Tampereen yliopisto

Ella Salovaara

KYBERVALMIUS OSANA KUNTIEN TOTEUTTAMAA RISKIENHALLINTAA

Kyberturvallisuuden järjestäminen suomalaisissa kunnissa – Case Kokemäen kaupunki

Johtamisen ja talouden tiedekunta
Kandidaatintutkielma
Huhtikuu 2020

TIIVISTELMÄ

Ella Salovaara: Kybervalmius osana kuntien toteuttamaa riskienhallintaa. Kyberturvallisuuden järjestäminen suomalaisissa kunnissa – Case Kokemäen kaupunki
Kandidaatintutkielma
Tampereen yliopisto
Hallintotieteiden tutkinto-ohjelma
Huhtikuu 2020

Tässä empiirisessä tutkimuksessa tarkasteltiin Kokemäen kaupunkiorganisaatioon heinäkuussa 2019 kohdistunutta kyberhyökkäystä ja sen vaikutuksia. Tämän kandidaatintutkielman tarkoituksena on muodostaa käsitys eritoten siitä, millaisia konkreettisia kyberturvatoimia tapaustutkimuksen kohteena olevassa Kokemäen kaupungissa on toteutettu ennen kyberhyökkäystä sekä toteutuneen hyökkäyksen jälkeen. Tutkimus pyrkii löytämään vastauksia myös siihen, kohdistettiinko kaupungin budjetoinnissa enemmän resursseja kyberturvatoimiin toteutuneen hyökkäyksen seurauksena. Tutkimuksen päätutkimuskysymyksenä on, miten Kokemäen kaupunki on parantanut kybervalmiuttaan kesän 2019 kyberhyökkäyksen jälkeen.

Tutkimus on empiriaan pohjautuva tapaustutkimus, jonka aineisto analysoitiin sisällönanalyysin keinoin. Tutkimuskohteena on Kokemäen kaupungin johtohenkilöstöön kuuluvia henkilöitä, jotka olivat mukana vastaamassa kesän 2019 kyberhyökkäyksen aiheuttamien vaurioiden korjaamisesta. Päättelymenetelmänä käytettiin induktiivista päättelymenetelmää. Tutkimusaineisto kerättiin teemahaastattelujen muodossa maaliskuussa 2020. Haastatteluin pyrittiin muodostamaan käsitys siitä, millä tavoin Kokemäen kaupungin kyberturvatoimet ovat mahdollisesti muuttuneet realisoituneen kyberhyökkäyksen seurauksena. Tutkimuksessa kartoitettiin myös sitä, millaisia kyberturvatoimia julkisyhteisöjen sekä erityisesti kuntien on mahdollista ja kannattavaa soveltaa osana omia riskienhallintaprosessejaan.

Aineiston analyysin tuloksena voitiin havaita, että tietyt kyberturvatoimet painottuvat merkittävämmin kuin toiset. Organisaation riskienhallinnan kannalta mahdollisesti tärkeimpänä kyberturvatoimena voitiin havaita henkilöstön tietoisuus ja kouluttaminen tietoturva-asioiden osalta. Muita merkitykselliseksi koettuja kyberturvaan tai sen ylläpitoon liittyviä toimia olivat koko organisaation kattavat tietoturvaohjeistukset, talouden resurssit, laitteiden ja järjestelmien virustorjunta sekä säännölliset palvelinpäivitykset. Tutkimuksessa havaittiin myös, että kaupunki kohdisti vuoden 2020 budjetoinnissaan investointimäärärahaa tietoturvan ylläpitoon. Jatkotutkimuksissa harkinnanvaraisen näytteen sijasta voisi olla mielekkäämpää laajentaa otantaa Suomen kuntasektorilla, jolloin suomalaisten kuntien kyberturvan tasosta voitaisiin muodostaa yleistettävä katsaus.

Avainsanat: kyberturvallisuus, kyberhyökkäys, kyberturvatoimet, riskienhallinta, kunta

SISÄLLYS

TAULUKKO- JA KUVIOLUETTELO

1. JOHDANTO

Yhteiskuntiin kohdistuneet kriittiset uhat ovat aikojen alusta lähtien olleet pääosin fyysisiä, eritoten erilaisia luonnonilmiöitä. Yhteiskuntia koetelleet luonnonilmiöt, kuten tulvat, myrskyt ja maanjäristykset, ovat kyenneet tuhoamaan kokonaisia kansoja. Perinteisiä yhteiskuntiin kohdistuneita uhkia ovat olleet myös muun muassa terrorismi, hallitsemattomat väestöliikkeet sekä vaaralliset tartuntataudit. Tällaisia uhkia varten yhteiskuntien on täytynyt kehittää erilaisia toimintatapoja ja strategioita, joiden avulla uhilta on kyetty välttymään, ja joiden kautta kriiseistä on ollut mahdollista toipua. Kuitenkin tieto- ja viestintäteknologia sekä niihin liittyvät palvelut muuttavat yhteiskuntamme toimintaa ja valtarakenteita ennenäkemättömällä tavalla. Digitalisoitumisen mukanaan tuoma tietoverkkoihin kohdistuva häirintä ja loukkaukset ovat nousseet yhteiskunnassamme lyhyessä ajassa yhtä lailla kriittisiksi turvallisuusuhiksi. (Huoltovarmuuskeskus, tietosuoja.) Tietoa menee verkkoon jatkuvasti yhä suurempia määriä. Näin ollen myös tiedon hallitsemisesta ja sen turvaamisesta tulee entistä tärkeämpää, mutta myös haastavampaa. Sisäministeriön teettämän kansallisen riskiarvion (2019, 31) mukaan kyberhyökkäysten kansalliselle turvallisuudelle aiheuttamat uhat voivat olla vakavuudeltaan ja vaikuttavuudeltaan verrattavissa jopa aseelliseen hyökkäykseen.

Kyberturvallisuus oli pitkään melko tuntematon aihe Suomen kuntakentällä. Digitalisaation ja erilaisten tietoverkkojen yhä yleistyessä kunnat ovat muiden organisaatioiden tavoin kuitenkin joutuneet viime vuosina kohtaamaan kyberturvallisuusasiat päivittäisessä toiminnassaan. Kuntaliiton (2019) mukaan julkishallinnon organisaatioihin kohdistuu yhä enemmän tietoturvaloukkauksia ja kyberturvallisuushyökkäyksiä. Kunnat ovat tietoverkkoineen yhä voimakkaammin haavoittuvaisia, ja näin ollen myös kyberturvallisuuteen on olennaista kohdistaa resursseja aiempaa enemmän. Kuitenkin julkissektoria ja erityisesti kuntakenttää nykypäivänä koettelevat taloudellisten resurssien niukkuus ja tehokkuusvaatimukset asettavat huomattavia rajoituksia myös kybervalmiuden ylläpitoon ja kyberturvallisuudesta huolehtimiseen. Suuremmissa kaupungeissa tietoturva-asioihin saattaa olla mahdollista ohjata tarpeeksi resursseja, kuten kohdistaa riittävissä määrin rahoitusta sekä kouluttaa osaavaa työvoimaa. Mutta millä tavoin pienemmät kunnat onnistuvat ylläpitämään tietoturvaansa riittävällä tasolla?

Kesällä 2019 Suomen kuntakentällä järisi, kun kolme suomalaista kaupunkia ilmoitti joutuneensa kyberhyökkäysten kohteeksi. Tietomurrot tapahtuivat Lahdessa, Kokemäellä ja Porissa. Lahden kaupungin tietojärjestelmiin tehty kyberhyökkäys näkyi niin ikään myös Päijät-Hämeen hyvinvointikuntayhtymän toiminnassa. Hyökkäys kohdistettiin kaupungin tietoverkkoon sekä työasemiin ja se havaittiin virustorjuntaohjelmistolla. (Kuntalehti 2019.) Erityisen haitallisia kyberhyökkäykset ovat silloin, kun ne kohdistuvat laajoihin tietojärjestelmiin, joissa sijaitsee esimerkiksi henkilö- ja potilastietoja. Lahden kyberhyökkäyksessä henkilötietoja ei mitä ilmeisimmin ollut joutunut ulkopuolisten haltuun, mutta esimerkiksi Kokemäen kaupunkiin kohdistuneessa hyökkäyksessä luonteeltaan arkaluontoisiin henkilötietoihin päästiin käsiksi. Joka tapauksessa henkilötietojen vakoiluun ja anastamiseen liittyvien uhkakuvien mahdollisuutta ei voida poissulkea tietomurtotapauksissa. Kunnat eivät voi enää tuudittautua ajatukseen, jossa kyberhyökkäykset ja tietomurrot koskisivat vain suuria ja kansainvälisiä liikeyrityksiä, vaan kyberturvallisuus ja kybervalmiuden ylläpitäminen ovat todellisuutta nykyhetkessä.

Kuten Lahden, Porin ja Kokemäen kaupunkien kesän 2019 kyberhyökkäyksissä kävi ilmi, henkilötiedot ovat usein eritoten julkisyhteisöjen tietoverkkoihin kohdistuvien hyökkäysten kohteena. Tällöin tietojärjestelmistä pyritään saamaan tietoja, joihin tietoa tavoittelevilla tahoilla ei ole oikeutusta. ”Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.” (Tietosuojavaltuutetun toimisto, tietoturvaloukkaukset-asiantuntijasivu). Lahden kaupungin kesäkuussa 2019 verkkoon ja työasemiin kohdistettu kyberhyökkäys päästi hyökkääjän kaupungin sisäverkkoon sekä koneiden keskitettyyn hallintajärjestelmään. Lahden kaupungin tietohallintajohtaja Marko Monni kertoi kyberhyökkäystä seuraavana päivänä, että hyökkäys on mahdollistanut myös henkilötietoihin käsiksi pääsyn. Hyökkäyksen seurauksena yhteys Lahden kaupungin ja Päijät-Hämeen hyvinvointikuntayhtymän välillä katkaistiin välittömästi, jotta sosiaali- ja terveyspalveluiden tiedot pysyisivät turvattuina. Yhteyden katkaisu aiheutti merkittäviä häiriöitä potilastietojärjestelmiin useiksi päiviksi. (Kuntalehti 2019.)

Alati kasvava työnteon ja palveluiden digitalisoituminen sekä kuntasektorilla jo tapahtuneet tietomurrot ovat vetäneet kunnat mukaan pohtimaan vakavasti tietoturvansa tilannetta. Suomalaisten kuntien kyberturvaa on tutkittu tieteessä suhteellisen vähän. Tämä lienee osaltaan seurausta siitä, että kunnat ovat laajemmalti saaneet pysyä poissa kyberhyökkääjien tähtäimistä. Toisaalta kuntien päätyminen tietomurtojen kohteeksi ei ole nykyisenä digitalisaation kulta-aikana lainkaan

epätodennäköistä, sillä onhan eriasteisia tietomurtotapauksia noussut esiin yksityisen puolen organisaatioissa jo usean vuoden ajan niin meillä kuin maailmalla. Esimerkiksi vuonna 2014 Yhdysvalloissa useat merkittävät yhtiöt joutuivat kyberhyökkäysten kohteeksi, muun muassa Home Depot, Target, Yahoo! sekä Google. Samaisena vuonna myös amerikkalaiset julkissektorin organisaatiot saivat osansa kyberhyökkäyksistä, kun hyökkäysten kohteeksi päätyivät Yhdysvaltain asevoimien päämaja USCENTCOM, Yhdysvaltain kansallinen postilaitos sekä Valkoinen talo. Näissä tietomurtotapauksissa aiheutui haittaa miljoonille henkilöille, kun muun muassa nimiä, osoitteita, sosiaaliturvatunnuksia ja luottokorttien tunnuslukuja joutui vääriin käsiin. (Norris, Joshi & Finin 2015, 196.) Oli niin sanotusti vain ajan kysymys, milloin kyberhyökkäykset rantautuisivat voimakkaasti myös Suomen julkissektorille ja erityisesti kuntakentälle. Kesää 2019 voidaankin pitää tilanteessa eräänlaisena käännekohtana.

Suomalaista kybervalmiutta on tieteessä tutkittu jonkin verran erityisesti valtion tasolla. (Esim. Lehto ym. 2017.) Tutkimusta aiheesta on tehty myös maailmalla, muun muassa Yhdysvalloissa. (Esim. Norris, Joshi & Finin 2015, Caruson ym. 2012). Yleiset kyberuhilta suojautumisen keinot ovat osittain sovellettavissa myös julkisyhteisöjen ja näistä erityisesti kuntasektorin käyttöön, mutta julkisyhteisöjen toiminnan erityinen luonne asettaa kuitenkin merkittäviä reunaehtoja soveltamiselle. Näihin ehtoihin lukeutuvat muun muassa talouden niukkuus sekä lainsäädäntö.

Tämä kandidaatintutkielma pyrkii löytämään vastauksia siihen, miten kuntaorganisaation tietohallintoa pystytään turvaamaan kyberuhilta ja millaisia konkreettisia toimia kohdekunnassa on tehty parantamaan kybervalmiuden tasoa. Tutkimus on luonteeltaan empiirinen tapaustutkimus ja tutkimuskohdetta kuvataan kvalitatiivisesti. Tutkimuskohteeksi on valikoitunut jo kyberhyökkäyksen kohteeksi joutunut kuntaorganisaatio, Kokemäen kaupunki, jossa on jouduttu viime aikoina toimimaan kybervalmiuden tason kehittämisen parissa. Tutkimuksen tavoitteena on siis selvittää, millaisia keinoja etenkin kuntaorganisaatioissa on mahdollista ja kannattavaa soveltaa kyberturvallisuuden ylläpitoon ja kehittämiseen kuntakentälle tyypillisten niukkojen resurssien puitteissa. Tutkimustiedosta voisi olla hyötyä eritoten kunnille, jotka saattavat yhä enenevissä määrin kamppailla riittävän tietoturvan tason ylläpitämisen kanssa.

Tutkimuksen aineistona käytetään Kokemäen kaupungin kesän 2019 kyberhyökkäyksen aikaan toimineen johtohenkilöstön haastatteluja sekä kaupungin vuosien 2019 ja 2020 talousarviodokumentteja. Tutkimus on luonteeltaan kvalitatiivinen. Analyysimenetelmänä käytetään teorialähtöistä sisällönanalyysiä ja päättelymenetelmänä induktiivista päättelymenetelmää. Näitä

menetelmävalintoja käsitellään tarkemmin luvussa kaksi. Kolmannessa luvussa on kuvattu tutkimuksen teoreettinen viitekehys ja keskeiset käsitteet. Neljännessä luvussa kuvataan tapaustutkimuksen kohteena olevan Kokemäen kaupungin joutumista kyberhyökkäyksen kohteeksi. Viidennessä luvussa esitellään aineistonkeruun tuloksena syntyneet analyysitulokset ja näiden tulkinta. Kuudennessa luvussa avataan tutkimuksesta esiin nousseita päätelmiä. Tutkimusraportin lopusta löytyvät lähde- ja liiteluettelot. Liitteissä on kuvattuna tutkimuksen teemahaastattelurunko, jota käytettiin pohjana tutkimuksen aineistonkeruussa.

2. TUTKIMUSMENETELMÄ

2.1 Tutkimuskohde ja rajaukset

Tämän kandidaatintutkielman empiirinen tutkimuskohde on heinäkuussa 2019 kyberhyökkäyksen kohteeksi joutunut Kokemäen kaupunki Satakunnan maakunnassa Lounais-Suomessa. Tutkimuskohteena on erityisesti Kokemäen kaupungin hallinnon johtohenkilöstöä. Tutkimuksen taustalla vaikuttavat niin ikään julkisyhteisöjen keskuudessa yhä yleistyvät tietoturvaloukkaukset, jotka ovat johdattaneet myös kunnat tarkastelemaan tietoturvansa tilaa aiempaa tarkemmin. Kyberturvallisuuden merkittävyys ja vakavuus ovat nousseet viime vuosina aiempaa vahvemmin näytille. Kun kyberuhat koskettavat yhä enenevissä määrin julkis- ja kuntasektoria, koskettavat ne samalla myös suoraan kansalaisten turvallisuutta ja hyvinvointia. Tietomurrot loukkaavat usein julkisyhteisöjen tietoverkoissa tyypillisesti sijaitsevia henkilö- ja potilastietoja, joiden joutuessa vääriin käsiin ne saattavat aiheuttaa vakavia vahinkoja laajoille henkilöjoukoille. IT-järjestelmät pitävät lisäksi sisällään pääsyn yhteisön varoihin. Erityisesti nämä seikat tekevät tutkimusaiheesta myös yhteiskunnallisesti merkittävän. Kokemäen kaupunki valikoitui tutkimuskohteeksi sen jo kokeman kyberhyökkäyksen vuoksi. Näin ollen on mahdollista tutkia sitä, millaisia toimia kaupunkiorganisaatiossa on tehty kyberuhilta suojautumisessa ja kybervalmiuden parantamisessa. Kokemäen kaupunki on myös organisaationa kandidaatintutkielmaa varten hallittavissa oleva tutkimuskohde, sillä se ei ole merkittävän suuri kaupunki. Tämän ansiosta myös aineiston keruu saattaa muodostua vaivattomammaksi. Kyberhyökkäys ilmaantui kyseiselle kaupunkiorganisaatiolle täytenä yllätyksenä, mikä on luontaista verkossa tapahtuvalle rikollisuudelle ja hyökkäyksille. Kaupungissa ei myöskään välttämättä löytynyt suoraan hallinto-organisaation sisältä tarpeeksi tietotaitoa ja osaamista vastaamaan kyberhyökkäyksen aiheuttamiin vaurioihin, ja asiassa jouduttiinkin turvautumaan niin poliisin kuin liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen apuun.

Tutkimuksen tarkoituksena on selvittää sitä, millä tavoin Kokemäen kaupunki on pystynyt palautumaan heinäkuussa 2019 tapahtuneesta kyberhyökkäyksestä, sekä miten toteutunut hyökkäys on muuttanut kaupungin toimintatapoja kyberturvallisuuden osalta. Tällöin on olennaista selvittää muun muassa sitä, millaisia konkreettisia toimia kaupungin sisäisessä organisaatiossa on tehty vahvistamaan tietoturvan haavoittumattomuutta. Tutkimus pyrkii löytämään vastauksia myös siihen, onko kyberturvallisuutta varten osoitettu aiempaa enemmän resursseja kaupungin talousarvioissa tai

onko kaupungin strategiassa huomioitu kybervalmiuteen liittyviä seikkoja osana kaupunkiorganisaation riskienhallintaprosesseja. Seuraavassa esitellään tutkimuksen tutkimuskysymykset.

Pääkysymys

Miten Kokemäen kaupunki on parantanut kybervalmiuttaan kesän 2019 kyberhyökkäyksen jälkeen?

Alakysymykset

Mitä käytännön toimia kaupungissa on alettu tekemään kyberturvallisuuden tason parantamiseksi?

Miten kyberturvallisuutta varten on osoitettu resursseja kaupungin talousarviossa ja miten se on huomioitu kaupungin strategiatasolla?

Tutkimus on luonteeltaan empiirinen. Se tarkastelee kuntia yhä merkitykseltään kasvavassa digitaalisessa kyberturvallisuusympäristössä, jossa kunnilla ei ole aiemmin ollut samankaltaista, yhtä merkittävää roolia. Tutkimus toteutetaan harkinnanvaraisena näytteenä.

2.2 Tutkimusaineiston keruu ja menetelmät

Tutkimuksen aineistona käytetään Kokemäen kaupungin strategia- ja talousarviodokumentteja sekä kaupungin johtohenkilöstön haastatteluja. Kokemäen kaupungin toimintatapoja suojautua kyberuhilta arvioidaan kvalitatiivisesti tarkastellen suojautumisen ja konkreettisten toimien muutosta suhteessa aikaan ennen kyberhyökkäystä sekä aikaan hyökkäyksen jälkeen. Tutkimus on näin ollen pitkittäistutkimus, joka tarkastelee sitä, millä tavoin kaupunki on tähän hetkeen mennessä muuttanut toimintaansa suojautua kyberuhilta kesän 2019 hyökkäyksen jälkeen.

Tutkimuksen aineisto tuotetaan itse haastattelemalla kaupungin johtoa ja asiantuntijoita, jotka olivat vastaamassa kyberhyökkäyksen aiheuttamien tuhojen selvittämisestä sekä vaurioiden korjaamisesta. Tarkoituksena on selvittää erityisesti kyberuhkien torjunnassa ja suojatutumisen tasossa tapahtuneita muutoksia. Tutkimuksessa käytetään hyödyksi myös kaupungin strategia- ja talousarviodokumentteja, joista käyvät ilmi mahdolliset kyberturvan ylläpitoon ja kyberuhkien

torjuntaan osoitetut resurssit ennen ja jälkeen hyökkäyksen. Tutkimuksessa keskitytään erityisesti vuosien 2019 ja 2020 dokumentteihin, jotta näyte säilyy relevanttina.

Tutkimuksessa käytettävä menetelmä on induktiivinen päättelymenetelmä, jossa yksittäisten havaintojen pohjalta päätellään teoriaa. Induktiivinen päättely on siis päättelyä, jossa yksittäisistä havainnoista esitetään teoreettista pohdintaa. Sen avulla pyritään saavuttamaan paras saatavilla oleva selitys, eikä se täten ole absoluuttisesti johdettu totuus eikä yleistys tutkittavasta kohteesta. (Tuomi & Sarajärvi 2018, 98-99.) Tässä tutkimuksessa tarkastellaan yhden suomalaisen kunnan, Kokemäen kaupungin, kyberuhilta suojautumisen tasoa ja toteutettuja kyberturvatoimia, eikä se näin ollen muodosta yleistystä tai kokonaiskuvaa kaikkien Suomen kuntien kybervalmiuden tilasta. Tutkimus on tapaustutkimus, jossa päätellään sitä, millaisia kybertoimia Kokemäen kaupunki on toteuttanut tai toisaalta jättänyt toteuttamatta osana omia riksienhallintaprosessejaan. Tutkimuksen aineistonkeruuta ja analyysimenetelmää tarkastellaan lähemmin seuraavissa kappaleissa.

2.3 Teemahaastattelu aineistonkeruumenetelmänä

Tutkimusaineisto kerättiin haastatteluiden muodossa. Haastattelukeinona käytettiin puolistrukturoitua teemahaastattelua. Hirsjärven & Hurmeen (2011, 47) mukaan teemahaastattelun ydin on kysymysten asettelemisessa teemoittain, jotka noudattavat tavanomaista etenemisjärjestystä. Tätä järjestystä voidaan havainnoida neljän eri vaiheen kautta. Tutkimusaineiston keruun ensimmäisessä vaiheessa tiedostettiin, että tutkimuksen kohteena oleva joukko on kokenut ilmiön, Kokemäen kaupungin tapauksessa kaupunkiorganisaatioon kohdistuneen kyberhyökkäyksen. Tätä kyberhyökkäystä ilmiönä pyrittiin tarkentamaan ja selventämään teemahaastattelun keinoin. Toisessa vaiheessa selvitettiin Kokemäen kyberhyökkäykseen liittyviä osia, rakenteita, prosesseja sekä kokonaisuutta. Kolmannessa vaiheessa kehitettiin näiden rakenteiden pohjalta teemahaastattelurunko, jonka kautta lähestyttiin tutkittavaa ilmiötä ja kokonaisuutta, eli esimerkiksi sitä, millaisia toimia kaupunkiorganisaatiossa on tehty kyberturvan suhteen ennen kyberhyökkäystä ja toisaalta toteutuneen hyökkäyksen jälkeen. Neljännessä vaiheessa kiinnitettiin huomiota haastateltaviin ja heidän omiin kokemuksiinsa kybertoimiin liittyen.

Teemahaastattelu antaa haastateltavalle tilaa tulkita kysymyksiä itse. Haastattelumuotona teemahaastattelu on lomakehaastattelun ja avoimen haastattelun välimuoto (Hirsijärvi, Remes & Sajavaara 2015, 208-209). Teemahaastattelussa kysymyksiä ei rajattu kovin tarkasti, jolloin

haastattelu muotoutui haastateltavien vastausten mukaisesti. Teemahaastattelun tarkoituksena oli tuoda esiin haastateltavien omia näkemyksiä kyberturvaan ja sen vaatimiin toimiin liittyen. Teemahaastattelu aineistonkeruumenetelmänä huomioi myös sen, että ihmisten tulkinnat eri asioista ovat keskeisiä ja muodostuvat vuorovaikutuksen kautta. Esimerkiksi kyberturvallisuus saattoi tarkoittaa eri vastaajille eri asioita, ja näin ollen haastateltavien vastaukset poikkesivat toisistaan. Myönteistä teemahaastattelussa on myös se, että itse haastateltava toimii tarkentajana kyberturvatoimiin liittyen ja näin ollen aineistoksi oli mahdollista kertyä tietoa, jota ilman teemahaastattelua ei välttämättä olisi saatu selville. (Hirsjärvi & Hurme 2011, 48, 66.) Haastateltavia valittiin teemahaastatteluun neljä. Jokainen haastattelu kesti 30-50 minuuttia ja litteroitua haastatteluaineistoa muodostui yhteensä 34 sivua. Haastattelut suoritti tämän tutkimusraportin kirjoittaja. Haastattelut myös nauhoitettiin.

2.4 Teorialähtöinen sisällönanalyysi

Aineiston analysoimiseksi tutkimuksessa käytettiin sisällönanalyysiä ja tarkemmin teorialähtöistä sisällönanalyysiä. Sisällönanalyysin ytimenä on tarkastella kerätyn tutkimusaineiston sisältöä sitä eritellen, eroja ja yhtäläisyyksiä tutkien. Sisällönanalyysi on siis tekstianalyysia. Tutkimusaineisto saatettiin tekstimuotoon, jolloin sitä oli mahdollista analysoida sisällönanalyysin keinoin. Haastatteluaineisto tuotiin tekstimuotoon litteroinnin avulla. Sisällönanalyysin kautta Kokemäen kaupungin kyberhyökkäyksestä pyrittiin muodostamaan tiivistetty kuvaus, joka toisi analysoidut tulokset kyberhyökkäysilmiön laajempaan kontekstiin ja sitä koskevaan aiempaan tieteeseen. Sisällönanalyysi on sanallista tekstin kuvailua ja analysointia. Laadullisessa tutkimusaineiston sisällönanalyysissa tutkimusaineisto pilkottiin erilaisiin kyberturvatoimiin analysointia varten ja analyysin jälkeen näistä osista muodostettiin uudenlainen laajempi kokonaisuus, jossa pohdittiin eri kyberturvatoimien suhdetta toisiinsa. (Tuomi & Sarajärvi 2018, 105, 109-116.) Teorialähtöisen sisällönanalyysista tekee se, että tutkimusaineistoa analysoitiin tutkimukseen valitun, jo olemassa olevan teorian valossa. Tarkoituksena on tämän teorian tai mallin peilaaminen uudessa yhteydessä, uuden tutkimustuloksen kontekstissa. (Kvalimotv, aineisto- ja teorialähtöisyys.) Aineiston analysoinnissa ja käsittelyssä käytettiin siis Tuomen & Sarajärven (2018, 105) kuvailemia sisällönanalyysin vaiheita, joita ovat pelkistäminen ja ryhmittely. Niiden avulla aineistosta saatiin havaittua oleellisimmat seikat kyberturvatoimiin liittyen. Näiden vaiheiden kautta muodostettiin käsitteellisyys ja ymmärrys Kokemäen kaupunkiorganisaatiota kohdanneesta kyberhyökkäyksestä

sekä kyberturvatoimista. Kuudennessa luvussa haastatteluaineistoa analysoidaan ja peilataan kolmannen luvun teoriaosuudessa käsiteltyihin seikkoihin.

3. TEOREETTINEN VIITEKEHYS

3.1 Kyberturvallisuuden käsitteistä

Kyberturvallisuus on käännös englannin kielen termistä *cyber security*. Se tarkoittaa organisaatioiden erilaisten tietoverkkojen ja tietopankkien turvallisuutta ja turvaamista esimerkiksi tietomurroilta. (Kyberturvallisuuskeskus, kyberturvallisuuden sanasto 2018, 10, 30.) Suomen turvallisuuskomitea ja Huoltovarmuuskeskus ovat yhdessä Suomen Sanastokeskuksen kanssa keränneet kyberturvallisuuteen liittyvän sanaston, jossa määritellään kyberturvallisuuteen liittyvä termejä. Sanastossa termin kyberturvallisuus kerrotaan olevan tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuus sisältää kaikki sellaiset toimenpiteet, joiden avulla kyberuhkia ja niiden vaikutuksia on mahdollista hallita ja pienentää. Kyberturvallisuutta voidaan vahingoittaa muuan muassa kyberhyökkäysten muodossa. Termi ”kyberhyökkäys” on määritelty tietoverkkohyökkäystä laajempana käsitteenä, sillä kyberhyökkäys ei koske välttämättä pelkästään tietoverkkojen kautta tapahtuvaa haitantekoa. Tietoverkkohyökkäys taas viittaa tietoverkkojen kautta tapahtuvaan toimintaan, jolla pyritään tietojärjestelmien ja laitteiden datan vahingoittamiseen, sekä käyttämään näistä lähteistä saatavia tietoja oikeudettomasti. Palvelunestohyökkäys ja haittaohjelmat ovat tyypillisiä tietoverkkohyökkäyksen ilmenemismuotoja. (Kyberturvallisuuskeskus, kyberturvallisuuden sanasto 2018, 10, 30.)

Arvokasta tietoa, jota yhteisöillä on hallussaan, voidaan kutsua kyberomaisuudeksi. Kyberomaisuus on siis omaisuutta, jota kyberrikolliset yrittävät anastaa yhteisöiltä. Sitä ovat muun muassa organisaation tietojärjestelmissä sijaitsevat henkilö- ja potilastiedot sekä pääsy yhteisön varoihin. Norppa & Peltomäki (2015, 63) ovat kyberrikollisuutta koskevassa teoksessaan listanneet esimerkkejä yritysten mahdollisesta kyberomaisuudesta. Siihen lukeutuvat muun muassa IPR- ja patenttitiedot, asiakastiedot, yrityksen sähköposti, henkilökunnan tiedot, raha, tarjoukset, talousluvut, asiakassuunnitelmat, tuotekehitystiedot sekä yrityskauppoja koskevat tiedot. Kyberomaisuus on samankaltaista myös julkissektorilla, mutta esimerkiksi kunnissa henkilö- ja potilastiedot ovat eritoten kriittisiä, sillä jokainen henkilö on jonkin kunnan asukas. Tämä kyberomaisuuden varastaminen muodostaa merkittävän kyberriskin yhteisölle, sillä luonteeltaan arkaluontoisia tietoja saattaa joutua ulkopuolisten tahojen haltuun.

3.2 Kybervalmius julkisyhteisöissä

Kuntien kybervalmius on osa kuntien toteuttamaa riskienhallintaa ja sisäistä valvontaa. Kuntien riskienhallintatyö on Suomessa suhteellisen tuore asia, sillä suunnitelmallista ja kaiken kattavaa riskienhallintaa on toteutettu kunnissa vasta noin 30 vuoden ajan. Riskille on asetettu erilaisia määritelmiä. Usein termiä riski käytetään kuvaamaan sellaisen tapahtuman mahdollisuutta, josta on mahdollista seurata taloudellisia tai organisatorisia menetyksiä. Kyberturvallisuudessa taloudellista tappiota voi koitua esimerkiksi tietomurtotapauksessa, jossa yhteisön varoihin päästään käsiksi. Henkilötietojen päätyminen ulkopuolisten haltuun ja niiden käyttäminen lainvastaisessa toiminnassa taas on esimerkki organisatorisesta menetyksestä. Toisaalta termiä riski voidaan käyttää myös tapauksissa, joissa toiminnan kannalta myönteisiä asioita menetetään tai tällaisia asioita jää tapahtumatta. Kuten yrityssektorilla, on myös kuntien toiminnassa olennaista riskeiltä suojautuminen. Suojautumisen mahdollistamiseksi kunnissa on otettu käyttöön ennalta ehkäiseviä toimenpiteitä, keskitetty erilaisia resursseja sekä tarkennettu kuntaorganisaation sisäisiä vastuusuhteita. Riskeiltä suojautuminen aloitetaan suuremmista riskeistä, mutta tavoitteena on lopulta myös kehittää suoja pienempiä riskejä vastaan. (Enberg 2002, 8.) Tietoturvasta ja sen oikeaoppisesta ylläpidosta on muodostunut viime vuosikymmenenä yksi organisaatioiden merkittävimmistä riskeistä. Usein juuri tieto on yhteisöjen tärkeintä omaisuutta ja sen ylläpitäminen sekä suojaaminen muodostavatkin organisaatioille uuden ulottuvuuden riksienhallinnassa. Suomalaiset kunnat ovat myös viime vuosina saaneet huomata, että kyberturva-asiat koskettavat suuryritysten ohella myös kuntasektoria. Erilaiset ja eriasteiset kyberhyökkäykset saattavat olla monissa yhteisöissä arkipäivää. Näin ollen kyberturva-asioiden merkitys kuntien riskienhallinnassa tulisi korostua.

Wirtz & Weyerer (2016, 1086) ovat todenneet, että valtionhallinto ja julkissektori yleisesti ottaen kuuluvat aloihin, jotka kohtaavat eniten tuhoisia kyberhyökkäyksiä. He myös havaitsivat, että julkiset IT-infrastruktuurit kohtaavat yleisesti ottaen samankaltaisia turvallisuusriskejä kuin mikä tahansa muukin sektori. Zhao & Zhao (2010, 51) ovat havainneet tutkimuksessaan, että yleisimmät julkissektorin kohtaamat haavoittuvuudet kyberturvallisuudessa liittyvät verkossa tapahtuvaan toimintaan, kuten verkkoselaamiseen, sähköpostin käyttöön sekä langattoman verkon väärinkäyttöön. He myös painottavat, että verkkoturvallisuuden haavoittuvuudet tulisi tunnistaa julkisyhteisöissä, jotta IT-järjestelmiä pystyttäisiin suojaamaan mahdollisimman kattavasti kyberhyökkäyksiltä. Norrisin, Joshin & Fininin (2015, 196) mukaan kyberhyökkäykset ilmenevät julkisyhteisöjen, erityisesti valtion ja suurempien kaupunkiorganisaatioiden keskuudessa useimmiten vahinkoa

aiheuttavina sähköpostiviesteinä. Tällaiset sähköiset kalasteluviestit ovat hyvin yleisiä sekä jatkuvia ja niiden määrä voi nousta jopa kymmeniin tuhansiin viesteihin päivässä. Norris ym. (2015, 196) toteavat yhdysvaltalaisia julkisyhteisöjä uhkaavia kyberhyökkäyksiä koskevassa tutkimuksessaan, että yhteisöjen suurin kyberuhka ovat inhimilliset erehdykset. Tällä tarkoitetaan erityisesti loppukäyttäjiä, jotka vahingossa tai tahallisesti avaavat tiedostoja tai linkkejä kalastusviesteistä ja näin ollen päästävät hyökkääjän hallinnon IT-järjestelmään. Onnistuneen kalastusviestin todennäköisyys arvioidaan myös suhteellisen suureksi. Caruson, MacManus & McPhee (2012, 2) toteavat kyberturvallisuuden paikallistason päätöksentekoa koskevassa tutkimuksessaan, että tietokuilu IT-asiantuntijoiden ja hallinnon virkamiesten välillä on suurempi paikallistason organisaatioissa kuin valtion tasolla. Samasta syystä myös valmius kyberuhilta suojautumiseen on kuntasektorilla usein jälkeen jäänyttä ja hidasta. Lambrinoudakis, Gritzalis, Dridi, & Pernul, (2003, 1873) havaitsivat tutkimuksessaan, että kyberturvatoimien toteuttaminen mahdollisimman tarkoituksenmukaisina ja toimivina, on organisaation välttämätöntä tunnistaa ja arvioida sitä mahdollisesti kohtaavia heikkouksia ja uhkia, sekä näiden uhkien realisoitumisen potentiaalisia seurauksia. Tällainen arviointi on mahdollista toteuttaa koko organisaation kattavan riskianalyysin avulla.

Kuvio 1. Kyberrikolliset käyttävät hyväkseen it-järjestelmien haavoittuvuutta. Mukaillen Gueldry, Gokcek & Hebron 2019, 183.

Gueldryn ym. (2019, 183) mukaan kyberhyökkäykset itsessään ja etenkin niiltä suojautuminen vaikuttavat haastavilta aihepiireiltä. Kuitenkin kyberturvallisuuden perustason ymmärryksen on koettu parantavan päätöksenteon tehokkuutta yhteisöissä. Useimmat hyökkäykset alkavat hyökkääjien tarkoituksesta saada it-järjestelmistä selville tietoja laittomasti. Hyökkäyksen

motiivina saattaa usein olla taloudellisen edun tavoittelu tai ideologiset syyt. Useat organisaatiot maailmalla ovat ottaneet käyttöön tietoturvavalvontaa ehkäisemään hyökkääjiä pääsemästä käsiksi tietovaroihin. Tätä valvontaa voidaan toteuttaa organisaatiossa joko sisäisesti tai ulkoistamalla se ulkoiselle palveluntarjoajalle. Hyökkääjät tunnustelevat jatkuvasti it-järjestelmien ja tietoturvavalvonnan heikkouksia saavuttaakseen päämääränsä hankkia heille tavalla tai toisella hyödyllisiä tietoja.

Haavoittuvuudet ovat perustavanlaatuisia heikkouksia, jotka ovat tyypillisiä monimutkaisille tietojärjestelmille. Kyberhyökkääjät käyttävät näitä järjestelmien haavoittuvuuksia hyväkseen hyökätessään sisään järjestelmiin ja samalla he tekevät itsestään järjestelmän tai sovelluksen käyttöoikeuksien haltijan. Useita uusia järjestelmien haavoittuvuuksia tulee ilmi kuukausittain ympäri maailmaa. Tietokoneohjelmistot sisältävät miljardeja transistoreja ja koodisarjoja, joiden olemassaolo johtaa siihen, että järjestelmissä on aina massoittain potentiaalisia epäkohtia, joista kyberrikollisilla on mahdollisuus päästä käsiksi näihin laitteisiin ja järjestelmiin. Monet näistä epäkohdista jäävät huomaamatta sekä näiden järjestelmien tuottajien että niiden käyttäjien eli asiakkaiden toimesta. Kuviossa 1 on kuvattu nämä neljä kyberhyökkäyksen vaihetta organisaatiossa uhkatekijöistä ja kyberhyökkääjien motiiveista aina tietojen vuotamiseen saakka. (Gueldry ym. 2019, 183.)

Julkisyhteisöt kohtaavat useita vastoinkäymisiä pyrkiessään estämään kyberhyökkäyksiä sekä yrittäessään korjata jo toteutuneiden hyökkäysten aiheuttamia vahinkoja. Tällaisia esteitä ovat muun muassa puutteellinen rahoitus ja kyberosaaminen, ongelmat organisaation johtamisessa, valvonnan puuttuminen sekä vajavaiset tai ei-pakottavat kyberturvallisuuslinjaukset. (Norris ym. 2015, 196.)

Usein todetaan, että ihmisten omalla toiminnalla on suuri merkitys siinä, miten kyberriskejä pystytään hallitsemaan. ”Kyberturvallisuuden heikoin lenkki on ihminen. Ihminen käyttää liian heikkoja salasanoja, unohtaa USB-tikun taksin takapenkille, asentaa tietämättään älypuhelimeensa kuunteluohjelman, hyväksyy sosiaalisen median ohjelmistojen käyttöoikeuden esimerkiksi kaikkiin kontakteihin tai valokuviin puhelimessaan ja niin edelleen.” (Norppa & Peltomäki 2015, 11.) Kyberturva-asioissa kaikkein tärkeintä on ihmisten huolellisuus. Sitä ei voida korostaa liikaa. McAfee arvioi vuonna 2014, että kyberrikollisuuden talousvaikutukset ovat maailmantaloudelle enemmän kuin 400 miljardia dollaria vuodessa ja nämä kustannukset jatkavat kasvamistaan edelleen. Tarkkaa lukua on kuitenkin hankalaa määritellä, sillä myös rikoksen jälkeiseen selvittelyyn uppoaa rahaa huomattavia summia. (Norris ym. 2015, 197.) Kyberrikollisuudessa on todellisuudessa kyse

suuresta taloudellisesta ongelmasta. Esimerkiksi Lähi-idässä kyberrikollisuudesta on muodostunut toiseksi yleisin talousrikosten muoto. Suomessa Poliisin tietoon tulleet tieto- ja viestintärikokset puolestaan lähes kolminkertaistuivat vuodesta 2004 vuoteen 2013 mennessä. (Norppa & Peltomäki 2015, 40.)

3.3 Kyberrikostyypeistä

Kuten perinteistä rikollisuutta, tehdään myös verkkorikollisuutta yleensä tarkoituksena hyötyä anastetuista tiedoista rahallisesti. Toimijat saattavat käydä järjestelmällisesti läpi organisaatioiden erilaisia tietoverkkoja ja tietokoneita yrittäen näin anastaa tietoja, joilla on mahdollista jälleenmyyntiarvoa. Kyberrikosten takana saattaa olla sekä yksityisiä henkilöitä että järjestäytyneitä organisaatioita. Verkkorikolliset saattavat olla erittäin taitavia toiminnassaan ja keksiä jatkuvasti uusia keinoja kyberhyökkäysten toteuttamiseen. Toisaalta joissain tapauksissa kyberrikolliset pyrkivät vahingoittamaan tietokoneita tai tietojärjestelmiä poliittisista tai henkilökohtaisista syistä. (Kaspersky, asiantuntijasivu.)

Kyberrikoksia voidaan toteuttaa hyvin monenlaisin keinoin. Tietoturvayhtiö Kaspersky on listannut kyberrikoksia koskevalla asiantuntijasivullaan erilaisia kyberrikosten tyyppejä. Näistä esimerkkejä ovat sähköposti- ja verkkohuijaukset, yritystietojen varkaudet ja myynti, verkkokiristys, jossa vaaditaan rahaa hyökkäyksen estämiseksi sekä kybervakoilu. Kaspersky myös jakaa kyberrikokset kahteen pääluokkaan: rikoksiin, jotka kohdistuvat tietokoneisiin ja rikoksiin, joissa tietokoneiden avulla tehdään rikoksia. Tietokoneisiin kohdistuvat kyberrikokset sisältävät usein viruksia ja muita haittaohjelmia. Palvelunestohyökkäyksen tarkoituksena taas on estää tietokonetta tai järjestelmää toimimasta niille kuuluvalla tavalla. Tämän tyyppinen hyökkäys siis kaataa järjestelmän lähettämällä siihen valtavan määrän yhteyspyyntöjä. Hyökkääjät saattavat käyttää palvelunestohyökkäystä kiristääkseen rahaa uhrilta.

Kuten aiemmin todettua, rikolliset saattavat yrittää kalastella tietoja myös tietojenkalasteluviestien muodossa. Tällaiset kalasteluviestit lähetetään suurina roskapostimassoina organisaation sähköpostiosoitteisiin ja toiminnan tarkoituksena on huijata loppukäyttäjiä tekemään tietoturvaa heikentäviä toimia. Roskapostit saattavat pitää sisällään viruksia sisältäviä liitteitä ja linkkejä, jotka avaamalla uhri saattaa tahattomasti luovuttaa rikollisille esimerkiksi omat henkilötietonsa. Kokonaisuudessaan sähköpostin käyttö on organisaatiolle aina riski. Sähköpostin päivittäinen

massiivinen määrä muodostaa rasitteen yhteisön kommunikoinnille. Sähköpostit liitetiedostoineen ja linkkeineen nähdään myös vaivattomana tapana syöttää haittaohjelma organisaation sisäverkkoon. (Norppa & Peltomäki 2015, 109.)

Sisäministeriön teettämässä kyberrikollisuutta koskevassa selvityksessä (2017, 24) todetaan, että kaikentyyppiset verkkorikokset ovat yhteensä lähes kaksinkertaistuneet kuuden vuoden aikana. Tilasto on neljän vuoden takaa, joten verkkorikollisuuden määrä on oletettavasti kasvanut entisestään vuosien kuluessa. Yleisimpiä poliisin tietoon tulleita verkkorikollisuuden muotoja ovat tietomurto ja viestintäsalaisuuden loukkaus. Suuressa roolissa ovat myös tietoliikenteen häirintä sekä henkilörekisteririkokset. Kasvavana trendinä voidaan nähdä tietojärjestelmien häirintä, sillä tällaisten kyberhyökkäystyyppien kasvu on ollut yli 12 kertainen vuodesta 2010 vuoteen 2016 tultaessa.

Norpan & Peltomäen (2015, 98) mukaan yksi syy verkkorikollisuuden suureen kasvuun on rikollisten yhä laajempi verkostoituneisuus globaalisti. Kansainväliset rikollisryhmät saavuttavat vuosittain jopa kahden miljardin dollarin hyötyjä tunkeutumalla yritysten ja yhteisöjen tietoverkkoihin maailmanlaajuisesti. Tämä tapahtuu käytännössä lamauttamalla ja lukitsemalla organisaation tietoverkot haittaohjelmalla, ja tämän jälkeen yhteisöä kiristetään luovuttamaan rahaa tietoverkkojen palauttamista vastaan. Keskuskauppakamarin ja Helsingin seudun kauppakamarin teettämän yritysten rikosturvallisuutta koskevan tutkimuksen (2012, 9) mukaan verkkorikosten kohteeksi valikoituivat eritoten suuret yritykset. Kuitenkin vain harvoissa tapauksissa tehtiin rikosilmoitus poliisille. Yritysten ja yhteisöjen merkittävin pääoma on nykyisin tieto. Näin ollen tiedon ylläpitämiseen vaaditaan myös toimivia tietoverkkoja.

3.4 Kyberriskeiltä suojautuminen

Edellä esiteltiin erilaisia kyberrikosten toteutustapoja ja kyberhyökkäysmuotoja. Keinot ovat moninaisia, mutta kyberriskeiltä on kuitenkin mahdollista myös suojautua. Tämä vaatii yhteisöltä tarkkaavaisuutta ja ketteryyttä, sekä jatkuvaa motivaatiota kehittää ja ylläpitää kybervalmiuden kiitettävää tasoa. Tämän tason ylläpitämiseksi organisaatioilla on usein tietohallintohenkilöstöä, joka vastaa kyberturvallisuuden ylläpidosta. On todettu, että tietotekniikka-asiantuntijat ja heidän muodostamansa järjestöt ovat kaikkein aktiivisimpia seuraamaan organisaation tietosuojan tilaa. (Caruson ym. 2012, 451.) Myös esimerkiksi viestintä- ja liikennevirasto Traficomin hallinnoima

Kyberturvallisuuskeskus valvoo tietoverkkojen toimintavarmuutta, sekä tuottaa tietoturvallisuuden tilannekuvaa ja näin ollen myös auttaa yhteisöjä tietoturvallisuuden ongelmatilanteissa.

Norris ym. (2015, 196) ovat todenneet, että joidenkin perustoimintatapojen avulla valtion ja kuntien on mahdollista parantaa kyberturvansa tasoa. Näihin toimintatapoihin lukeutuvat muun muassa yleisten tietoturva-aukkojen arviointi, haavoittuvuuden jatkuva tarkkailu ja testaus, vakuutuksen hankkiminen kyberuhkien varalle, loppukäyttäjien vahva todentaminen ja valtuutuksien varmistaminen heidän käyttäessään organisaation it-järjestelmiä, loppukäyttäjien kouluttaminen ja ohjaaminen, ulkoisten laitteiden käytön valvominen, joihin lukeutuvat muun muassa USB-muistitikut, kyberhyökkäyksiä koskevan tiedon ja kyberturvallisuuden toimintatapojen jakaminen muiden julkisyhteisöjen kanssa sekä kyberturvallisuuskulttuurin luominen valtion tasolla. Kyberturvallisuuskulttuurin vahvistamisessa tärkeää on, että loppukäyttäjät, mutta yhtä lailla myös poliitikot ja virkamiehet, ymmärtäisivät kiitettävän tason kyberturvan merkityksen, ovat koulutettuja ja motivoituneita kyberturva-asioihin ja, että he ovat kyberturva-asioista tilivelvollisia. Tietojärjestelmien ja sovellusten kaksivaiheista todentamista pidetään hyvänä toimintatapana vahvistaa kybersuojaa, mutta se nähdään myös julkisorganisaatioille taloudellisesti hintavana keinona. (Norris ym. 2015, 196.) Toisaalta kyberturvasta huolehtiminen ennalta saattaa kuitenkin muodostua yhteisölle edullisemmaksi, kuin kyberriskin realisoituessa. Andreasson, Riikonen & Ylipartanen (2017, 56) ovat todenneet: ”Asioiden jälkikäteinen selvittely on aina huomattavasti kalliimpaa kuin niiden ennaltaehkäisy. Järjestelmällinen tietosuojariskien hallinta on avain palvelujen turvalliseen toteutukseen, tehokkuuteen ja laatuun. Samalla pystytään hallitsemaan parhaiten aikatauluja ja kustannuksia.”

Wirtz & Weyerer (2016, 1089) mukaan kyberturvatoimet voivat käsittää laajan skaalan erilaisia toimenpiteitä aina perinteisistä toimista nykyaikaisempiin ja teknisempiin kybertoimiin. Perinteisiin kyberturvatoimiin lukeutuvat muun muassa tietojärjestelmien käyttäjävalvonta sekä henkilöstön koulutukset. Nykyaikaisempia ja teknisempiä toimintatapoja ovat esimerkiksi palomuurit, virustorjuntaohjelmistot sekä tiedon salausmenetelmät. Wirtz & Weyerer (2016, 1089) toteavat myös, että mikäli organisaation kyberturvatoimet eivät kykene ehkäisemään kyberhyökkäystä, tulee kriisijohtamisen olla organisaatiossa kiitettävällä tasolla. Näin ollen organisaation IT-asiantuntijuuden täytyy olla korkeatasoista, jotta kyberuhkia pystytään hallitsemaan. Assante & Tobey (2011, 12-13) ovat todenneet, että alati muuttuvat kyberuhat haastavat perinteisiä kyberturvallisuustoimia. Näin ollen organisaatioiden on huomattava, että uudenlaiset kyberuhat

edellyttävät IT-asiantuntijoilta yhä kehittyneempiä kybertoimia ja yhä parempaa asiantuntijuutta. He myös toteavat, että tietohallinnon asiantuntijat saattavat olla usein rajoittuneita omiin organisaatioihinsa, mikä saattaakin aiheuttaa eräänlaista siiloutumista asiantuntijoiden keskuudessa. Tätä asiantuntijuuden siiloutuneisuutta tulisikin pyrkiä purkamaan tietohallinnon asiantuntijoiden keskinäisellä yhteistyöllä.

Olennaista yhteisön kyberhyökkäyksiltä suojautumisessa on organisaation oman kybervalmiuden tilannekuvan tiedostaminen ja ymmärtäminen. On myös oleellista tunnistaa se tieto, joka on yhteisön toiminnan kannalta merkityksellistä ja keskeistä, ja joka väärinkäytettynä muodostaa yhteisölle suuren riskin toteutumisen. Tämän jälkeen yhteisön tulisi kyetä havaitsemaan, ennakoimaan ja torjumaan potentiaalisia tietoturvariskejä. Olisi myös hyvä pohtia, millaiset vaikutukset tietoverkkojen kaatumisella olisi organisaatiolle. Keskiössä tietoturvasta huolehtimisessa on kokonaisuuden hallinta. Jos organisaatio on päättänyt ulkoistaa tietoturvaansa, on olennaista olla tietoinen siitä, kuka yhteisön tietohallintoa hoitaa ja missä kaikkialla yhteisön omistamaa tietoa sijaitsee. Tässä organisaatio ei kuitenkaan voi ulkoistaa vastuutaan kyberturvallisuuden ylläpidossa, vaan organisaation on oltava jatkuvasti tietoinen siinä tapahtuvista muutoksista. Ensiarvoisen tärkeää yhteisössä on hoitaa perusasiat tietoturvan kannalta kuntoon. Se koskee ennen kaikkea perustaitojen kouluttamista henkilöstölle, sekä ohjeiden noudattamisen vaatimista jokaiselta. Olennaista yhteisön kyberriskeiltä suojautumisessa on myös se, että vastuut ja palautumissuunnitelmat poikkeustilanteita varten ovat olemassa. Näistä suunnitelmia on myös hyvä testata säännöllisesti. Yhteisön tulisi niin ikään pohtia, keille kaikille annetaan käyttöoikeudet tietojärjestelmiin ja sovelluksiin. Myös tietoverkon virustorjunnan ja palomuurien täytyy olla kunnossa. (Norppa & Peltomäki 2015, 104-112.) Haasio (2017, 98.) on verkkorikoksia koskevassa teoksessaan listannut erilaisia toimenpiteitä, joita tulisi toteuttaa esimerkiksi haittaohjelman päästyä käsiksi tietokoneisiin. Ensimmäiseksi organisaation tulisi ajaa virustorjuntaohjelmisto laitteillaan ja varmistua siitä, että käytössä on ohjelmiston tuorein versio. Toiseksi korostetaan sitä, että arkaluontoisten sivujen käyttö tulisi lopettaa välittömästi. Arkaluontoisiin sivustoihin voidaan lukea esimerkiksi organisaation sähköposti ja järjestelmät, joissa hallinnoidaan sen varoja. Myös koneen kiintolevy tulisi tyhjentää ja järjestelmät tulisi asentaa uudelleen. Tässä oleellista on, että organisaatio on varmuuskopioinut tietojaan säännöllisesti. Mikäli tietokoneet ja järjestelmät on saatu puhdistettua haittaohjelmasta, tulisi kaikkien järjestelmien salasanat vaihtaa välittömästi.

Sisäministeriön teettämän tietoverkkorikollisuuden torjuntaa koskevan selvityksen (2017, 32-33) mukaan verkossa tapahtuvan rikollisuuden ennaltaehkäisyyn tarvitaan yhteistyötä eri toimijoiden kesken. Myös rikosilmoituksen tekeminen verkkorikostapauksissa nähdään toimivana keinona näiden rikosten ehkäisyssä, ja yhteisöjen tulisikin ilmoittaa organisaatiossaan ilmenevistä kyberhyökkäyksistä poliisille useammin. Arviossa myös todetaan, että tehokkaan kybersuojautumisen tason ylläpidossa on tärkeä niin ikään viranomaisten, syyttäjien ja tuomareiden osaamisen parantaminen koulutusten avulla. Tämä kuitenkin edellyttää näiden toimijoiden osaamisen tunnistamista sekä tämän tunnistamisen pohjalta asianmukaisen koulutuksen järjestämistä.

4. CASE-KAUPUNKI KYBERHYÖKKÄYKSEN KOHTEENA

Tässä luvussa esitellään ja analysoidaan sitä, miksi ja millä tavoin Kokemäen kaupunki joutui kyberhyökkäyksen kohteeksi. Hyökkäys onnistui yllättämään kaupunkiorganisaation täydellisesti, sillä se ei antanut minkäänlaisia merkkejä itsestään ennakkoon. Sen syyt ja hyökkäystapa jäivät myös osittain epäselviksi. Hyökkäys aiheutti myös useita ongelmia organisaation päivittäiselle toiminnalle. Normaali arkitoiminta muuttui nopeasti kriisitilaksi, jossa vallitsi epätietoisuutta. Myöskään talousvaikutuksilta ei säästytty. Seuraavassa kappaleessa on esitelty lainsäädännöllistä taustaa verkkorikosten takana.

4.1 Lainsäädännöllinen tausta

Suomen rikoslaki sääntelee melko kattavasti erilaisia ja eriasteisia rikoksia ja rikosten muotoja. Toki tässäkin esiintyy puutteita, eikä sääntely ole aukotonta. Rikoslaki jättää kuitenkin isohkon aukkokohdan eritoten rangaistusmaksimien osalta verkkorikostapauksissa, sillä ne eivät nykyisellään vastaa tämän päivän uhkakuvia. Rangaistusmaksimien olemassaololla on merkittävä vaikutus siihen, millaiset mahdollisuudet poliisilla on ratkaista verkossa tapahtuvia rikoksia. Rikoslain ohella kyberrikollisuutta säännellään hajanaisesti eri laeissa, kuten tekijänoikeuslaissa, puolustuslaissa, valmiuslaissa, aluevalvontalaissa sekä sähköisen viestinnän tietosuojalaissa. Tietoverkkorikoksen käsitteeseen liittyy tietojenkäsittelyrauha, joka on ikään kuin verrattavissa kotirauhan käsitteeseen. Kun tietojenkäsittelyrauhaa rikotaan, rikoksen tunnusmerkistö täyttyy. Laki on säädetty suojaamaan tietojenkäsittelyn luottamuksellisuutta. Tietomurrosta säädellään rikoslain luvun 38 pykälässä 8. (Norppa & Peltomäki 2015, 73, 77-78.)

Verkkorikolliset keksivät jatkuvasti uusia ja yhä innovatiivisempia tapoja toteuttaa kyberhyökkäyksiä ja kalastella tietoa verkossa. Tämä johtaa siihen, että lainsäädännön on hyvin vaikeaa pysyä alati muuttuvien tekotapojen perässä, eikä uutta lainsäädäntöä keretä valmistella samaan tahtiin. ”Lainsäädännön uusiminen jatkuvasti muuttuvien rikosten tekotapojen ehkäisemiseksi ja rankaisemiseksi on yhtä helppoa kuin neliskulmaisen palikan työntäminen pyöreään reikään. Yritykset saada aikaan kyberrikollisuutta koskevia kansainvälisiä sopimuksia ovat myös hidasta puuhaa” (Norppa & Peltomäki 2015, 73.) Kyberrikollisuus on niin kutsuttua rajat ylittävää rikollisuutta, sillä globaalissa maailmassa näiden rikosten suunnittelu ja toteuttaminen käyvät helposti yli kansallisten rajojen. Tämä johtaakin siihen, että kyberrikosten tekijöiden ja toisaalta kyberrikosten

kohteeksi joutuvien uhrien fyysisellä sijainnilla ei ole merkitystä. Samalla lakien säätämisestä tulee entistä haastavampaa. Sisäministeriön kyberrikollisuutta käsittelevän asiantuntijasivun mukaan suurin osa tietoverkkoihin kohdistuvasta rikollisuudesta jää tulematta poliisin tietoon. Ne verkkorikokset, joista poliisi käynnistää esitutkinnan, eivät useimmiten ratkea koskaan täysin. (Sisäministeriö, asiantuntijasivu.)

Vuoden 2020 alussa tuli Suomessa voimaan laki koskien julkisen hallinnon tiedonhallintaa. Lain tarkoituksena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja tietoturvallinen käsittely. Lain pykälässä 13 käsitellään julkisyhteisöjen tietoaineistojen ja tietojärjestelmien tietoturvaa. Siinä on todettu, että tietoa hallinnoivan julkisyhteisön on seurattava toimintaympäristönsä tietoturvan tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on myös selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. (Tiedonhallintalaki, 13 §.)

Lain mukaan viranomaisen on järjestettävä tietohallintonsa tiedonhallintayksiköissä. Erillisiä tiedonhallintayksiköitä muodostavat muun muassa kunnat ja kuntayhtymät, joihin liittyvät kaikki kyseisen kunnan tai kuntayhtymään kuuluvat viranomaiset. Tiedonhallintayksikön velvollisuuksiin kuuluu suunnitella, miten lain vaatimukset toteutetaan yksikön sisällä. Velvollisuuksiin kuuluvat myös ohjeistuksen laatiminen, tarvittavan koulutuksen järjestäminen sekä lain vaatimusten toteuttamisen ja ohjeiden noudattamisen valvominen. (Aitta & Herrala 2019, 8.)

4.2 Kokemäen kaupunkiorganisaatioon kohdistunut hyökkäys

Kokemäen kaupungin kyberhyökkäystapauksessa moni asia jäi lopulta osittain epäselväksi. Selvittämättä jäivät muun muassa se, mikä taho hyökkäyksen alun perin käynnisti sekä se, millä tavoin kuntaorganisaation tietojärjestelmiin päästiin käsiksi. Kuten aiemmin tutkimusraportissa on todettu, sisäisiin tietojärjestelmiin on mahdollista päästä sisään hyvin monin eri keinoin. Näihin lukeutuvat muun muassa tietojenkalasteluviestit sekä virustorjunnan heikkouksien hyväksikäyttö. Myöskään hyökkäyksen toteuttamisen konkreettinen ajankohta ei selvinnyt kuntaorganisaatiolle koskaan. Hyökkäys osui kesälomakauteen, jolloin suuri osa organisaation työntekijöistä oli poissa työpaikaltaan. Hyökkäys huomattiin heinäkuisena maanantainaamuna, kun työntekijät palasivat viikonlopun vietosta töiden pariin. Haittaohjelma oli näin ollen saanut tehdä tuhoa kaupungin sisäverkkoon yhteydessä olleissa laitteissa koko viikonlopun ajan. Ongelmien tultua ilmi toimet

tietojen mahdolliseksi pelastamiseksi aloitettiin välittömästi. Hyökkäys ilmeni sisäiseen verkkoon ujutettuna haittaohjelmatiedostona, joka pyrki järjestelmällisesti ja mahdollisimman laajasti kopioimaan itseään ja kryptaamaan kaikki tiedostot, jotka se pystyi sisäisessä verkossa käsittelemään.

”Mutta se ongelma on ehkä Kokemäen tapauksessa se, että eihän siitä ole tosiasiallista tietoa, että koska se (haittaohjelma) on sinne verkkoon tullut, koska se ohjelma tai se hyökkäys on ollut tavallaan niin hyvin suunniteltu, että ne kaikki jäljet on myöskin pystytty peittämään. Eli tämmöiset niin sanotut lokitiedostot, mitä tommoisissa järjestelmissä aina tulee koko ajan kaikista asioista, niin Kokemäen kaupungin tapauksessa myös ne kaikki menetettiin.” – Haastateltava 1

Haittaohjelma myös lukitsi kaupungin sisäverkossa sijaitsevat tiedostot. Tämän jälkeen kaupunki vastaanotti sähköpostiviestin, jossa vaadittiin rahaa tiedostojen ja järjestelmien lukitsemisen avaamista sekä tietojen palauttamista vastaan. Tähän viestiin kaupunki ei kuitenkaan luonnollisesti reagoinut millään tavoin, vaan tiedot pyrittiin palauttamaan itsenäisesti muilla tavoin. Hyökkäyksestä tehtiin rikosilmoitus poliisille, joka pyrki mahdollisuuksiensa mukaan keräämään todistusaineistoa hyökkäyksestä. Tutkinnassa ei kuitenkaan selvinnyt hyökkäyksen aiheuttajatahoa eikä tekotapaa, sillä todistusaineistoa oli haittaohjelman toimesta pystytty merkittävissä määrin tuhoamaan. Poliisitutkinta tapauksesta on kaupunkiorganisaation mukaan jo päättynyt.

4.3 Hyökkäyksen vaikutukset kaupunkiorganisaatioon ja asukkaisiin

Kyberhyökkäys aiheutti eriasteista haittaa Kokemäen kaupunkiorganisaatiolle sekä kaupungin asukkaille. Merkittävimpänä hyökkäyksen aiheuttamana haittana läpi haastattelujen nähtiin maksuliikenteen keskeytyminen. Myös kaikki asiakastietojärjestelmät ja koulutoiminnan järjestelmät olivat poissa käytöstä. Helpotuksena koettiin se, että Kokemäen kaupungilla ei ollut omaa potilastietojärjestelmää, jonka tiedot olisivat niin ikään erittäin kriittisiä ja riskialttiita joutuessaan tietomurron kohteeksi. Kuitenkin yhteydet kuntayhtymässä sijaitseviin potilastietojärjestelmiin jouduttiin sulkemaan hyökkäyksen seurauksena, jotta ne säilyisivät saastumattomina. Maksuliikenteen häiriöt kulminoituivat sosiaalihuollossa, jossa esimerkiksi täydentävää ja ennaltaehkäisevää toimeentulotukea ei kyetty myöntämään tietojärjestelmien avulla, vaan asiassa jouduttiin turvautumaan manuaaliseen päätöksentekoon ja maksamiseen. Kaupunki ei kyennyt maksujärjestelmissään maksamaan ainuttakaan laskua hyökkäystä seuraavien kahden viikon aikana,

eikä myöskään kirjanpitoa tehty. Välttämättömimmät maksut hoidettiin pankin kanssa manuaalisesti. Myös kaupungin sähköpostiliikenne oli poikki, eikä muutaman viikon aikaisia sähköposteja pystytty palauttamaan lainkaan.

Kuntalaisten kannalta ehkä merkittävin haitta aiheutui, kun hyökkäyksen yhteydessä päästiin käsiksi kaupungin ylläpitämiin henkilötietoihin. Kaupunki ei ole pystynyt poissulkemaan sitä uhkakuvaa, etteivät hyökkäyksen aiheuttajat olisivat onnistuneet onkimaan henkilötietoja järjestelmistä. Toisaalta kaupunki ei ole kuitenkaan havainnut merkkejä siitä, että asukkaiden henkilötietoja olisi käytetty hyväksi laittomasti.

”Niin tämä tietosuojapuoli on tässä itseasiassa varmaan tämä kaikista semmoinen harmillisin asia ja asia, joka koskettaa kuntalaisia ehkä kuitenkin eniten. Mutta ei siitä ymmärtääkseni sen jälkeen mitään viitteitä olisi, että niitä (henkilötietoja) olisi myöskään mitenkään käytetty kuntalaisia vastaan tai mitään tällaista. Mutta jos sitä näin jälkeen päin katsoo, niin se ehkä se huolestuttavin piirre siinä tapahtuneessa hyökkäyksessä oli, että se hyökkääjä pääsi käsiksi niihin henkilötietoihin. Ja mahdollisesti on pystynyt myöskin anastamaan niitä tietoja sieltä.” – Haastateltava 1

Kaupunki pystyi kuitenkin varmistumaan siitä, että tietokannat, jotka olivat päällä hyökkäyksen tapahtuessa, säästyivät henkilötietojen kaappaukselta. Näin ollen hyökkäyksen kohteeksi joutui ainoastaan pienempiä tiedostoja, joista henkilötietoja on saattanut joutua ulkopuolisten haltuun. Tämä varmisti sen, että suurin tiedostomassa säästyi haittaohjelmahyökkäykseltä. Haittaohjelma nähtiin kuitenkin ainoastaan viruksena, joka lukitsi järjestelmät ja tiedostot, ja joka vaati rahaa tiedostojen palauttamiseksi. Näin ollen se ei lähtökohtaisesti pyrkisi välttämättä anastamaan järjestelmissä sijaitsevia tietoja, vaan pelkästään lukitsemaan ne rahallisessa hyötymistarkoituksessa. Kokemäen kaupungin tapauksessa kyseessä on kuitenkin tietoturvaloukkaus, sillä näihin arkaluontoisiin tietoihin päästiin käsiksi ja niitä muutettiin siten, että ne eivät olleet enää kuntaorganisaation itsensä käytettävissä.

4.4 Hyökkäyksen vaikutukset kuntatalouteen

Kokemäki on kokonsa puolesta suhteellisen pieni kuntaorganisaatio. Näin ollen myös kunnan budjetti ei ole merkittävän suuri. Henkilöstöä on vähemmän kuin suuremmissa kaupungeissa ja tästä syystä

myös toiminnassa käytettävien laitteiden ja tarvittavien järjestelmälisenssien määrä ei ole valtava. Verraten samoihin aikoihin toteutuneisiin kyberhyökkäyksiin Lahden ja Porin kaupungeissa, aiheutti Kokemäen kaupunkiin kohdistunut hyökkäys vähemmän talousvaikutuksia. Joitain kuluja ei kuitenkaan pystytä tarkasti laskemaan. Esimerkiksi kuntaorganisaation oma henkilöstö saattoi tehdä merkittävästi arvioitua enemmän töitä kriisitilan hoidossa, sillä kaikki muut työt olivat keskeytettynä. Tämä saattoikin myös aiheuttaa ylimääräisiä kuluja kaupunkiorganisaatiolle.

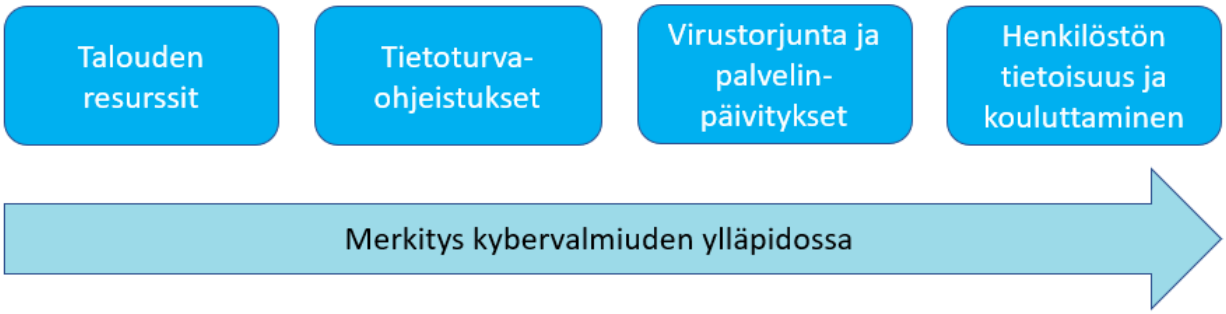
”Palkat juoksee tehdään mitä tahansa, ja iso osa henkilökunnasta teki kyberturvallisuushyökkäykseen liittyviä töitä ja muut työt oli taka-alalla.” – Haastateltava 3

Suurin osa hyökkäyksen seurauksena muodostuneista kustannuksista olivat seurausta asiantuntijapalveluista, joita jouduttiin ostamaan usean kuukauden ajan enemmän kuin tavallisesti. Haittaohjelman seurauksena massoittain organisaation järjestelmiä saastui ja niitä jouduttiin ostamaan ja asentamaan uudelleen palveluntarjoajilta. Osittain näistä uudelleenasennuksista muodostui myös kuluja. Kunnalle muodostui käyttömenoja palvelinten ja järjestelmien alasajosta ja niiden saattamisesta jälleen käyttökelpoisiksi. Karkeasti arvioiden hyökkäyksen aiheuttamat kustannukset olivat Kokemäen kaupungille noin 30 000-40 000 euroa.

Välillisiä, pidemmällä aikavälillä muodostuvia kustannuksia saattaa koostua tietoturvan kehittämistyöstä, jota on alettu tehostaa toteutuneen hyökkäyksen jälkeen. Näihin kustannuksiin lukeutuvat muun muassa laitekannan ja uusien käyttöjärjestelmien päivittäminen, mikä saattaa pidemmällä aikavälillä viedä suurenkin osan kaupungin budjetoinnista. Toisaalta järjestelmien ja laitteiden päivittäminen nähtiin työnä, jota jouduttaisiin joka tapauksessa tekemään ennemmin tai myöhemmin. Nyt menot näistä päivityksistä ainoastaan realisoituvat luultavasti suunniteltua aiemmin.

5. ANALYYSITULOKSET JA TULKINTA

Analyysiosiossa esitellään aineistosta esiin nousevia, tutkimusalueelle kuuluvia tuloksia ja tulkitaan niitä tutkimusongelmaan vastaten. Tutkimuksen empiiriseksi kohteeksi valittiin Kokemäen kaupungin johtohenkilöstöä, joka oli mukana vastaamassa kesän 2019 kyberhyökkäyksen aiheuttamien vahinkojen korjaamisesta sekä kriisiviestinnästä niin kuntaorganisaation sisä- kuin ulkopuolellekin. Tutkimuksessa kartoitettiin kyseisen kaupungin johtohenkilöstön näkemyksiä muun muassa siitä, millä tavoin ja toimin kaupunki on parantanut kybervalmiutensa tasoa kuntaorganisaatiossa, sekä millaisia potentiaalisia kyberturvallisuustoimia yhteisöjen olisi yleisesti ottaen suotavaa toteuttaa kiitettävän kybervalmiuden tason ylläpitämiseksi. Analyysiosion teema muodostuu tutkimuskysymysten mukaisesti: Millaisia toimia Kokemäen kaupunki on tehnyt kybervalmiutensa parantamiseksi, sekä millä tavoin kyberturvallisuutta on huomioitu kaupungin talousarvio- ja strategiadokumenteissa. Tutkimuskohteena olevien henkilöiden nimiä ja virkasuhteita ei paljasteta ja heidän vastauksensa kuvataan siten, etteivät nämä henkilöt ole suoraan tunnistettavissa. Kyseisiä henkilöitä lähestyttiin sähköpostitse, ja tutkimusaineisto kerättiin 30-50 minuuttia kestäneillä teemahaastatteluilla maaliskuussa 2020. Haastatteluvalinnat tehtiin tutkimuksen tavoitteiden pohjalta siten, että tutkimuskysymyksiin saataisiin vastauksia mahdollisimman laajasti usealta asiantuntija-alalta. Haastateltavia tutkimuksessa oli neljä.



Kuvio 2. Eri toimenpiteiden ja resurssien merkitys kyberturvallisuudessa.

5.1 Talouden resurssit

Haastatteluaineistoon peilaten taloudelliset resurssit nousivat yhdeksi oleelliseksi seikaksi pohdittaessa kyberturvatoimia ja niiden vaatimia resursseja. Talouden resurssit ovat väistämättä osa

kyberturvatoimia, sillä ilman riittävää pääomaa kiitettävän tason kyberturvan ylläpito muodostuu mahdottomaksi tehtäväksi. Suuria kulueriä kyberturvatoimien osalta ovat muun muassa päätelaitteiden sekä ohjelmistojen ja järjestelmien hankinnat. Myös mahdollinen tietoturvan ulkoistaminen lisää organisaation kyberturvamenoja. Organisaatiossa myös nähtiin, että pienessä kunnassa tietoturvan järjestäminen saattaa kohdata enemmän resurssipulaa, kuin vaikkapa suuremman kokoluokan kaupungeissa. Taloudellisiin resursseihin ja niiden puutteeseen nähtiin liittyvän myös osaavan ja asiantuntevan henkilöstön hankkiminen.

”Että sekä se, että pienessä kunnassa, jossa on itse järjestetty tietohallinto, niin ensinnäkin henkilöstön ihan ajalliset resurssit, ja toinen on sitten se asiantuntijuus, että kuinka perillä siitä ollaan. Että jos sen organisaation tietohallinto on pari-kolme ihmistä, niin ei ne voi kaikkea osata, eikä niillä kaikkeen riitä aika, jos niitä päätteitä, jotka ovat kiinni siinä verkossa, on iso määrä --. Ja taloudelliset resurssit nyt vähän viitaten siihen henkilöstöön, mutta myöskin siihen, että saadaan ne kaikki laitteet pidettyä ajan tasalla. Että kun ne nyt aina vaan silloin tällöin vanhenevat ja niihin ei välttämättä uusimpia käyttöjärjestelmiä saa asennettua tai päivitettyä. Niin sitä infraa pitää uusia aktiivisesti ennen kuin se tulee tiensä päähän.”– Haastateltava 1

Pienessä kunnassa myös resurssien saaminen tietohallintoa varten saattaa olla haasteellista, sillä kunnan taloudelliset resurssit kohdistetaan luonnollisesti ensin välttämättömien, lain edellyttämien tehtävien hoitoon. Laissa julkisen hallinnon tiedonhallinnasta on todettu, että tietoa hallinnoivan julkisyksikön on seurattava toimintaympäristönsä tietoturvan tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Laissa todetaan myös, että tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. (Tiedonhallintalaki, 13 §.) Laki ei kuitenkaan määrittele tarkemmin kiitettävän tietoturvan konkreettista tasoa, vaan siinä korostetaan ainoastaan tietoturvallisuustoimenpiteiden mitoittamista julkisyhteisöjä mahdollisesti kohtaavia riskejä vastaaviksi. Näin ollen tietoturvan tasossa saattaa olla merkittävääkin vaihtelua eri kuntaorganisaatioiden välillä, eikä resurssien saaminen tietoturvan ylläpitoon ole täysin itsestään selvää. Kokemäen kaupungin tapauksessa talouden resurssien kohdentaminen juuri kyberturvan ylläpitoon on jossain määrin parantunut tapahtuneen hyökkäyksen johdosta.

”-- ja sitten tietysti vuosittain on saatu tietty summa käyttää tähän toimintojen kehittämiseen. Että se on vähän niin kuin vakiintunut meille, että saadaan pidettyä nämä ajan tasalla, ettei tartte tehdä vanhoilla laitteilla ja ohjelmistoilla töitä sen takia, että rahat olisivat loppu. Että se ei ole sinänsä

ollut esteenä. Että mitä me tuossa (nimi) kanssa ollaan haluttu taikka vaadittu, niin se on kyllä saatu." – Haastateltava 4

Kokemäen kaupunki on vuoden 2020 talousarviossaan kohdistanut investointimäärärahaa ohjelmistovaraukselle. Tämä varaus käsittää muun muassa ohjelmistojen ja järjestelmien päivitys- ja uudelleenhankkimiskustannuksia. Osittain se muodostuu esimerkiksi Ofiice365-lisenssimaksuista. Ohjelmistovarauksen kokonaissummaksi on merkitty 75 000 euroa.

Kysyttäessä siitä, millaisia ongelmia kuntaorganisaatio on kohdannut oman kybervalmiutensa ylläpidossa, olivat vastaukset osittain talouden resursseihin liittyviä puutteita.

"No osittain tietysti tulee aina ne taloudelliset asiat vastaan. Ei se oo ihan sillä tavalla, että sormia napsautetaan ja me laitetaan kaikki nyt kuntoon. Vaan se, että jonkinlainen etenemissuunnitelma siinäkin pitää olla, että mitkä on ehdottomasti laitettava nyt just kuntoon" – Haastateltava 3

Toisaalta kuitenkin nähtiin, että kuntaorganisaation koko ei välttämättä ole aina yhteyksissä siihen, millä tasolla tietohallintoa ja kyberturvaa pystytään ylläpitämään. Samoihin aikoihin toteutuneet hyökkäykset Lahden ja Porin kaupungeissa osoittavat, että suuremmat kaupungit ovat yhtä lailla alttiita verkossa toteutettaville hyökkäyksille, eivätkä talouden resurssit tai kaupunkiorganisaation koko korreloi aina parhaan tietoturvan tason kanssa. Merkitystä on niin ikään myös muilla seikoilla, kuten koko organisaation kattavilla tietoturvaohjeistuksilla sekä henkilöstön asiantuntevuudella ja tietoisuudella tietoturvariskeistä.

5.2 Tietoturvaohjeistukset

Kaupungilla oli ennen heinäkuun 2019 kyberhyökkäystä käytössään erilaisia ja eriasteisia toimia, joilla pyrittiin ylläpitämään kybervalmiuden riittävää tasoa. Kaupunki oli esimerkiksi laatinut muutamaa vuotta aiemmin tietoturvaperiaatteet ja -ohjeistukset, joita oli ehditty kouluttaa henkilöstölle kiitettävissä määrin. Näissä tietoturvaa koskevissa ohjeistuksissa oli määritelty muun muassa salasanakäytäntöjä ja käyttäjäohjeistusta sähköpostin käytössä. Sähköpostiohjeistus koski erityisesti turvallista sähköpostin käyttöä ja ohjeistusta roskapostiin sekä epäilyttäviin linkkeihin ja liitetiedostoihin liittyen. Osittain näitä ohjeistuksia jouduttiin kuitenkin muuttamaan kyberhyökkäyksen jälkeen, jolloin niitä muutettiin entistä tarkemmiksi ja vahvemmiksi. Kaikki

tietoturvaperiaatteet ja -ohjeistukset on käyty kyberhyökkäyksen jälkeen uudelleen läpi ja niitä on tiukennettu. Niitä on myös käyty uudelleen läpi koko henkilöstön kanssa

Herrala (2019, 8) toteavat, että tiedonhallintayksikön velvollisuuksiin kuuluu tietoturvaohjeistuksen laatiminen, tarvittavan koulutuksen järjestäminen sekä tiedonhallintalain vaatimusten toteuttamisen ja näiden ohjeiden noudattamisen valvominen. Kuten Norppa & Peltomäki (2015, 98) ovat todenneet, riittävät tietoturvaohjeistukset ovat elinehto kyberturvallisuuden ylläpidossa. Kokemäen tapauksessa nämä ohjeistukset saattoivat säästää kaupunkiorganisaation suuremmilta vaurioilta, sillä kriisitoimet hyökkäyksen jälkeen pystyttiin aloittamaan välittömästi. Kuntaorganisaatiossa koettiinkin, että nimenomaan valmiina olleiden suunnitelmien ja ohjeistusten avulla henkilöstö pystyi tekemään tarvittavat toimenpiteet ennalta määrätyssä järjestyksessä. Tietoturvaperiaatteissa ja -ohjeistuksissa oli määritelty muun muassa se, mitkä järjestelmät ovat kuntaorganisaation toiminnan kannalta kaikkein kriittisimmät. Nämä ohjelmistot myös palautettiin ensimmäisinä takaisin toimintaan.

5.3 Virustorjunta ja palvelinpäivitykset

Tietokoneiden suojaaminen kaikenlaisilta verkossa esiintyviltä viruksilta ja haittaohjelmilta tapahtuu ensisijaisesti virustorjuntaohjelmistoilla ja niiden sisältämillä palomuureilla. Kokemäen kaupungilla oli luonnollisesti käytössään virustorjuntaohjelmistot ja näennäisesti toimiva palomuuri. Palomuurin sääntöjä oli ennen hyökkäystä käyty läpi ja sen oli todettu olevan kunnossa. Palomuurin täydestä toimivuudesta ei kuitenkaan saatu kaupunkiorganisaation sisällä täyttä varmistusta, sillä haittaohjelman aiheuttajasta ja sisäänmenoaukosta ei saatu koskaan varmuutta.

”Että siinä mielessä oli ollut tietoturvaan liittyviä toimia paljonkin, mutta saattoi olla esimerkiksi, kun se tietoturva liittyy tavallaan kaikkeen, jokaiseen tietokoneeseen, joka on kiinni siinä sisäisessä verkossa, niin välttämättä sitä ihan koko ICT-infrastruktuuria ei ollut tarpeeksi tarkalla tasolla käyty läpi. Että kaikissa tietokoneissa ja palvelimissa olisi välttämättä ihan se viimeisin käyttöjärjestelmäpäivitys olemassa ja näin.” – Haastateltava 1

Kaupunki toteutti organisaatiossaan myös säännöllisiä palvelinpäivityksiä, jotka käsittävät kaupungin käytössä olevien järjestelmien säännölliset päivitykset Myös kaikkien kaupungin käytössä olevien työasemien päivitykset tehtiin säännöllisesti. Kaupunki oli hankkinut virustorjuntaohjelmistostaan uusimman version, jonka olisi kuulunut tarttua haittaohjelmaan kiinni. Virustorjuntaohjelmisto ei kuitenkaan reagoinut haittaohjelmahyökkäykseen millään tavoin. Myöhemmissä

Kyberturvallisuuskeskuksen ja poliisin tuottamissa selvityksissä kävi ilmi, että myös haittaohjelma oli uusinta versiota tunkeutuessaan kaupungin sisäverkkoon ja näin ollen virustorjuntaohjelmistolla ei olisi ollut mahdollisuuksia havaita hyökkäystä.

Kyberhyökkäyksen jälkeen eri palvelinten ja järjestelmien seuranta on muuttunut kaupungissa entistä aktiivisemmaksi. Organisaatiossa nähtiin, että yleisesti ottaen kyberturvallisuuden aktiivisessa ylläpidossa päivitysten tulee olla kunnossa, laitteiston ajan tasalla sekä palomuureja ja järjestelmien lokeja tulisi seurata jatkuvasti.

”Että tavallaan se koko ICT-infra pitää ottaa aktiivisemmin tarkasteluun, ja ei saa tuudittautua siihen harhaluuloon, että joku virustorjuntaohjelmisto tekisi autuaaksi.” – Haastateltava 1

Toisaalta kuitenkin nähtiin, että myös kyberrikolliset kehittävät jatkuvasti uusia keinoja toteuttaa verkkorikollisuutta, ja näin ollen kyberriskeiltä suojautumisesta saattaa muodostua organisaatiolle suuriakin haasteita.

”Että tietysti tää kyberturvallisuus on varmaan semmoista, että siellä vastapuolellakin varmaan koko ajan kehitetään uusia ja uusia systeemeitä, että päästäisiin tulemaan läpi ja tekemään haittaa, niin kyllähän se jatkuvaa taistelua on tällä puolella. -- mutta kyllä mä näkisin, että kun se kautta linjan on se päivitysrakenne sillä tavalla, että pidetään ne mahdollisimman ajan tasalla ja turvallisina, niin emmä näkis, että mitä täällä voisi sitten toisin tehdä.” – Haastateltava 4

Kuten Norris ym. (2015, 196) toteavat, yleinen tietoturva-aukkojen havainnointi, haavoittuvuuden jatkuva tarkkailu ja testaus sekä ulkoisten laitteiden käytön valvominen ovat julkishallinnon kyberturvan perustoimintatapoja, joilla kyberriskejä voidaan pienentää. Näitä toimintoja myös Kokemäen kaupunki on organisaatiossaan vahvistanut kyberhyökkäyksen jälkeisinä toimenpiteinä. Havainnointia ja valvontaa on tehostettu niin tietohallinnon kuin organisaation muidenkin työntekijöiden osalta. Kaikki sisäisessä verkossa kiinni olevat laitteet, mukaan lukien yksittäiset tietokoneet ja palvelimet, on päivitetty. Tietokoneita ja muita laitteita on myös uusittu jonkin verran. Kaupunki on käynnistänyt uuden Windows-10 -projektin, jonka seurauksena laitteistoja ja sovelluksia on uusittu ja päivitetty laajemmin. Kaupungin kaikki salasanakäytännöt on muutettu ja monimutkaistettu.

”Sitä verkkoa on muistaakseni ja minun käsittääkseni pyritty edelleen rajaamaan pienempiin osiin silleen, että siellä ei tavallaan sillä yhdellä tunnuksella pääse verkon osasta toiseen liikkumaan.” – Haastateltava 1

Myös erilaisten järjestelmien lokien seurantaa on tehostettu. Muuta käytännön valvontaa tietoturvan osalta on muutettu aktiivisemmaksi ja laaja-alaisemmaksi, jotta tietoturvassa tapahtuviin muutoksiin pystyttäisiin vastaamaan mahdollisimman nopeasti.

Kuten Gueldryn ym. (2019, 183) toteavat, kyberrikolliset tunnustelevat jatkuvasti tietojärjestelmien ja tietoturvavalvonnan heikkouksia, joiden kautta organisaatioiden sisäverkkoihin on mahdollista päästä käsiksi. Kokemäen kaupunki on hyökkäyksen seurauksena toteuttanut ulkoisen tietoturva-auditoinnin, jossa ulkoisen palveluntarjoajan toimesta on pyritty käymään läpi kaikki mahdolliset sisäverkossa esiintyvät heikkoudet. Tässä niin kutsutussa penetraatiotestauksessa pyrittiin varmistamaan se, että kaupungin verkko on ulospäin mahdollisimman turvallinen.

”-- elikkä käytiin läpitte yhden yrittäjän toimesta se, että meidän ulkoisten ip-osoitteiden näkyvyys maailmalle tarkistettiin, että ne on kunnossa. Että sieltä ei ole olemassa mitään semmosia ongelmia niiden suhteen, että ne olisi väärin ohjelmoitu, tai mahdollistaisi näiden haittaohjelmahyökkäysten tulemisen tai näiden väärinkäytön.” – Haastateltava 4

Testauksen tulos oli siinä mielessä myönteinen, että siinä ei löytynyt syytä, joka olisi voinut selittää kyberhyökkäyksen aiheutumisen. Näin ollen kuntaorganisaatio pystyi testauksen avulla ikään kuin varmistumaan siitä, että virustorjunta ja palomuurit toimivat niille kuuluvalla tavalla vastaisuudessa.

”Tarkoittaa silloin, että meidän nämä palomuurit ja muut on hyvässä kunnossa ja niissä ei ollut mitään häiriöö taikka vikaa” – Haastateltava 4

5.4 Henkilöstön tietoisuus ja kouluttaminen

Kuten aiemmin raportissa on todettu, henkilöstön tietoisuus ja asiantuntevuus tietoturva-asioissa on jopa tärkeimpiä asioita kyberriskien toteutumisen torjunnassa. Samoin Norris ym. (2015, 196) ovat todenneet, että yhteisöjen suurin kyberuhka ovat loppukäyttäjien inhimilliset erehdykset päivittäisessä työssään. Näiden erehdysten kautta organisaation henkilöstö joko vahingossa tai

tahallisesti avaa esimerkiksi sähköpostiviestien mukana tulleita tiedostoja ja linkkejä. Tutkimukset ovat myös osoittaneet, että tieto- ja asiantuntijuuskuilu tietohallinnon asiantuntijoiden ja hallinnon virkamiesten välillä on suurempi paikallistason organisaatioissa kuin valtion tasolla. (Caruson, MacManus & McPhee 2012, 2). Kokemäen kaupunkiorganisaatiossa koettiin, että tietoturva-asiantuntijuus on keskittynyt enemmän tietohallinnon asiantuntijoille, eivätkä vikamiehet kokeneet olevansa ammattitaitonsa puolesta täysin kykeneviä vastaamaan kyberturvallisuuden ylläpidon mukanaan tuomiin haasteisiin. Kuntaorganisaatiossa koettiin myös, että henkilöstön kouluttaminen sekä tiedon ja ohjeistusten jakaminen on merkittävässä roolissa etenkin sähköpostin kautta tulevien virusten ja haittaohjelmien ehkäisyssä. Henkilöstölle annetun ohjeistuksen tulisi olla mahdollisimman selkeää ja yksinkertaista, jotta kyberriskien realisoitumista olisi mahdollista ehkäistä.

”Ja tietysti aina korostetaan sitä, että siinä näppäimistön ja tuolin välissä se on se suurin tietoturvariski, eli se käyttäjä itse. Eli henkilöstöllä on oikeasti tarpeeksi hyvät ja yksinkertaiset ohjeet siihen, että mitä henkilöstö saa tehdä ja mitä ei saa tehdä, mikä on tietoturvallista ja mikä ei oo tietoturvallista. -- Eli se henkilöstön kouluttaminen on erittäin tärkeässä asemassa.”

– Haastateltava 1

Kuntaorganisaatiossa nähtiin, että kyberturvan ylläpidossa tärkeintä on koko organisaation ymmärrys tietoturva-asioista. Tähän liittyy se, että kautta koko organisaation kaikkien asioiden tulisi olla kunnossa. Yksi vähemmälle huomiolle jätetty osa-alue saattaa aiheuttaa koko tietoturvaketjun romahtamisen. Henkilöstön kouluttamiseksi kaupunkiorganisaatio on hankkinut palvelun, jossa jokaisen henkilöstön jäsenen on suoritettava tietoturvakoulutus.

”Tänä vuonna meillä on ainakin ostettu semmoinen (järjestelmä) palvelu, se on koko vuoden meidän käytössä ja sieltä on kaikkien pakko käydä suorittamassa tietoturvallisuusosuudet.”

– Haastateltava 3

Toisaalta hyökkäyksen seurauksena henkilöstöstä on tullut myös tietoisempaa tietoturvan osalta. Työntekijät tarkkailevat omia työasemiaan nykyään tarkkaavaisemmin ja huomioivat epäilyttävää toimintaa laitteillaan aktiivisemmin. Henkilöstöön liittyvien tietoturvaheikkouksien nähtiin olevan usein seurausta henkilöstön huolimattomuudesta ja piittaamattomuudesta. Myös tähän nähtiin

ratkaisuna jatkuva henkilöstön ohjeistaminen ja opastaminen, sekä tietoturva-asioiden aktiivinen esillä pitäminen. Kuntaorganisaatiossa todettiin myös, että ohjeita ja sääntöjä laiminlyötäessä jokaisella työyhteisön jäsenellä on velvollisuus tuoda ongelmakohdat esille organisaatiossa.

5.5 Analyysitulosten yhteenveto

Taulukko 1. Kyberturvatoimet Kokemäen kaupunkiorganisaatiossa ennen kyberhyökkäystä ja hyökkäyksen jälkeen

Kyberturvatoimet ennen hyökkäystä	Kyberturvatoimet hyökkäyksen jälkeen
Virustorjuntaohjelmistot ja palomuuri	Virustorjuntaohjelmistot ja palomuuri
Säännölliset palvelinpäivitykset	Säännölliset palvelinpäivitykset
Tietoturvaperiaatteet ja -ohjeistukset	Tietoturvaperiaatteet ja -ohjeistukset ja niiden uudelleen läpikäynti
	Salasanakäytäntöjen muuttaminen ja monimutkaistaminen
	Ulkoinen tietoturva-auditointi
	Uusien järjestelmien ja laitteiden hankkiminen
	Palvelinten ja järjestelmien aktiivisempi seuranta ja päivittäminen
	Valvonnan ja havainnoinnin tehostaminen läpi organisaation

Yleisesti voidaan todeta, että kyberturvatoimet Kokemäen kaupungissa ovat parantuneet ja lisääntyneet kyberhyökkäyksen myötä. Myös täysin uusia toimia on otettu käyttöön, kuten esimerkiksi ulkoinen tietoturva-auditointi. Kuten aineiston analyysissa kävi ilmi, henkilöstön tietoisuudella ja kouluttamisella on tietoturva-asioissa usein merkittävin rooli. Tämä edellyttää sitä, että organisaatio on tietoinen henkilöstönsä osaamisesta tietoturvan suhteen. Osana henkilöstön tietoisuuden ja osaamisen kasvattamista voidaan pitää tietoturvaohjeistuksia, joiden avulla henkilöstön on mahdollista perehtyä organisaation tietoturvaan. Tämän perehtymisen tulisi olla myös pakollista koko henkilöstölle, jotta voidaan varmistua siitä, että tietoturva-asiat koskettavat koko organisaatiota. Tietoturvaohjeistusten avulla henkilöstö pysyy myös ajan tasalla siitä, mikä organisaatiossa on tietoturvan kannalta hyväksyttyä, ja millaisia toimintatapoja henkilöstön tulisi välttää toiminnassaan.

Tietoturvaperiaatteissa ja -ohjeistuksissa saattaa niin ikään olla ohjeistusta organisaation virustorjuntaohjelmistoista sekä palomuureista. Tietoturvaperiaatteissa saattaisi olla hyvä käydä läpi organisaation tietoturvaprosesseja virusturvaan ja palomuureihin liittyen, jotta koko henkilöstöllä on mahdollisuus perehtyä näihin prosesseihin. Yhteisön olisi suotavaa perehdyttää henkilöstöään tietoturva-asioihin, jotta tietoturva-aukkojen havainnoinnista ja valvonnasta muodostuisi koko organisaation henkilöstön kattava prosessi. Henkilöstön olisi hyvä olla valveutunut havainnoimaan omilla laitteillaan ja työpisteillään ilmeneviä epäkohtia, ja heidän tulisi myös viedä nämä havainnot tietohallinnon sekä tietosuojavastaavan tietoon. Organisaatio pystyy vahvistamaan omaa kybervalmiutensa tasoa, kun henkilöstöä koulutetaan valvomaan ja havaitsemaan mahdollisia väärinkäytöksiä tietoverkoissa. Samalla henkilöstö pystyy myös tarkastelemaan omia tietoturvaan liittyviä toimintatapojaan ja muuttamaan niitä vähemmän riskialttiiksi.

Kuten aineiston analyysissa todettiin, henkilöstöllä on oltava tarkat ohjeet siitä, mitkä toimintatavat ovat tietoturvan suhteen sallittuja, ja millaisia toimia ei ole suotavaa tehdä. Tällaista ohjeistusta on hyvä sisältyä tietoturvaperiaatteiseen ja -ohjeistuksiin. Näin ollen organisaatio voi ainakin osittain varmistua siitä, että epäedullisia toimia ei toteuteta. Tätä varmistumista edesauttaa entisestään, jos organisaatio velvoittaa koko henkilöstöään osallistumaan pakollisiin tietoturvakoulutuksiin. Tällaisten koulutusten avulla organisaation kybervalmiuden tasoa on mahdollista nostaa. Kyberturvallisuudesta huolehtiminen on loppujen lopuksi yhteistoimintaa, jossa jokaisen henkilöstön jäsenen myötävaikutuksella on merkitystä.

6. JOHTOPÄÄTÖKSET

Tämän tutkimuksen empiirinen tutkimuskohde oli Kokemäen kaupunki Satakunnan maakunnassa. Tutkielman tarkoitus oli tutkia sitä, millä tavoin Kokemäen kaupunki on parantanut kybervalmiutensa tasoa heinäkuussa 2019 toteutuneen kyberhyökkäyksen jälkeen. Tutkimuksessa selvitettiin myös sitä, millaisia konkreettisia toimia kaupunkiorganisaatiossa on otettu käyttöön kiitettävän kybervalmiuden tason ylläpidossa, sekä miten näitä asioita on huomioitu kaupungin vuodelle 2020 tekemässä budjetoinnissa. Tutkimuksen tarkoituksena oli siis selvittää, millaisia toimia suomalaisissa kuntaorganisaatioissa on mahdollista ja kannattavaa toteuttaa kybervalmiuden ja tietoturvan ylläpidossa.

Tutkimuksen keskeisimmiksi tuloksiksi muodostuivat kuntaorganisaation kybertoimia osittain rajoittavat talouden resurssit, virustorjunnan ja järjestelmien päivitysten tärkeys, koko organisaation kattavat tietoturvaohjeistukset sekä ehkä tärkeimpänä seikkana henkilöstön tietoisuuden ja kouluttamisen merkitys. Tutkimustulokset ovat linjassa tutkimukseen valitun analyysimenetelmän kanssa, joka oli laadultaan teorialähtöinen sisällönanalyysi. Tutkimustulokset ovat peilattavissa aiheesta jo tuotetun tieteen kanssa, sillä tutkimuksen kohteena olleen kaupunkiorganisaation mainitsemat kyberturvatoimet ovat samankaltaisia esimerkiksi Norris ym. (2015) ja Caruson, MacManus & McPhee (2012) löytämien havaintojen kanssa. Norris ym. (2015, 196) havaitsivat tutkimuksessaan hyvin samantapaisia kyberturvallisuuden vaatimia toimenpiteitä. Näitä ovat muun muassa tietoturva-aukkojen arviointi, haavoittuvuuden jatkuva tarkkailu ja testaus, loppukäyttäjien vahva todentaminen ja valtuutuksien kehittäminen heidän käyttäessään organisaation it-järjestelmiä, loppukäyttäjien kouluttaminen ja ohjaaminen sekä kyberhyökkäyksiä koskevan tiedon ja kyberturvallisuuden vaatimien toimintatapojen jakaminen organisaation sisällä. Norris ym. (2015, 196) myös havaitsivat, että kyberturvallisuuskulttuurin vahvistamisessa tärkeää on, että loppukäyttäjät, mutta yhtä lailla myös poliitikot ja virkamiehet ymmärtäisivät kiitettävän tason kyberturvan merkityksen, ovat koulutettuja ja motivoituneita kyberturva-asioihin ja että he ovat kyberturva-asioista tilivelvollisia. Tietojärjestelmien ja sovellusten kaksivaiheinen todentaminen nähtiin niin ikään hyvänä toimintatapana vahvistaa kybersuojaa organisaatiossa. Kokemäen kaupunki toteutti kaikkia näitä kybertoimia joko jo ennen kyberhyökkäystä, tai viimeistään hyökkäyksen seurauksena aloitettuina toimenpiteinä vahvistaakseen kybervalmiutta kuntaorganisaatiossa. Erityisesti tietoturvan jatkuva tarkkailu ja havainnointi sekä loppukäyttäjien kouluttaminen ja

ohjaaminen nousivat Kokemäen kaupungin tapauksessa erittäin kriittisiksi kybertoimiksi, joita ei voida laiminlyödä.

Tutkimustuloksilla saattaa olla merkitystä suomalaille kuntaorganisaatioille, jotka ponnistelevat oman tietoturvansa ylläpidon tai sen kehittämisen parissa. Kesällä 2019 tapahtuneet kyberhyökkäykset kolmessa suomalaisessa kaupungissa ovat mitä luultavimmin johdattaneet muutkin suomalaiset kunnat pohtimaan vakavammin kybervalmiutensa tasoa. Tutkimuksen esiin tuomilla toimilla kunnat voivat arvioida oman tietoturvansa tilannetta sekä sitä, olisiko siinä parantamisen varaa. Näillä toimilla on mahdollista pienentää kyberriskien realisoitumista. Näihin riskeihin lukeutuvat muun muassa Kokemäen kaupunkia kohdannut haittaohjelmahyökkäys. Tutkimuksen vaikutusta tieteen kannalta voidaan perustella sillä, että näiden tutkimustulosten pohjalta on mahdollista toteuttaa jatkotutkimusta, ja näin paikata kyberturvatoimiin Suomen kuntakentällä liittyvää tutkimusaukkoa. Mikäli kesän 2019 suomalaisella kuntasektorilla toteutuneet kyberhyökkäykset ovat näkymää tulevaisuudesta, on kuntien ensiarvoisen tärkeää tarkastella kybervalmiutensa tasoa jatkossa yhä tarkemmin. Maailmanlaajuinen digitalisaatio ei tule pysähtymään. Erilaiset tietoverkot ja järjestelmät yleistyvät kiihtyvällä tahdilla ja tietoa menee verkkoon jatkuvasti yhä suurempia määriä. Kunnat ovat alkaneet digitalisoimaan järjestelmiään ja palveluitaan yhä enenevissä määrin. Näin ollen myös kyberriskit kuntaorganisaatioiden keskuudessa kasvavat. Tämän tutkimuksen tulosten avulla käytännön toimijat kunnissa, mutta yhtä lailla myös yrityssektorilla pystyvät tarkastelemaan omia kyberturvatoimiaan sekä niiden mahdollisia puutteita.

Tutkimuksen validiteettia heikentää se, että tutkimuksessa kartoitettiin kyberturvan tason parantamista ja erilaisia kyberturvatoimia kuntaorganisaatiossa, mutta kuntaorganisaation virkamiehet eivät ole tietohallinnon asiantuntijoita. Näin ollen teemahaastattelun tuottama aineisto ei välttämättä anna tarkkoja vastauksia kyberturvan edellyttämistä toimista. Aineistonkeruutavaksi valittu teemahaastattelu antaa haastateltavalle tilaa tulkita kysymyksiä itse, joten vastaukset riippuvat haastateltavien tulkinnoista ja näkemyksistä. Aineisto ei ole myöskään välttämättä tarpeeksi riittävä, jotta siitä voitaisiin tehdä johtopäätöksiä kaupungin, saati koko suomalaisen kuntasektorin kybervalmiuden tasosta. Reliabiliteettia heikentää se, että toistettaessa tutkimus saattaisi tuoda esiin erilaisia päätelmiä, sillä teemahaastattelun keinoin tuotettu aineisto on vastaajasta riippuvainen. Myös eri tutkijan tekemä aineiston analyysi voisi tuottaa erilaisia päätelmiä.

Tulevaisuudessa aihetta voisi tutkia laajemmin, ja selvittää muun muassa sitä, millä tavoin ja toimin useammassa suomalaisessa kunnassa on toteutettu kyberturvatoimia. Laajemmalla otannalla

tutkimuksesta olisi mahdollista tehdä yleistettävämpi. Aiemmin tuotetussa tieteessä (esim. Caruson ym. 2012) on todettu, että kyberturvaan liittyvä tietokuilu IT-asiantuntijoiden ja hallinnon virkamiesten välillä on merkittävämpää paikallistason organisaatioissa kuin valtion tasolla. Kyseisen tutkimustuloksen pohjalta voisi olla mielenkiintoista jatkaa tutkimusta Suomen julkishallinnossa, sillä Kokemäen kaupungin tapauksessa oli havaittavissa merkkejä hallinnon virkamiesten asiantuntijuuden puutteesta kyberturva-asioissa. Jatkotutkimusta voisi tuottaa myös siitä, eroavatko kuntaorganisaatioiden ja yksityissektorin yritysten kyberturvatoimet toisistaan ja millä tavoin. Toisaalta voisi olla mielekästä selvittää, millä tavalla päätöksenteko julkisorganisaatioissa vaikuttaa kybervalmiuden ylläpitoon ja kyberturvasta huolehtimiseen, tai millä tavoin kyberturvan ylläpidolle on mahdollista ansaita legitimiteetti julkishallinnossa.

Tutkimusaiheesta Suomen kuntasektorilla ei ole tehty merkittävissä määrin tutkimusta aiemmin. Erilaisissa kyberturvatoimissa erityisesti Suomen kuntakentällä esiintyy siis jonkinlainen tutkimusaukko, jota myös tällä tutkimuksella pyrittiin paikkaamaan. Tulevaisuudessa tämän tutkimuksen voisi toteuttaa kattavammin valitsemalla tutkimusmenetelmäksi harkinnanvaraisen näytteen sijasta otannan, jossa esiintyy useampia kuntia. Näin ollen tutkimus olisi mahdollista yleistää kaikkiin suomalaisiin kuntiin.

7. LÄHTEET

Aitta, M., Herrala, A. (2019). Miten uusi tiedonhallintalaki vaikuttaa viranomaisiin? Deloitte Oy. Haettu 21.3.2020 osoitteesta https://www2.deloitte.com/content/dam/Deloitte/fi/Documents/risk/Miten%20uusi%20tiedonhallintalaki%20vaikuttaa%20viranomaisiin.pdf

Andreasson, A., Riikonen, J., Ylipartanen, A. (2017). Osaava tietosuojavastaava. Helsinki: Tietosanoma Oy.

Assante, M., Tobey, D. (2011). Enhancing the Cybersecurity Workforce. IT Professional 13/2011. Haettu 28.4.2020 osoitteesta https://ieeexplore-ieee-org.libproxy.tuni.fi/stamp/stamp.jsp?tp=&arnumber=5708280

Caruson, K., MacManus, S., McPhee, B. (2012). Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success. Haettu 20.2.2020 osoitteesta https://www.degruyter.com/downloadpdf/j/jhsem.2012.9.issue-2/jhsem-2012-0003/jhsem-2012-0003.pdf

Enberg, M. (2002). Kuntien riskienhallinta. Suomen kuntaliitto. Haettu 3.2.2020 osoitteesta https://docplayer.fi/17930468-Kuntien-riskienhallinta.html

Gueldry M., Gokcek G., Hebron L. (2019). Understanding New Security Threats. Lontoo: Taylor Francis Ltd.

Haasio, A. (2017). Verkkorikokset. Vantaa: BTJ Finland Oy.

Hirsjärvi, S., Hurme, H. (2011). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2015). Tutki ja kirjoita. Helsinki: Kustannusosakeyhtiö Tammi.

Huoltovarmuuskeskus. Tietoyhteiskunta-asiantuntijasivu. Haettu 25.3.2020 osoitteesta https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta/

Kaspersky Lab. Vinkkejä kyberrikoksilta suojautumiseen. Haettu 20.3.2020 osoitteesta https://www.kaspersky.fi/resource-center/threats/what-is-cybercrime

Keskuskauppalamari & Helsingin seudun kauppakamari. (2012). Yritysten rikosturvallisuus 2012: Riskit ja niiden hallinta. Haettu 30.3.2020 osoitteesta https://kauppakamari.fi/wp-content/uploads/2012/01/Yritysten_rikosturvallisuus_2012-.pdf

Kirves, J. (2019). Miten Väestörekisterikeskus auttaa kuntia digiturvallisuuden kehittämisessä? Kuntamarkkinoiden julkaisu. Yleiskirje 12/2019. Haettu 2.2.2020 osoitteesta https://kuntamarkkinat.fi/blogit/miten-vaestorekisterikeskus-auttaa-kuntia-digiturvallisuuden-kehittamisessa/

Kokemäen kaupunki. (2019). Talousarvio 2020. Taloussuunnitelma 2020-2023. https://kokemaki.fi/wp-content/uploads/2019/12/Talousarvio-2020_20.11-v2.3.pdf

Kuntalehti (2019). Lahti joutui kyberhyökkäyksen kohteeksi – tilanne päällä ja tutkinnassa. Yleiskirje 6/2019. Haettu 27.1.2020 osoitteesta https://kuntalehti.fi/uutiset/tekniikka/lahti-joutui-kyberhyokkayksen-kohteeksi-tilanne-paalla-ja-tutkinnassa/

Kuntalehti (2019). Lahti, Kokemäki, Pori – kyberiskut ovat jo täällä. Yleiskirje 8/2019. Haettu 2.2.2020 osoitteesta https://kuntalehti.fi/uutiset/lahti-kokemaki-pori-kyberiskut-ovat-jo-taalla/

Kuntaliitto (2019). Kyberhyökkäykseen liittyvistä uhkakuvista tiedottaminen. Yleiskirje 9/2019. Haettu 2.2.2020 osoitteesta https://www.kuntaliitto.fi/yleiskirjeet/2019/kyberhyokkaykseen-liittyvista-uhkakuvista-tiedottaminen

KvaliMOTV. Yhteiskuntatieteellinen tietoarkisto, menetelmäopetuksen tietovaranto. Aineisto- ja teorialähtöisyys. Haettu 29.3.2020 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L2_3_2_3.html

Laaksonen, M. (2015). Suomen kyberturvallisuus suuressa määrin kuntien vastuulla. Kuntamarkkinat yleiskirje 9/2015. Haettu 2.2.2020 osoitteesta https://kuntamarkkinat.fi/blogit/suomen-kyberturvallisuus-suuressa-maarin-kuntien-vastuulla/

Laki julkisen hallinnon tiedonhallinnasta (906/2019).

Lambrinoudakis C., Gritzalis S., Dridi F., Pernul G. (2003). Security requirements for e-government services: a methodological approach for developing a common PKI-based security-policy. Haettu 25.4.2020 osoitteesta https://www-sciencedirectcom.libproxy.tuni.fi/science/article/pii/S0140366403000823

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., Salminen M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Haettu 2.2.2020 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila%2c__tavoitetila_ja.pdf?sequence=1&isAllowed=yhttps://tietosuoja.fi/tietoturvaloukkaukset

Norppa K., Peltomäki J. (2015). Rikos meni verkkoon – Näkökulmia kyberrikollisuuteen ja verkkoturvallisuuteen. Helsinki: Talentum Media Oy.

Norris D., Joshi A., Finin T. (2015). Cybersecurity Challenges to American State and Local Governments. Haettu 18.2.2020 osoitteesta https://ebiquity.umbc.edu/_file_directory_/papers/844.pdf

Sarajärvi A., Tuomi J. (2018). Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Kustannusosakeyhtiö Tammi.

Sisäministeriö (2019). Kansallinen riskiarvio 2018. Sisäinen turvallisuus. Sisäministeriön julkaisuja 2019:5. Helsinki. Haettu 3.3.2020 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161332/5_2019_Kansallinen%20riskiarvio.pdf

Sisäministeriö. Kyberrikollisuus ylittää rajat tietoverkoissa. Asiantuntijasivu. Haettu 28.4.2020 osoitteesta https://intermin.fi/poliisiasiat/kyberrikollisuus

Sisäministeriö (2017). Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisuja 2017:14. Helsinki. Haettu 8.4.2020 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79866/Tietoverkkotorjuntaselvitys_VERKKO_.pdf

Tietosuojavaltuutetun toimisto. Tietoturvaloukkaukset. Haettu 29.4.2020 osoitteesta https://tietosuoja.fi/tietoturvaloukkaukset

Tuomi, T. (2019). Kokemäen kyberhyökkäys muistuttaa laajasta valuviasta – tuore väitöstutkimus paljastaa, että monet julkishallinnon it-järjestelmistä ovat jo käyttöönotettaessa vanhentuneita. Satakunnan Kansa 8/2019. Haettu 3.2.2020 osoitteesta https://www.satakunnankansa.fi/a/0f2e9614-259f-4d9e-88e9-d60d28ec55e7

Turvallisuuskomitea (2018). Kyberturvallisuuden sanasto. Helsinki: Sanastokeskus TSK ry. Haettu 26.1.2020 osoitteesta https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Wirtz B., Weyerer J. (2016). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes With Digital Threats. Haettu 25.4.2020 osoitteesta https://wwwtandfonlinecom.libproxy.tuni.fi/doi/full/10.1080/01900692.2016.1242614

Zhao J., Zhao S. (2010). Opportunities and threats: A security assessment of state e-government websites. Haettu 25.4.2020 osoitteesta https://www.sciencedirect.com/science/article/abs/pii/S0740624X09001099?via%3Dihub

8. LIITTEET

Liite 1. Haastattelurunko

Kesän 2019 kyberhyökkäys

1. Mitä kyberturvallisuus/kybervalmius sinulle tarkoittaa?
2. Voisitko kuvailla kesän 2019 kyberhyökkäystä, eli mitä siinä konkreettisesti tapahtui?
3. Mitkä syyt aiheuttivat hyökkäyksen?
4. Miten kunta olisi mahdollisesti voinut estää hyökkäyksen tai pienentää sen vaikutuksia?
5. Miten arvioisit sitä, kuinka hyvin kunta reagoi kyberhyökkäykseen?
6. Millaisia ongelmia hyökkäys aiheutti kuntaorganisaatiolle?
7. Entä toisaalta kuntalaisille?
8. Saiko kaupunki ulkopuolista apua kyberhyökkäyksen aiheuttamien ongelmien korjaamiseen?
9. Mistä ja millaista?
10. Osaatko arvioida,
11. kuinka merkittävästi kyberhyökkäys vaikutti kuntaorganisaation talouteen?

Kriisitilan hoitaminen

12. Miten kyberhyökkäyksestä mielestäsi toivuttiin?
13. Kävikö toipuminen joutuisasti vai näkyykö hyökkäys organisaatiossa edelleen?
14. Millaisia toimia organisaatiossa tehtiin, jotta niin sanottuun normaalitilaan päästiin takaisin?

Kyberturvatoimet

15. Millaisia konkreettisia kybervalmiuteen liittyviä toimintatapoja teillä oli organisaatiossanne ennen kesän 2019 kyberhyökkäystä?
16. Millaisia konkreettisia kyberturvallisuustoimia olette tehneet organisaatiossanne hyökkäyksen jälkeen? Miten kybervalmiuden tilaa on parannettu näin kesän hyökkäyksen jälkeen?
17. Millaisia erilaisia toimia kyberturvallisuudessa pitäisi mielestäsi tehdä, jotta kybervalmius olisi organisaatiossa kiitettävällä tasolla?
18. Millaisia ongelmia olette kohdanneet kyberturvallisuuden järjestämisessä?
19. Millaisia ongelmia kybervalmiuden yläpidossa voi mielestäsi yleisesti ottaen esiintyä?
20. Mitkä ovat eri kyberhyökkäysmuotojen vaatimia toimia? Vaativatko erilaiset hyökkäykset erilaisia toimia?

Toimintaedellytykset

21. Osoitettiinko tämän vuoden talousarviossa enemmän resursseja kyberturva-asioihin, viime kesän hyökkäyksestä oppineena?
22. Kuinka suuri rooli taloudella on mielestäsi kybervalmiuden ylläpidossa?
23. Onko kyberturva-asioita huomioitu kaupungin nykyisessä strategiassa merkittävämmin kuin ennen hyökkäystä?
24. Koetko olevasi ammattitaitosi puolesta kykenevä vastaamaan kyberturvallisuuden aiheuttamiin työnkuvan muutoksiin tai kyberturvasta huolehtimiseen?

25. Mikä oli henkilökohtainen tunneperäinen kokemuksesi, joka nousi esiin kyberhyökkäyksen tapahtuessa?