännöt (opitietosuojaa.fi)

Peltomäki, J & Norppa, K. 2015. Rikos meni verkkoon. Helsinki: Talentum

Puolustusministeriö 2010. Yhteiskunnan turvallisuusstrategia. Viitattu 5.11.2021 https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia-2010/

Puolustusministeriö 2015. Suomalaisen tiedustelulainsäädännön suuntaviivoja. Viitattu 5.11.2021 Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf (defmin.fi)

RISKIQ 2019. The Evil Internet Minute 2019. Viitattu 19.11.2021 https://www.riskiq.com/resources/infographic/evil-internet-minute-2019/

Ronikonmäki, N. & Sirviö, T. 2021. Kansantaloudellinen aikakauskirja – 117. vsk. – 2/2021. Taloustieteellisiä näkökulmia kyberturvallisuuteen. Viitattu 21.11.2021 (https://www.taloustieteellinenyhdistys.fi/wp-content/uploads/2021/06/KAK_2_2021_WEB-127-140.pdf

Sisäministeriö a. Kyberrikollisuus. Viitattu 10.12.2021 Kyberrikollisuus - Sisäministeriö (intermin.fi)

Sisäministeriö b. Rikollisuus. Viitattu 17.12.2021 https://sisainenturvallisuus.fi/rikollisuus

Sähköisen viestinnän tietosuojalaki 516/2004. Viitattu 8.2.2022 https://finlex.fi/fi/laki/alkup/2004/20040516

Tietosuojalaki 5.12.2018/1050. Viitattu 8.2.2022 https://www.finlex.fi/fi/laki/ajantasa/2018/20181050#L6P37

Tietosuojavaltuutetun toimisto a. Viitattu 25.11.2021 https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto b. Korjaavat toimivaltuudet. Viitattu 27.12.2021 Korjaavat toimivaltuudet | Tietosuojavaltuutetun toimisto

Tietoyhteiskuntakaari 917/2014. Viitattu 8.12.2022 https://www.finlex.fi/fi/laki/alkup/2014/20140917

Tivi 2021a. Nyt tuli vakava varoitus: uudelle java-haavoittuvuudelle alttiina satoja miljoonia laitteita – ”eräs pahimmista, ellei pahin”. Viitattu 9.2.2022 https://www.tivi.fi/uutiset/nyt-tuli-vakava-varoitus-uudelle-java-haavoittuvuudelle-alttiina-satoja-miljoonia-laitteita-eras-pahimmista-ellei-pahin/fbb8c73d-79c4-4b08-9f29-72c463325f79

Tivi 2021b. Varo tällaisia huijauspuheluita – Poliisi: ihmisiltä viety yli 200 000 euroa. Viitattu 8.2.2022 Huijauspuhelut piinaavat suomalaisia – poliisi varoittaa | Tivi

Tivi 2022a. Jarno Limnéll valaisee Venäjän kybersodan taktiikkaa – Nato luo suomalaisille yrityksille mahdollisuuden läpimurtoon. Viitattu 1.6.2022 Jarno Limnéll valaisee Venäjän kybersodan taktiikkaa – Nato luo suomalaisille yrityksille mahdollisuuden läpimurtoon | Tivi

Turun kaupunki. Smart&Wise. Viitattu 25.11.2021 https://www.turku.fi/smart-and-wise

Turvallisuuskomitea 2014. Kyberturvallisuusstrategian toimeenpano-ohjelma. Viitattu 5.11.2021 Kyberturvallisuusstrategian toimeenpano-ohjelma – Turvallisuuskomitea

Turvallisuuskomitea 2017. Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 - 2020. Viitattu 5.11.2021 Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020 – Turvallisuuskomitea

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Viitattu 20.11.2021 https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Valtioneuvosto 2013. Suomen kyberturvallisuusstrategia. Viitattu 5.11.2021 kyber_taitto2_fi.indd (defmin.fi)

Valtioneuvosto 2014. Älykäs kaupunki – Smart City. Katsaus fiksuihin palveluihin ja mahdollisuuksiin. Viitattu 19.11.2021 http://urn.fi/URN:ISBN:978-952-243-397-8

Valtioneuvosto 2017. Yhteiskunnan turvallisuusstrategia. Viitattu 31.12.2021 YTS_2017_suomi.pdf (turvallisuuskomitea.fi)

Valtioneuvosto 2018a. Kyberturvallisuuden strateginen johtaminen Suomessa. Viitattu 5.11.2021 28-2018-Kyberturvallisuuden strateginen johtaminen.pdf (valtioneuvosto.fi)

Valtioneuvosto 2018b. Media- ja telealan toimintaedellytyksiin parannuksia. Viitattu 8.2.2022. https://valtioneuvosto.fi/-/media-ja-telealan-toimintaedellytyksiin-parannuksia

Valtioneuvosto 2019. Suomen kyberturvallisuusstrategia 2019. Viitattu 5.11.2021 Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf (turvallisuuskomitea.fi)

Valtioneuvosto 2021. Kyberturvallisuuden kehittämisohjelma. Viitattu 19.11.2021 http://urn.fi/URN:ISBN:978-952-243-599-6

Valtioneuvoston kanslia 2017. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Viitattu 31.12.2021 https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila,+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/

Valtiontalouden tarkastusvirasto 2017. Tuloksellisuustarkastuskertomus Kybersuojauksen järjestäminen. Viitattu 5.11.2021 https://www.vtv.fi/app/uploads/2018/05/22102159/kybersuojauksen-jarjestaminen-16-2017.pdf

Valtiovarainministeriö 2020a. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka). Viitattu 31.1.2022. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka) (valtioneuvosto.fi)

Valtiovarainministeriö 2020b. Valtioneuvoston periaatepäätös 8.4.2020. Viitattu 5.11.2021 http://julkaisut.valtioneuvosto.fi/handle/10024/162169

Valtiovarainministeriö 2020c. Digitaalisen turvallisuuden kustannus-vaikuttavuusarviointi julkisessa hallinnossa selvitystyön raportti 1.6.2020. Viitattu 31.1.2022 https://vm.fi/documents/10623/306832/Digitaalisen+turvallisuuden+kustannu

s-vaikuttavuusarviointi+julkisessa+hallinnossa+(selvitysty%C3%B6n+raportti+1.6.2020)/c79cab0d-ba57-1d20-1e17-772cd24a9d62/Digitaalisen+turvallisuuden+kustannus-vaikuttavuusarviointi+julkisessa+hallinnossa+(selvitysty%C3%B6n+raportti+1.6.2020).pdf

Valtiovarainministeriö 2021a. Kuntien digitaalisen turvallisuuden riskikyselyn tulokset. Viitattu 31.1.2021 https://vm.fi/documents/10623/31227348/Kuntien+digiturvariskien+kyselyn+syksy+2020+tulokset.pdf/

Valtiovarainministeriö 2021b. Digiturvallisuuden riskikyselyn tuloksia. Viitattu 2.2.2022 https://dvv.fi/documents/16079645/0/Digiturvallisuuden_riskikyselyn_tulokset_syksy2021.pdf/

Verdict Media Limited 2020. History of smart cities: Timeline 2020. Viitattu 25.11.2021 https://www.verdict.co.uk/smart-cities-timeline/

VTT blogi 2018. Mitä Smart City tarkoittaa? Sinä päätät. Viitattu 19.11.2021. https://www.vttresearch.com/fi/uutiset-ja-tarinat/mita-smart-city-tarkoittaa-sina-paatat

Yksityisyyden suoja 759/2004. Viitattu 8.2.2022 Laki yksityisyyden suojasta työelämässä 759/2004 - Ajantasainen lainsäädäntö - FINLEX ®

Yle 2019a. Kaupunginjohtaja Lahden kyberhyökkäyksestä: "Tietoturvan taso ei ole ollut riittävä". Viitattu 19.11.2021 https://yle.fi/uutiset/3-10869368

Yle 2019b. Kiristäjät vaativat lunnaita Kokemäen kaupungilta – haittaohjelma pisti kaupungin verkon polvilleen. Viitattu 19.11.2021 https://yle.fi/uutiset/3-10899982

Yle 2019c. Taas tietomurto Satakunnassa: Tällä kertaa kohteena Porin kaupunki. 8.8.2019. Viitattu 19.11.2021 https://yle.fi/uutiset/3-10913191

Yle 2020. Analyysi: Vastaamon tietomurto on kuin lento-onnettomuus – hirveä tilanne, josta kaikki voivat oppia jotain. Viitattu 19.11.2021 https://yle.fi/uutiset/3-11611291

Liite 1: Kyberturvallisuuspalvelutoimittajan haastattelurunko

Haastateltavan taustatiedot

Kerro taustastasi: koulutuksestasi, työtehtävistäsi ja vastuistasi (Ei käytetä raportissa)

1. Mitkä ovat mielestäsi merkittävimpiä kyberuhkia suomalaisille kunnille yleisesti ja miten suurena riskinä pidät näitä kyberuhkia suomalaisten kuntien näkökulmasta tällä hetkellä asteikolla 1–5 (1 pieni - 3 keskikokoinen - 5 suuri)?
2. Miten arvioisit kyberuhkien kehitysnäkymiä suomalaisten kuntien osalta asteikolla 1–5 (1 vähenee - 3 pysyy samana - 5 kasvaa merkittävästi)?
    a. Perustele?
3. Millaisena pidät mahdollista äärimmäistä vahinkoa, joka voisi kunnalle kyberuhan kohteeksi joutumisesta syntyä ja kuinka mahdollisena pidät kyseistä katastrofivahinkoa kuntien näkökulmasta tällä hetkellä asteikolla 1–5 (1 pieni - 3 keskikokoinen - 5 suuri)?
4. Millaisia kyberturvakontrolleja (teknisiä tai toiminnallisia) kunnilla olisi mielestäsi vähintään välttämätöntä olla käytössä?
5. Millaisia kyberturvalisäsuojauksia/-toimia suosittelit kuntien ottamaan käyttöön?
6. Millaisia hallinnollisia tietoturvakäytäntöjä kunnilla tulisi olla käytössä?
7. Mitkä ovat mielestänne paljon esillä olevien älykaupunkien (Smart City) kyberturvahaasteet?
8. Millaisia kyberturvasuojauksia suosittelisit kuntien ottamaan IoT järjestelmien suojaukseen?
9. Millaista eri tietoturvatarjontaa teidän yrityksenne voisi tarjota kunnille?
10. Jos saisit esittää kunnille heidän kyberturvaansa liittyvän yhden kysymyksen, mitä kysyisit?

Liite 2: Kunnan edustajan haastattelurunko

Haastateltavan taustatiedot

Kerro taustastasi: koulutuksestasi, työtehtävistäsi ja vastuistasi (Ei käytetä raportissa)

1. Mitkä ovat mielestäsi merkittävimpiä kyberuhkia suomalaisille kunnille yleisesti ja miten suurena riskinä pidät näitä kyberuhkia suomalaisten kuntien näkökulmasta tällä hetkellä asteikolla 1–5 (1 pieni - 3 keskikokoinen - 5 suuri)?
2. Miten arvioisit kyberuhkien kehitysnäkymiä suomalaisten kuntien osalta asteikolla 1–5 (1 vähenee - 3 pysyy samana - 5 kasvaa merkittävästi)?
    a. Perustele?
3. Millaisena pidät mahdollista äärimmäistä vahinkoa, joka voisi kunnalle kyberuhan kohteeksi joutumisesta syntyä ja kuinka mahdollisena pidät kyseistä katastrofivahinkoa kuntien näkökulmasta tällä hetkellä asteikolla 1–5 (1 pieni - 3 keskikokoinen - 5 suuri)?
4. Millaisena pidät teidän kunnan kyberturvallisuuden tasoa asteikolla 1–5 (1 huono - 3 hyvää keskitasoa - 5 erittäin hyvä)?
    a. Miten tähän arvioon päädyit? Onko esimerkiksi ulkopuolinen taho arvioinut sen?
5. Millaiset kyberturvakontrollit / -suojaukset teidän kunnassanne on käytössä?
6. Millaisia hallinnollisia tietoturvakäytäntöjä teidän kunnassanne on käytössä?
    a. Millaisen päätösprosessin kautta olette näihin käytäntöihin päätyneet?
7. Mitkä ovat mielestänne paljon esillä olevien älykaupunkien (Smart City) kyberturvahaasteet?
8. Millaisia kyberturvasuojauksia teillä on käytössä IoT järjestelmien suojaukseen?
9. Mikä on se suurin este kuntien tietoturva toteuttamiselle, kun jätetään pois kaksi vastausta: raha ja osaajapula?
10. Onko teillä kyberjohtamisen strategia olemassa?

Liite 3: Muiden kyberturvatoimijoiden haastattelurunko

Haastateltavan taustatiedot

Kerro taustastasi: koulutuksestasi, työtehtävistäsi ja vastuistasi (Ei käytetä raportissa)

1. Mitkä ovat mielestäsi merkittävimpiä kyberuhkia suomalaisille kunnille yleisesti ja miten suurena riskinä pidät näitä kyberuhkia suomalaisten kuntien näkökulmasta tällä hetkellä asteikolla 1–5 (1 pieni – 3- keskikokoinen - 5 suuri)?
2. Miten arvioisit kyberuhkien kehitysnäkymiä suomalaisten kuntien osalta asteikolla 1–5? (1 vähenee - 3 pysyy samana - 5 kasvaa merkittävästi)?
    a. Perustele?
3. Millaisena pidät mahdollista äärimmäistä vahinkoa, joka voisi kunnalle kyberuhan kohteeksi joutumisesta syntyä ja kuinka mahdollisena pidät kyseistä katastrofivahinkoa kuntien näkökulmasta tällä hetkellä asteikolla 1–5 (1 pieni - 3 keskikokoinen - 5 suuri)?
4. Millaisena pidät kuntien kyberturvallisuuden tasoa keskimäärin asteikolla 1–5 (1 huono - 3 hyvää keskitasoa - 5 erittäin hyvä)?
    a. Miten tähän arvioon päädyit?
5. Millaisia kyberturvakontrolleja (teknisiä tai toiminnallisia) kunnilla olisi mielestäsi vähintään välttämätöntä olla käytössä?
6. Millaisia kyberturvalisäsuojauksia/-toimia suosittelit kuntien ottamaan käyttöön?
7. Millaisia hallinnollisia tietoturvakäytäntöjä kunnilla tulisi olla käytössä?
8. Mitkä ovat mielestänne paljon esillä olevien älykaupunkien (Smart City) kyberturvahaasteet?
9. Millaisia kyberturvasuojauksia suosittelisit kuntia ottamaan IoT järjestelmien suojaukseen?
10. Jos saisit esittää kunnille heidän kyberturvatilanteeseensa liittyvän yhden kysymyksen, mitä kysyisit?