jamk.fi

Kyberhäiriöiden hallinnan prosessien ja toimintaohjeiden kehittäminen terveydenhuollon ympäristöissä

Elina Suni

Opinnäytetyö
Helmikuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Suni, Elina	Opinnäytetyö, AMK	Helmikuu 2021
	Sivumäärä 59	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: Kyllä

Työn nimi

Kyberhäiriöiden hallinnan prosessien ja toimintaohjeiden kehittäminen terveydenhuollon ympäristöissä

Tutkinto-ohjelma

Tieto- ja viestintätekniikan tutkinto-ohjelma, insinööri (AMK)

Työn ohjaaja(t)

Tero Kokkonen ja Karo Saharinen

Toimeksiantaja(t)

Jyväskylän ammattikorkeakoulun IT-instituutti/ JYVSECTEC

Tiivistelmä

Terveydenhuollon häiriöherkkyys tekee alasta erittäin kiinnostavan kohteen kyberrikollisuudelle. Maailmalla on uutisoitu lukuisista kyberhyökkäyksistä terveydenhuollon organisaatioihin koronakriisin aikana, ja myös Suomessa on tapahtunut vakavia kyberhäiriötilanteita.

Tarve kehittää kyberhäiriöiden hallinnan prosesseja ja toimintaohjeita on erittäin suuri ja aihe valitettavan ajankohtainen. Tavoitteena oli kehittää terveydenhuollon kyberhäiriöiden hallinnan prosesseja ja toimintaohjeita ja turvata yhteiskunnan kannalta kriittisen terveydenhuollon toimintaa. Toinen tavoite oli koronakriisin aiheuttamien haasteiden ratkaiseminen terveydenhuollon kyberturvallisuuteen liittyen, sillä vallitseva pandemia on synnyttänyt uudenlaisia kyberuhkia.

Laadullisessa tutkimuksessa hyödynnettiin konstruktiivista tutkimustapaa, jolla pyritään ratkaisemaan reaalimaailman ongelmia. Lopputuloksena syntyy konstruktio, joka poikkeaa kaikesta jo olemassa olevasta. Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille -teos syntyi konstruktiona kehittämisprosessista.

Vastaavan laajuista käsikirjaa, jonka sisältämät prosessit, ohjeet ja tarkistuslistat on esitetty helposti käytäntöön vietävässä muodossa ja jossa myös koronakriisin aikaiset uhat on huomioitu, ei ole Suomen terveydenhuollon kyberturvallisuuteen liittyen aikaisemmin toteutettu.

Avainsanat (asiasanat)

Kyberturvallisuus, terveydenhuolto, kyberhäiriöt, koronakriisi

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Suni, Elina	Bachelor's thesis	February 2021
		Language of publication: Finnish
	59	Permission for web publication: Yes

Title of publication

Developing Cyber Security Incident Response Processes for Healthcare Environments

Degree programme

Bachelor's Degree Programme in Information and Communications Technology

Supervisor(s)

Tero Kokkonen ja Karo Saharinen

Assigned by

JAMK University of Applied Sciences, Institute of Information Technology/ JYVSECTEC

Abstract

Vulnerability of the healthcare sector makes the industry a very interesting target for cybercrime. Numerous cyber-attacks on healthcare organizations have been reported around the world during the COVID-19 crisis, and serious cyber disruptions have also occurred in Finland.

The need to develop cyber security incident response processes and guidelines is great, and the subject is unfortunately very topical. The aim was to develop cyber security incident response processes and guidelines for healthcare to secure healthcare´s ongoing processes that are critical for the society. Another goal was to address the challenges posed by the COVID-19 crisis in terms of cyber security in healthcare, as the current pandemic has created new types of cyber threats.

The qualitative research utilized a constructive research approach aimed at solving real-world problems. The end result is a unique construction differing from anything that already exists in the field. A Handbook on Cyber Security Incident Response Processes for Healthcare Actors was created as a construction from the development process.

A handbook of a similar scope, including processes, instructions, and checklists which have been presented in an easily practical form, and which also takes into account the threats during COVID-19 crisis, has not been implemented before in the field of cyber security for the Finnish healthcare.

Keywords/tags (subjects)

Cyber security, healthcare, cyber incident, COVID-19 crisis

Miscellaneous (Confidential information)

Sisältö

Kuviot

Termit ja lyhenteet

CERT Computer Emergency Response Team

ENISA The European Union Agency for Cyber Security

Hakkeri tarkoittaa tietokonealan harrastajaa sekä tietojärjestelmiin murtautujaa (rikollinen hakkeri).

Häiriön käsittely (englanniksi incident response, IR) kuvaa organisaation prosessia käsitellä kyberhyökkäyksiä. Häiriön käsittelyä käytetään minimoimaan vaikuttavuutta organisaation liiketoimintaan, tutkimaan ja rajaamaan hyökkäystä, sekä palautumaan hyökkäyksestä. (Vertainen, Suni, Vatanen, Hautamäki, Laava & Piispanen 2021, 5.)

ICMT Information, Communication and Medical Technology

IEEE Institute of Electrical and Electronics Engineers

IEEE Xplore on digitaalinen kirjasto IEEE:n julkaisemille tieteellisille julkaisuille ja teknisille standardeille.

IoC Indicators of Compromise

IoT Internet of Things

IR Incident Responce

JAMK Jyväskylän ammattikorkeakoulu

JYVSECTEC - Jyväskylä Security Technology on Suomen johtava riippumaton kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus. JYVSECTEC toimii osana Jyväskylän ammattikorkeakoulun IT-instituuttia.

Kyberhäiriö/-poikkeama (englanniksi cyber incident) on yksi tai useampi toisiinsa liittyvä odottamaton tai ei-toivottu toteutunut kyberuhka. Kyberhäiriö/-poikkeama vaarantaa tietojen ja palvelujen tietoturvan ja vaikuttaa organisaation toimintaan epäsuotuisasti. (Vertainen ym. 2021, 5.)

Lokit ovat organisaation tietojärjestelmistä kerättäviä tapahtumatietoja. Lokeista nähdään esimerkiksi, milloin ja kuka on kirjautunut järjestelmään ja mitä tietoja on muutettu. Lokeja voidaan käyttää häiriötilanteiden selvittämisessä. (Vertainen ym. 2021, 39.)

NCSA National Communications Security Authority

NIST National Institute of Standards and Technology

NIST CSF NIST Cyber Security Framework

PHR-model Prepare, Hunt & Respond (JYVSECTEC)

SOC Security Operations Center

THL Terveyden ja hyvinvoinnin laitos

Tietojenkalastelu tarkoittaa sitä, että verkossa vaaniva rikollinen urkkii jonkun henkilön/ organisaation tärkeitä tietoja. Tavoitteena rikollisella on saada ihminen tekemään toimia, joiden avulla rikolliselle aukeaa pääsy luottamuksellisiin tietoihin, joita voivat olla, vaikka salasana- ja maksukorttitiedot. Tietojenkalastelua tapahtuu esimerkiksi sähköpostitse ja tekstiviesteillä. Usein viesteissä pyydetään klikkaamaan linkkiä. (CYBERDI Tietojenkalastelu n.d.)

Tor-verkko (pimeä verkko) tarjoaa käyttäjälleen korkean tason anonymiteetin. Tutkimukset osoittivat, että Tor-verkossa on laajasti laillisia sekä laittomia palveluita ja toimintoja. (Biswas, Fidalgo & Alegre 2017, 7.)

VAHTI (Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä) on julkisen hallinnon digitaalisen turvallisuuden kehittämisestä sekä keskeisten palveluiden tuottamisesta vastaavien organisaatioiden laajapohjainen yhteistyö-, valmistelu- ja koordinaatioelin. Toiminnasta vastaa Digi- ja väestötietovirasto. (Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI, n.d.)

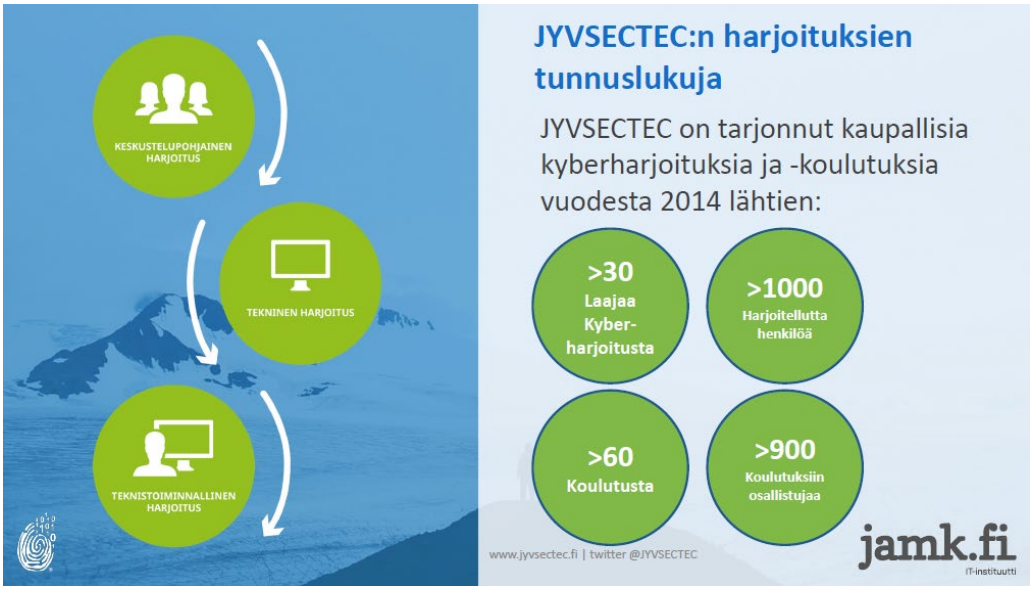
1 Johdanto

Maailmalla on uutisoitu lukuisista kyberhyökkäyksistä terveydenhuollon organisaatioihin koronakriisin aikana ja myös Suomessa on tapahtunut vakavia kyberhäiriötilanteita. Terveydenhuollon häiriöherkkyys tekee siitä yhden merkittävimmistä kyberhyökkäysten kohdealoista. Kyberrikollisuus terveydenhuoltoalaa kohtaan on lisääntynyt ja toimintaa haittaavia kyberhyökkäyksiä tapahtuu yhä useammin (Huoltovarmuuskeskus, 2020). Sekä Yhdysvalloissa että muissa maissa kiristysohjelmilla tehdyt tietomurtoiskut terveydenhuoltojärjestelmiin ovat lisääntyneet, varoittavat Yhdysvaltain viranomaiset. Samaan aikaan, kun koronaviruspandemia pahenee monissa maissa, pelätään tämän synnyttävän uusia vakavia uhkakuvia terveydenhuoltojärjestelmien näkökulmasta. Lokakuussa 2020 Yhdysvaltain viranomaisten julkaisemassa raportissa todetaan, että sairaaloihin ja julkiseen terveydenhuoltoon on kohdistunut kyberhyökkäysten aalto. Samalla painotetaan, että sairaaloiden tulisi pikaisesti päivittää tietoturvaansa. Sairaaloihin kohdistuvat kyberhyökkäykset ovat lisääntyneet myös Aasiassa, Euroopassa ja Lähi-idässä. (Huusko 2020.)

Tarve kehittää kyberhäiriön/-poikkeamanhallinnan prosesseja ja toimintaohjeita on erittäin suuri ja aihe valitettavan ajankohtainen. On erittäin tärkeää varautua kyberhäiriöihin, jotta niiltä voidaan mahdollisimman hyvin välttyä. Aiheen ajankohtaisuuden vuoksi työlle on erittäin kova tarve sekä kansallisesti että globaalissa mittakaavassa. Työ tuo aiheesta uutta tietoa, sillä vastaavan laajuisia tuotoksia, joissa prosessit ja toimintaohjeet ovat helposti käytäntöön vietävässä muodossa ja joissa myös koronakriisin aikaiset uhat on huomioitu, ei ole Suomen terveydenhuollon kyberturvallisuuteen liittyen aikaisemmin toteutettu.

Työn toimeksiantajana on Jyväskylän ammattikorkeakoulun IT-instituutin JYVSECTEC - Jyväskylä Security Technology, jossa kirjoittaja työskentelee. JYVSECTEC on Suomen johtava riippumaton kyberturvallisuuden tutkimus-, kehitys- ja koulutuskeskus. JYVSECTEC toimii osana Jyväskylän ammattikorkeakoulun (JAMK) IT-instituuttia käytössään monialainen asiantuntijaverkosto. JYVSECTECillä on toimintaa mm. seuraavilla asiantuntijuusalueilla: sovellettu kyberturvallisuus, tekoäly ja uudet teknologiat. Lisäksi JYVSECTEC on tunnettu teknistoiminnallisten

kyberturvallisuusharjoitusten järjestäjä, myös kansallisen tason harjoituksissa. JYVSECTECin järjestämistä kyberturvallisuusharjoituksista on tunnuslukuja kuviossa 1. (JYVSECTEC by Jamk About Us 2020.)



Kuvio 1. Tunnuslukuja JYVSECTECin kyberturvallisuusharjoituksiin liittyen (JYVSECTEC kyberharjoitus esitysdiat n.d.)

Työ liittyy projektiin nimeltään **Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä**. Projektin sekä tämän työn tavoitteena oli kehittää terveydenhuollon ympäristöihin liittyviä kyberpoikkeamienhallinnan prosesseja ja toimintaohjeita parantamaan ja varmistamaan yhteiskunnan kannalta kriittisen terveydenhuollon jatkuvuutta myös kyberhyökkäyksien tapahtuessa. Työssä keskitytään lisäksi koronakriisin aiheuttamien haasteiden ratkaisemiseen kyberturvallisuuteen liittyen, sillä vallitseva pandemia on synnyttänyt uudenlaisia uhkia ja lisännyt terveydenhuollon haavoittuvuutta. Tulokset ovat terveydenhuollon toimijoiden vapaasti hyödynnettävissä. (Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma 2020.)

Kirjoittaja toimi projektissa projektipäällikkönä. Projektipäällikkö koordinoi projektin toteutusta ja oli päävastuussa projektin hallinnollisista sekä sisällöllisistä asioista.

Projektipäällikkö myös tuotti sisältöjä projektin lopputuotokseen yhdessä projektitiimin kanssa. Projekti toteutettiin puolen vuoden aikana, ajanjaksolla 1.8.2020-31.1.2021. Tämä työ on rajattu tutkimaan terveydenhuollon kyberpoikkeamienhallinnan prosesseja ja toimintaohjeita Suomen tasolla. Samoin aihe on rajattu koskemaan terveydenhuoltoa, eli sosiaalihuolto ei kuulu tämän työn aihealueeseen. Nämä rajaukset tulevat projektisuunnitelmasta.

Projektin viralliset yhteistyökumppanit olivat

- Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus,
- Huoltovarmuuskeskus ja
- Terveyden ja hyvinvoinnin laitos (THL).

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tehtävä on kehittää ja valvoa viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Kyberturvallisuuskeskus tuottaa myös tietoturvallisuuden tilannekuvaa. Keskus tuottaa useita erilaisia tilannekuvatuotteita organisaatioiden ja kansalaisten käyttöön. Merkittävimmistä kyberuhkista kyberturvallisuuskeskus varoittaa ja tiedottaa myös kansalaisia, lisäksi tilannekuvatuotteet antavat kyberturvallisuuskeskuksen asiakkaille ajantasaista tietoa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä. (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Tilannekuva ja verkostojohtaminen 2021.) Keskuksella on lisäksi muun muassa CERT-toiminto, jonka tehtävänä on ennaltaehkäistä tietoturvaloukkauksia ja tiedottaa tietoturva-asioista. Kyberturvallisuuskeskuksen CERT-toiminnan tavoitteina on yleisten viestintäverkkojen sekä viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen sekä yhteiskunnan elintärkeiden toimintojen turvaaminen. (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Cert 2020.) NCSA-toiminto, eli toimiminen määrättynä turvallisuusviranomaisena ja kansallisena tietoturvaviranomaisena kuuluu myös Kyberturvallisuuskeskukselle. NCSA-toiminnon puitteissa he vastaavat turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista. Kyberturvallisuuskeskuksen NCSA-toiminnon palvelut tukevat organisaatioiden ennaltaehkäisevää turvallisuustyötä sekä toimintamahdollisuuksia. (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus NCSA 2021.)

Huoltovarmuuskeskus on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on Suomen huoltovarmuuden ylläpitäminen. Lisäksi sen tehtäviin kuuluu huoltovarmuuden kehittämiseen liittyvä suunnittelu sekä operatiivinen toiminta. Elinkeinoelämän ja julkishallinnon yhteistyö huoltovarmuuden varmistamisessa on tärkeää. Huoltovarmuuskeskus tukee yhteistyötä muun muassa kehittämällä yrityksille jatkuvuudenhallinnan työkaluja ja kouluttamalla yrityksiä niiden käytössä. Lisäksi Huoltovarmuuskeskus toteuttaa viranomaisten ja yritysten yhteisiä harjoituksia. (Huoltovarmuuskeskus 2021.) Lisäksi huoltovarmuuskeskus tukee ja ohjaa sektorien ja poolien toimintaa. Elinkeinoelämän johdolla toimivina toimieliminä poolit vastaavat operatiivisesta varautumisesta. Poolien tehtävä on muun muassa kehittää omien alojensa huoltovarmuutta. Työtä tehdään yhdessä alan yritysten kanssa. Alan yritykset osallistuvat myös poolin järjestämään koulutukseen ja kehittämistyöhön. Näiden lisäksi ne noudattavat poolien antamia ohjeita varautumiseen liittyen. (Huoltovarmuuskeskus Sektorit ja poolit 2021.) Terveydenhuolto on yksi ala, jonka huoltovarmuutta koordinoi Huoltovarmuuskeskuksen perustuotanto-osasto, Terveydenhuoltosektori sekä sektorin alaiset Terveydenhuoltopooli, Vesihuoltopooli ja Jätealan toimikunta (Huoltovarmuuskeskus Terveydenhuolto 2021).

Terveyden ja hyvinvoinnin laitos on vastuussa Suomen kansallisesta tiedonhallinnan ohjauksesta, jonka tavoite on varmistaa sote-tietojen saatavuus, löydettävyys ja hyödynnettävyys. THL ohjaa sote-tiedonhallintaa tietoarkkitehtuurin, toiminnallisen suunnittelun, määräysten, ohjeiden ja määrittelyjen avulla. THL:n rooliin sote-tiedonhallinnan ohjauksessa kuuluu myös kansainvälinen yhteistyö muun muassa rajat ylittävän tiedonvaihdon ja standardien kehittämisessä. THL käyttää ohjausprosessissa toiminnallisia määrittelyjä ja tietosisältöjä sekä vaatimuksia sosiaali- ja terveydenhuollon organisaatioiden käytössä oleville tietojärjestelmille. Sote-palveluissa käytössä olevien tietojärjestelmien on täytettävä kansallisesti määritellyt olennaiset vaatimukset. Kanta-palveluihin liittyvien järjestelmien sertifioinnin ohjaus on myös THL:n vastuulla. (Tiedonhallinta sosiaali- ja terveysalalla 2020.)

Yhteistyötä tehtiin myös kahden muun alan hankkeen kanssa. Jyväskylän ammattikorkeakoulun Healthcare Cyber Range -hankeen, jossa tavoitteena on varmistaa potilaiden turvallisuuden ja hoidon jatkuvuus digitaalisessa terveydenhuollossa. Tavoite

saavutetaan rakentamalla terveydenhuollon digitaalinen harjoitusympäristö sekä kehitetään terveydenhuollon toimijoiden kyberturvallisuustoimintaa. Tämän mahdollistaa se, että JYVSECTECin harjoitusympäristö RGCE (Realistic Global Cyber Range) laajentuu terveydenhuollon järjestelmillä ja prosesseilla (Healthcare Cyber Range (HCCR) 2020). Toinen yhteistyöhanke oli Kyber-Terveys-hanke, jossa muun muassa jaetaan koulutussisältöjä sekä alan parhaita käytäntöjä, kehitetään aktiivista havainnointikykyä sekä edistetään tietoturvallisten ohjelmistojen ja palvelujen hankintaa (Kyberturvallisuuden tähden 2018).

Yllä mainittujen toimijoiden lisäksi projektissa tehtiin yhteistyötä Telian kanssa. Telialla on liiketoimintaa terveydenhuollon alalla. Esimerkkinä heidän tietoturvavalvomonsa (SOC), joka valvoo 2M-IT:n tietoturvaa. 2M-it on Suomen suurin sosiaali- ja terveydenhuollon tietoteknisiä palveluita tuottava julkisomisteinen yhtiö (Tietoturva tuottaa ratkaisuja hyvinvointiin 2020).

Terveydenhuollon alalta tehtiin yhteistyötä lisäksi Keski-Suomen sairaanhoitopiirin ja Pirkanmaan sairaanhoitopiirin kanssa. JAMKin hyvinvointiyksikön kanssa tehtiin myös yhteistyötä viestinnän osalta. Hyvinvointiyksikkö järjestää muun muassa sosiaali- ja terveysalan AMK- ja YAMK-koulutuksia, kuten esimerkiksi sairaanhoitajakoulutusta, toteuttaa alan liiketoimintaa, koulutusvientiä sekä TKI-toimintaa.

2 Tutkimusmetodologia

Tutkimusmetodologia luvussa esitellään päätutkimuskysymys sekä alakysymys. Lisäksi luvussa esitellään tutkimuksen metodologiset valinnat sekä tutkimuksen konteksti. Luku sisältää myös tietoa tutkimukseen liittyvistä eettisistä periaatteista.

2.1 Tutkimuskysymys

Tutkimuksen aiheen päättämisen jälkeen seuraava vaihe on muotoilla tutkimusongelma. Jokaisella tutkimuksella tulee olla tutkimusongelma, johon vastataan tutkimusmetodologialla ja materiaaleilla. Tutkimusongelman muuttaminen tutkimuskysymykseksi helpottaa prosessia, koska on helpompi vastata kysymykseen kuin ongelmaan. Sekä tutkimusongelma että tutkimuskysymys ohjaavat tutkijaa ja tutkimuksen etenemistä. Tutkimusongelma ratkaistaan lopulta oikeilla kysymyksillä, joita voi olla yksi tai useampi. (Kananen 2015, 46–48.)

Laadullisen tutkimuksen tutkimuskysymykset ovat usein tutkivia ja kuvaavia. Ne kuvaavat sosiaalista ilmiötä ja niiden merkityksiä asiaankuuluville toimijoille (mitä kysymyksiä) ja selittävät ja ymmärtävät sosiaalisia malleja ja prosesseja (miten kysymykset). On tärkeää huomata, että kvalitatiivisessa tutkimuksessa erotetaan toisistaan **mitä** ja **miten** kysymykset. Mitä kysymykset keskittyvät siihen, mitä tapahtuu, mitä ihmiset tekevät ja mitä se merkitsee heille. Painopiste on olemassa olevissa, yksilöistä ja sosiaalisista olosuhteista syntyvissä ja niistä johtuvissa merkityksissä. Tavoitteena on kuvata todellisuutta siten, mitä se luonnollisesti on. Miten kysymykset puolestaan keskittyvät siihen, miten merkitys tuotetaan. Tutkimuksessa keskitytään jokapäiväisiin käytäntöihin, joiden avulla jokapäiväisen elämän merkitykselliset realiteetit muodostuvat ja niitä ylläpidetään. (Hesse-Biber & Leavy 2011, 39–40.) Tämän tutkimuksen päätutkimuskysymys on miten kysymys, sillä kysymyksessä keskitytään siihen, miten merkitys tuotetaan. Alakysymys taas on mitä kysymys, sillä kysymys keskittyy siihen mitä vallitsevassa pandemiatilanteessa tapahtuu.

Opinnäytetyössä vastataan seuraavaan päätutkimuskysymykseen:

> Miten terveydenhuollon organisaatioissa tulee varautua kyberhäiriöihin sekä reagoida ja palautua niistä?

Päätutkimuskysymystä täsmennetään seuraavalla alatutkimuskysymyksellä:

Mitä uudentyyppisiä kyberuhkia koronakriisi on aiheuttanut terveydenhuoltoalalle?

2.2 Tutkimusmenetelmä

Tämän tutkimuksen päätavoitteena on auttaa terveydenhuollon organisaatioita kehittämään kyberhäiriöiden hallinnan prosessejaan ja toimintaohjeitaan huomioiden koronakriisin aiheuttamat haasteet kyberturvallisuuteen liittyen. Kananen (2017) sanoo, että kvalitatiivisessa tutkimuksessa ei pyritä tekemään kvantitatiivisen tutkimuksen kaltaista yleistyksiä, joiden takana on aina teorioita ja malleja. Laadullisessa tutkimuksessa pääpaino on ilmiössä, ja iso kysymys on, mistä siinä on kyse. (32.) Tässä tutkimuksessa käsitellään ilmiönä terveydenhuollon kyberturvallisuutta, pyritään ymmärtämään mistä siinä on kyse ja kehittämään toimintamalleja terveydenhuollon kyberturvallisuuden vaalimiseen.

Konstruktiivinen tutkimustapa on saanut paljon positiivista huomiota tekniikan ja liiketalouden tutkijoilta. Konstruktiivinen tutkimusote tuottaa innovatiivisia konstruktioita. Tuotetuilla konstruktioilla yritetään ratkaista reaalimaailman ongelmia. Näin tuotetaan kontribuutioita tieteenalalle, jossa tutkimustapaa sovelletaan. Tutkimusotteen ydinkäsite on (uusi) konstruktio. Tämä käsite on abstrakti ja sillä on loputtomasti mahdollisia toteutumia. Esimerkiksi kaikki ihmisen luomat suunnitelmat, mallit, diagrammit, kaupalliset tuotteet, organisaatiorakenteet ja tietojärjestelmämallit ovat konstruktioita. Näille on tunnusomaista se, että ne keksitään ja kehitetään eli niitä ei ole löydetty. Kehittämällä konstruktio, jollaista ei aikaisemmin ole ollut olemassa, luodaan täysin uutta todellisuutta. (Lukka n.d.)

Konstruktiivisessa tutkimusotteessa

- Keskitytään tosielämän ongelmiin, jotka halutaan saada ratkaistua.
- Tuotetaan innovatiivinen konstruktio, jolla ratkaistaan alkuperäinen tosielämän ongelma.
- Tutkija ja käytännön edustajat tekevät erittäin läheistä yhteistyötä tiimimäisesti, joka voi mahdollistaa kokemuksellisen oppimisen.

- Edellytetään, että tutkimus on kytketty huolellisesti olemassa olevaan teoreettiseen tietämykseen.
- Kiinnitetään huomiota empiiristen löydösten heijastamiseen takaisin teoriaan. (Lukka n.d.)

Yllä mainittujen seikkojen perusteella konstruktiivinen tutkimusote sopii hyvin tämän laadullisen tutkimuksen kehittämisprosessin tutkimusotteeksi. Lisäksi konstruktiivisen tutkimuksen kautta syntyneeseen ratkaisuun kuuluu aina normatiivinen piirre, sillä ongelmaan yritetään löytää hyvä ratkaisu, jota voidaan suositella. Ratkaisulla saavutetaan joitain etuja verrattuna aikaisempaan tilanteeseen. Tässä tutkimuksessa tavoite oli juuri kehittää nykyisiä terveydenhuollon kyberpoikkeamien hallinnan ohjeita ja prosesseja paremmiksi kuin mitä ne olivat. Konstruktio perustuu aina olemassa olevaan tietoon, teoriaan. Teoriaa käytetään havaintojen jäsentämiseen. Lisäksi tarvitaan keskustelua aiheen parissa työskentelevien henkilöiden kanssa. Näiden vaiheiden jälkeen kehitetään uutta. Työn valmistuttua siitä keskustellaan aiheen parissa työskentelevien kanssa ja tutkija tarkastelee ratkaisun hyödynnettävyyttä laajemmin. (Virtanen 2006, 51.)

Konstruktiivisessa tutkimusotteessa, kuten missä tahansa tutkimusmenetelmässä tai -otteessa on syytä tarkastella sen mahdollisia puutteita. Konstruktiivisen tutkimusotteen tunnettu heikkous on objektiivisuuden puute, kun tutkija on itse tekemässä uutta konstruktiota omaan ongelmaansa. Tässä työssä tämä haaste on otettu siten huomioon, että työn tuloksena syntyvän tuotoksen sisältöihin on pyydetty aihe-ehdotuksia ja palautetta yhteistyöverkostolta, joka koostuu useista tutkimusryhmän ulkopuolisista organisaatioista. Yhteistyöverkosto on siis ollut mukana ideoimassa tuotosta, vaikuttamassa konstruktioon.

2.3 Tutkimusetiikka

Tutkimuksessa on huomioitu hyvä tieteellinen käytäntö. Tähän kyseiseen tutkimukseen liittyen keskeisinä huomioina on nostettu esiin seuraavat asiat:

- Tutkimuksessa noudatettiin rehellisyyttä, tarkkuutta ja huolellisuutta kaikissa sen vaiheissa.

- Tutkimukseen käytettiin tieteellisen tutkimuksen kriteerien mukaisia ja eettisesti kestäviä tutkimus- tiedonhankinta-, ja arviointimenetelmiä sekä toteutettiin avointa ja vastuullista viestintää tutkimuksen tuloksista.
- Muiden tutkijoiden työt otettiin huomioon asiaankuuluvalla tavalla kunnioittaen niitä ja heidän julkaisuihinsa viitattiin oikeaoppisesti sekä annettiin saavutuksille niille kuuluva merkitys.
- Tutkimus suunniteltiin sekä toteutus ja raportointi tehtiin tieteelliselle tiedolle asetettujen vaatimusten mukaisesti. Tietoaineistot tallennettiin myös tieteellisen tiedon vaatimusten mukaisesti. (Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2012.)

Yllä listattujen lisäksi tutkimustyön tekemisessä käytettiin lisensoituja ohjelmistoja. Tutkimusetiikan kannalta on myös syytä pohtia voisiko tätä tutkimusta käyttää hyödyksi rikollisessa toiminnassa. Tämän työn tuloksena syntynyt projektin tuotos voisi herättää rikollisten hakkereiden huomion, mikäli terveydenhuolto olisi kyseessä olevien rikollisten toiminnan kohteena. Rikollinen voisi saada tuotoksen kautta informaatiota organisaatioiden varautumismalleista kyberhyökkäyksiin. Tämä huomioidaan tuotoksessa siten, ettei se sisällä liian tarkkoja kuvauksia tai teknisiä ratkaisumalleja esimerkiksi kyberhäiriöihin varautumisen osalta. Jokainen organisaatio itse rakentaa varsinaiset toteutukset tuotoksen sisältämien suositusten ja prosessissa huomioitavien asioiden pohjalta.

3 Kirjallisuuskatsaus

Kirjallisuuskatsauksessa kuvataan erilaisia käsitteitä, joilla on tutkimuskysymyksen näkökulmasta merkitystä. Lähteet on valittu systemaattisesti huomioiden ilmiön kannalta mahdollisimman tuore ja aiheen kannalta olennainen aineisto. Suurin osa lähteistä on kansainvälisiä. Tärkeimmät tietolähteet kirjallisuuskatsauksessa ovat kansainväliset akateemiset artikkelit, jotka ovat pääosin peräisin IEEE Xplore:n digitaalisesta kirjastosta ja Google Scholar verkkosivustolta. Hakusanoina artikkeleita etsiessä käytettiin muun muassa seuraavia: cyber security in healthcare, cyber security risks

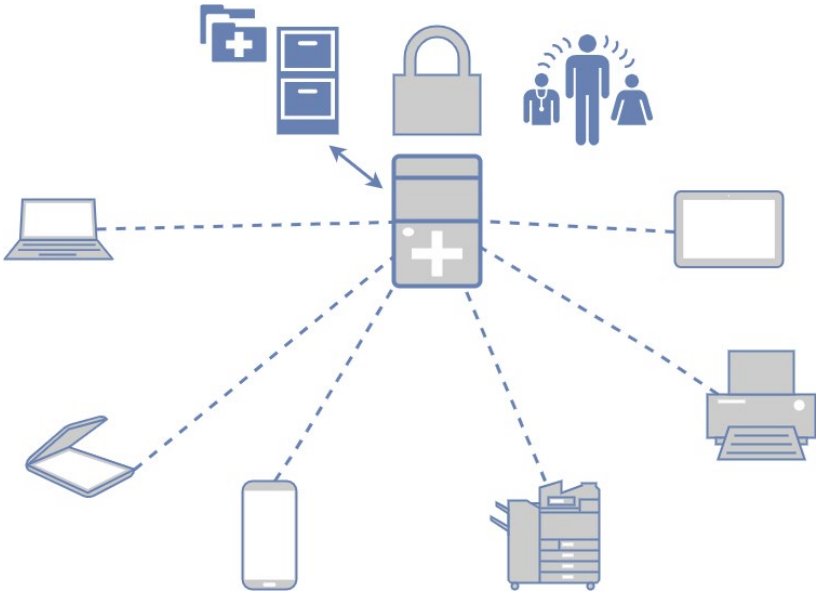
in healthcare, cyber security in hospitals, human errors in cyber security ja cyber security risks in a pandemic. Myös julkaistuja kirjoja hyödynnettiin. Lisäksi joitain yritysten verkkosivustoja ja yritysraportteja tarkasteltiin. Kirjallisuuskatsauksen pääteemoiksi on valittu **terveydenhuolto kyberrikosten kohteena** ja **kyberturvallisuus terveydenhuollossa.**

3.1 Terveydenhuolto kyberrikosten kohteena

Terveydenhuolto kuuluu aloihin, joihin kohdistuu eniten kyberhyökkäyksiä maailman laajuisesti (Argaw, Troncoso-Pastoriza, Lacey, Florin, Calcavecchia, Anderson, Burleson, Vogel, O'Leary, Eshaya-Chauvin & Flahault 2020). Lunnasohjelmien ja muiden kyberhyökkäysten uhka on kasvava monille arkaluonteisia tietoja käsitteleville aloille, mutta terveydenhuoltoala on erityisen kiinnostava kohde rikollisille, koska sairaalat, klinikat, terveysasemat ja muut terveydenhuollon organisaatiot käsittelevät arkaluontoisia potilastietoja. Vähäiset investoinnit terveydenhuoltosektorin kyberturvallisuuteen ja organisaatioiden IT-osastoihin ovat herättäneet pahantahtoisten toimijoiden huomion. Nämä pyrkivät varastamaan ja myymään pimeillä markkinoilla erittäin tuottoisia terveystietoja. Potilastiedot voivat sisältää paljon henkilökohtaista informaatiota kuten henkilön nimen, sosiaaliturvatunnuksen, kotiosoitteen, vakuutustiedot, maksu- ja luottokorttitiedot, ajokortin sekä terveystietohistorian. Varastetut tiedostot, jotka sisältävät terveystietoja, voivat olla erittäin arvokkaita Tor-verkossa. (Swasey 2020, 2.) Terveydenhuoltoala nähdään helppona kohteena, jonka kautta päästään käsiksi suureen määrään arvokasta tietoa (Martin, Martin, Hankin, Darzi & Kinross 2017, 1).

Toinen uhkia lisäävä tekijä on terveydenhuollossa hyödynnettävien teknologioiden kehittyminen. Teknologiaympäristö on jatkuvasti muuttuva. Uusia teknologioita toteutetaan nopeammin kuin turvatoimenpiteet saadaan luotua tai päivitettyä laitteiden suojaamiseksi. Lääkinnälliset laitteet, jotka ovat perinteisesti olleet erillisiä järjestelmiä, ovat integroitumassa sairaalan verkkoon ja muihin järjestelmiin, eivätkä ne täten ole enää immuuneja perinteisille kyberhyökkäyksille. Lääkinnällisten laitteiden valmistajat toteuttavat ja laajentavat verkottuneita lääkinnällisiä laitteita, mutta eivät pysy mukana verkon integraation aiheuttamien mahdollisten tietoturvauhkien

kiertämisessä. Monet tietotekniikan asiantuntijat ovat huolissaan siitä, että viimeaikaisten trendien perusteella verkkorikolliset tulevat kohdentamaan hyökkäyksiä lääkinnällisiin laitteisiin, kuten sydämentahdistimiin tai tehohoitoyksikön hengityskoneisiin. (Kruse, Frederick, Jacobson & Monticone 2017, 4.) Kuviossa 2 havainnollistetaan muuttunutta terveydenhuollon toimintaympäristöä, jossa yhä useampi työväline ja laite on kytketty sairaalan verkkoon.



Kuvio 2. Muuttunut terveydenhuollon toimintaympäristö

Lääkinnällisten laitteiden valmistajien etäyhteydet lääkintälaitteisiin saattavat myös aiheuttaa haavoittuvuutta. Valmistajat voivat valvoa sekä säätää etäyhteyden avulla esimerkiksi sädehoitolaitteistoja. Tämä toimenpide voi parantaa laitteiden vikojen ennakoimista sekä nopeuttaa vikojen korjaamista. Toisaalta käytäntö voi vaatia terveydenhuollon yksiköitä avaamaan yhteydet heidän sisäverkkonsa ja internetin välille. Tämän turvallinen toteuttaminen vaatii, että etäyhteyksien tekniikasta on riittävän tarkat tiedot. Turvallinen toteuttaminen vaatii lisäksi huolellista valvontaa ja toteutusta. Haasteita syntyy myös, mikäli laitevalmistajat eivät joko pysty tai halua kertoa etäyhteyksistään yksityiskohtia. Useimmiten lääkinnälliset laitteet sisältävät ohjelmistoja. Ohjelmistoista paljastuu usein vikoja ja täten niissä voi ilmetä haavoittuvuuksia. Haavoittuvuuksien hyväksikäyttö saattaa estää lääkintälaitteiden oikeaoppi-

sen käyttämisen. Valmistajan vastuulla on ohjelmistojen päivitys ja muut lääkinnällisten laitteiden korjaavat toimenpiteet. Lääkinnällisen laitteen ohjelmistoa korjatessa valmistajan täytyy varmistaa sen vaatimukset uudestaan. Tämän takia tunnettujen haavoittuvuuksien korjaamisessa voi olla hitautta. (Vuorinen 2019, 19.)

Alat kuten finanssiala ovat pohtineet kyberturvallisuuskysymyksiä jo vuosikymmenien ajan sekä laatineet tiukkoja turvallisuuspolitiikoita ja investoineet kyberturvallisuuteen. Terveydenhuollolla taas on haasteita antaa riittävästi huomiota ja resursseja ongelmaan, joka on alalle suhteellisen uusi. Lisäksi terveydenhuollon varojen ollessa rajalliset niitä ei välttämättä kohdisteta riittävästi tietoturvallisuustyöhön. (Argaw ym. 2020.)

Esimerkkejä terveydenhuoltoon kohdistuneista kyberhyökkäyksistä

Vuonna 2015 kyberrikolliset varastivat 80 miljoonan ihmisen terveystiedot eräästä amerikkalaisesta sairausvakuutusyhtiöstä. Huomioiden, että yksittäisten henkilöiden terveystiedoilla käydään kauppaa pimeillä markkinoilla noin 50 dollarin kappalehintaan, tämän rikkomuksen markkina-arvo oli laskennallisesti yli miljardi dollaria. Terveystiedot ovat pimeillä markkinoilla arvokkaampia kuin luottokorttitiedot, koska ne sisältävät useita pysyviä tunnisteita ja taloudellisia tietoja. Toisin kuin luottokorteissa, näitä tunnuksia ei voi vaihtaa. Lisäksi henkilön tietueet saattavat sisältää tarpeeksi tietoa pankkitilien avaamiseen sekä lainan tai passin hankkimiseen. (Martin, Martin, Hankin, Darzi & Kinross 2017, 1.)

Toukokuussa 2017 tapahtui maailmanlaajuinen WannaCry-Ransomware-hyökkäys ja sen arvioidaan vaikuttaneen noin 200 000 järjestelmään yli 150 maassa. Hyökkäys vaikutti suoraan noin 50 sairaalaan Iso-Britanniassa, ja monet muut sairaalat sulkivat ennaltaehkäisevästi tietojärjestelmiään, mistä aiheutui huomattavia häiriöitä. Vaikutukset ulottuivat hoidon järjestämiseen, vaaransivat potilasturvallisuuden ja mahdollisesti heikensivät luottamusta. Hyökkäyksessä käytettiin Ransomware-ohjelmistoa eli kiristyshaittaohjelmaa, joka salaa uhrin tiedot, estää pääsyn niihin ja uhkaa julkaista tai poistaa niitä, ellei lunnaita makseta. Myös Turun yliopistollisesta keskussai-

raalasta löytyi vuonna 2017 WannaCry-haittaohjelma. Virus löytyi kuvantamiseen liittyvistä koneista. Koneet oli kytketty samaan verkkoon noin 7 000 perustyöaseman kanssa. Vahinkoa ohjelma ei onneksi Turussa päässyt aiheuttamaan. (Keränen 2017.)

Vuonna 2020 Suomessa tapahtui poikkeuksellisen laaja ja törkeä tietomurto. Toistaiseksi tuntematon rikollinen hakkeri murtautui psykoterapiakeskuksen potilastietojärjestelmään arviolta jo vuonna 2018, vaikka tietomurto selvisi yritykselle vasta syksyllä 2020. Poliisin antamien tietojen perusteella tapaukseen liittyen on tehty noin 25 000 rikosilmoitusta. (Hämäläinen & Kallunki 2020.) Tietomurrossa vietiin kymmenien tuhansien asiakkaiden henkilötietoja ja potilaskertomuksia. Tietojärjestelmiä ei otettu haltuun hyökkääjän toimesta, mutta varastetuilla asiakastiedoilla yritettiin kiristää ensin murron kohteeksi joutuneelta organisaatiolta noin puolen miljoonan euron arvosta lunnaita ja sen jälkeen kiristykset kohdistettiin suoraan asiakkaisiin. Ainakin 300 ihmisen tiedot julkaistiinkin Tor-verkossa. Tapausta pidetään Suomen tähänastisen rikoshistorian pahimpana tietomurtona. (Hämäläinen & Rummukainen 2020.)

Koronakriisin aiheuttamat kyberuhat terveydenhuollossa

Williams, Chaturvedi ja Chakravarthy korostavat artikkelissaan Cyber Security Risks in a Pandemic (2020), että terveydenhuollon organisaatioista tulee ensisijaisia kohteita kyberrikollisille terveyskriisien (kuten pandemioiden) aikana. Etävastaanottojen valtava kasvu uusien teknisten alustojen avulla on avannut uusia kyberhyökkäysmahdollisuuksia rikollisille. (Williams ym. 2020.)

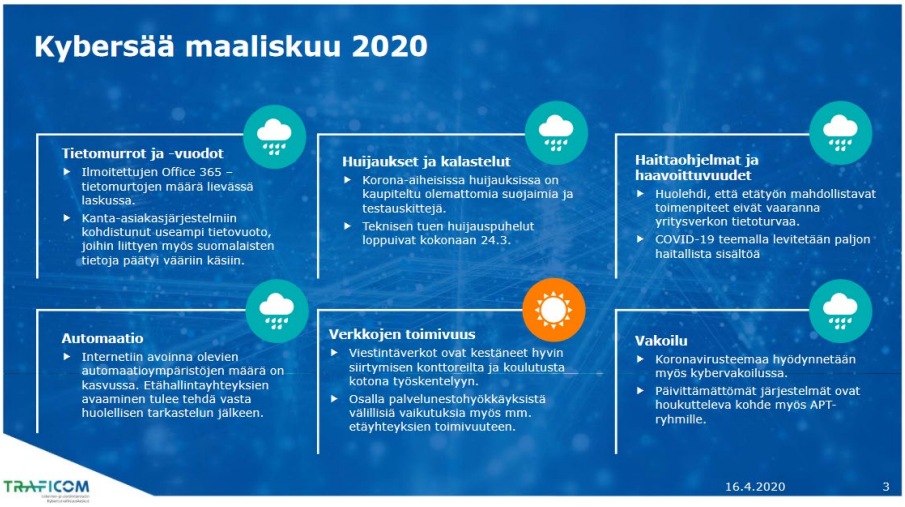
Kiireen ja sen välillä, että terveydenhuollon työntekijä avaa tietojenkalastelusähköpostin, on myös tunnistettu yhteys. Tämä on erityisen ongelmallista, sillä pandemioiden aikana työmäärät voivat olla kaikkien aikojen korkeimmat. (Williams ym. 2020.) Kiireessä ihminen tekee myös helpommin virheitä. Tutkimuksissa on osoitettu, että puolessa organisaatioihin kohdistuneista kyberhyökkäyksistä on taustalla inhimillisiä virheitä. Yhdysvaltain vuoden 2014 kyberrikollisuutta koskevasta tutkimuksessa havaittiin lisäksi, että terveydenhuollossa yksityisten tai arkaluontoisten tietojen tahattomasta paljastamisesta ilmoittaneiden määrä oli 83 % suurempi kuin vastaajien yleensä. Tämä nähtiin kriittisenä asiana erittäin säännellylle terveydenhuollon alalle,

joka käsittelee arkaluonteisia henkilökohtaisia tietoja. (Evans, Maglaras, He & Janicke 2016, 4670–4677.)

Ongelmia aiheuttavat myös ympäri maailmaa lisääntyneet Ransomware-kiristyshaittaohjelmat. Esimerkkinä tästä on verkkorikollisuusryhmä "Netwalker", joka hyökkäsi ainakin kahteen terveydenhuollon organisaatioon Yhdysvalloissa ja organisaatiot päättivät maksaa lunnaat saadakseen ohjelmistonsa takaisin käyttöönsä. Organisaatiot kärsivät silti isoista tulonmenetyksistä, kun ohjelmistot olivat lukittuina. Lisäksi organisaatiot kärsivät muun muassa mainehaitoista. (Williams ym. 2020.)

Yksi uusi kyberrikollisille auennut hyökkäysmahdollisuus liittyy koronakriisin aikana kotona työskentelevien terveydenhuollon työntekijöiden määrän lisääntymiseen. Yrittäessään siirtää työntekijät kotiin työskentelemään mahdollisimman nopeasti, monet työnantajat eivät osanneet ottaa huomioon kaikkia mahdollisia turvallisuusuhkia, joita uudet työtavat mahdollistavat. Kotona yhteydet tai käytössä olevat tietokoneet eivät välttämättä ole niin turvallisia kuin työpaikalla. (Williams ym. 2020.)

Koronakriisin varjolla tehtyjä huijausviestejä on myös ollut paljon liikkeellä. Kyberturvallisuuskeskuksen julkaisemassa maaliskuun 2020 kybersäässä (ks. kuvio 3) mainitaan muun muassa, että korona-aiheisissa huijauksissa on kaupiteltu esimerkiksi olemattomia suojaimia ja testauskittejä. Lisäksi mainitaan, että koronavirusteemaa on hyödynnetty kybervakoilussa. (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Kybersää Maaliskuu 2020 2020, 3.)



Kuvio 3. Ote Kybersää maaliskuu 2020 -julkaisusta (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Kybersää Maaliskuu 2020 2020, 3)

Lisäksi syyskuun 2020 kybersäässä mainittiin, että maailmalla on paljon havaintoja terveysalan toimijoihin kohdistuneista kiristyshaittaohjelmista. Esimerkkitapauksena mainittiin syyskuussa 2020 Universal Health Services sairaalaketjuun kohdistunut kiristyshaittaohjelmahyökkäys. Haittaohjelman raportoitiin käynnistyneen viikonlopun aikana ja sen vaikutukset kestivät noin viikon ajan. Tuona aikana hoitolaitokset toimivat ilman sisäisiä IT-järjestelmiään. Lisäksi raportoitiin, että joitain potilaita jouduttiin käännyttämään pois tai ohjaamaan toisiin sairaaloihin. Universal Health Services on varmistanut, että kiristyshaittaohjelmalla oli vaikutuksia kaikkiin heidän hoitolaitoksiinsa Yhdysvalloissa. Sairaalaketjulla on yhteensä 400 hoitolaitosta Yhdysvalloissa ja Iso-Britanniassa. (Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Kybersää Syyskuu 2020 2020, 3–7.)

3.2 Kyberturvallisuus terveydenhuollossa

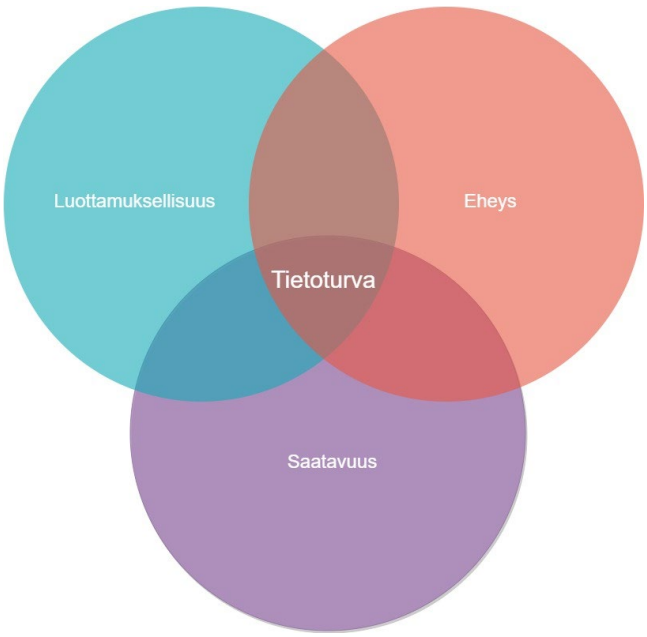
”Kyberturvallisuus on osa sosiaali- ja terveydenhuollon palveluiden varmistamista ja kuuluu kokonaisturvallisuuteen” (Vuorinen 2019, 11).

Terveydenhuollon ammattilaiset hyödyntävät päivittäin työssään digitaalisia palveluita. Palveluita toteutetaan paljolti tieto- ja viestintäteknologiaa hyödyntäen. Esimerkiksi mobiiliteknologiaa, pilvipalveluita, tekoälyä, IoT:ta ja ICMT-teknologiaa hyödynnetään. Nopea teknologioiden kehitys lisää haasteita tuottaa tietoturvallisia ja vaatimukset täyttäviä palveluita. (Vuorinen 2019, 11.)

Jotta terveydenhuollon organisaatioiden tietoturvan taso olisi hyvä, on käytössä olevien tietojärjestelmien oltava laadukkaita. Tarvitaan ainakin vakaata sovelluskantaa ja IT-infrastruktuuria. Tätä voi olla erityisen vaikea saavuttaa terveydenhuollon ympäristöissä johtuen resurssien puutteesta, budjettien rajoituksista, liian vähäisistä investoinneista ja monimutkaisesta sovelluskannasta. Se on kuitenkin kyberturvallisuuden näkökulmasta ratkaisevan tärkeää. (Argaw ym. 2020.)

Sairaaloiden lääkinnälliset laitteet ovat nykyään usein internetiin kytkettyjä, tämän lisäksi ne kytketään usein sairaaloiden tietoverkkoihin sekä toisiin laitteisiin. Nämä seikat lisäävät tietoturvariskejä. Verkottuminen on lisääntynyt sekä teknologian kehittymisen että ihmisten käyttötottumusten myötä. Lisähaasteen tuo se, että lääkintälaitteiden hyväksyntäkriteereissä kyberturvallisuuden vaatimuksia ei ole vielä osattu huomioida riittävästi. (Vuorinen 2019, 15.) Lääkinnällisten laitteiden valmistajien keskuudessa kyberturvallisuutta on viime aikoina pyritty edistämään. Lähestymistapaa on muutettu motivoimalla laitevalmistajia arvostamaan kyberturvallisuutta ja myymään laitteita sitä hyödyntäen. Kyberturvallisuutta ei liitetä laitteisiin jälkikäteen, vaan siitä on tullut yksi suunnittelun ennakkoedellytyksistä. (Argaw ym. 2020.)

Terveydenhuollossa erityistä huomiota tulee kiinnittää henkilö- ja asiakastietojen käsittelyyn tietojen arkaluonteisuuden vuoksi. Yksityisyyden takaamiseksi tietojen luottamuksellisuutta on suojattava. Jo lainsäädäntö velvoittaa tähän, mutta lisäksi kyse on terveydenhuollon maineesta ja uskottavuudesta arkaluontoisten terveystietojen käsittelijänä. Tietojen turvallisuudessa korostuvat eheys ja saatavuus, arkaluonteisuuteen liittyvän salassapidon, eli luottamuksellisuuden lisäksi (ks. kuvio 4). Asiakkaan palvelu ja potilaan hoito perustuvat tietoihin, joiden täytyy olla oikeita ja yhdistettävissä oikeaan potilaaseen (tiedon eheys). Tietojen on myös oltava käytettävissä juuri sillä hetkellä, kun niitä tarvitaan (tiedon saatavuus). (Vuorinen 2019, 13–14.)



Kuvio 4. Tiedon luottamuksellisuus, eheys ja saatavuus

Kyberhäiriöihin varautuminen terveydenhuollossa

100-prosenttisen varmaa kyberturvallisuutta ei ole, joten organisaation riskienhallintaprosessit ovat avainasemassa. Jopa hyvän IT-infrastruktuurin, mietittyjen käytäntöjen sekä ennakoivan asenteen ja tietoturvatoimien jälkeen hyökkäysriski on aina olemassa. Siksi yhdysvaltalaisen National Institute of Standards and Technologyn (NIST) suosittelemat kyberturvallisuuden hallinnan ohjeet ja Euroopan unionin verkko- ja tietoturvaviraston (ENISA) suositukset perustuvat riskiperusteiseen lähestymistapaan. On tärkeä tunnistaa riskialttiit IT-laitteet ja toiminnot, esimerkiksi järjestelmien haavoittuvuudenhallinnan kautta. Tätä korostaa kriittisen infrastruktuurin NIST Cyber Security Framework (NIST CSF) ensimmäisenä askeleena. Riskien tunnistamisen jälkeen organisaation tulee osata priorisoida riskit niiden mahdollisten vaikutusten kautta. Täten riskiarvio on tärkeä osa kyberturvallisuuden hallintaa. (Argaw ym. 2020.)

Kyberhyökkääjät pyrkivät usein pääsemään organisaatioiden tietoihin käsiksi yksittäisen ihmisen kautta ja siksi tietoisuuden lisääminen sekä henkilöstön kouluttaminen on erittäin tärkeää. Usein sanotaan, että ihminen on kyberturvallisuuden näkökul-

masta heikoin lenkki. Gyunkan ja Christianan (2017, 10) mukaan hyökkääjät hyödyntävät tehokkaasti ihmisen manipulointiin suunniteltuja hyökkäystekniikoita, ja tutkimuksen tulokset paljastivat, että inhimilliset tekijät ovat syynä 95 prosentissa kaikista kyberhäiriötapauksista.

Kyberhyökkäykset ovat yleistyneet terveydenhuollossa viime vuosina, ja täten terveydenhuollon organisaatioiden tulisi laatia prosessit ja toimintaohjeet kyberpoikkeamienhallintaan ja liiketoiminnan jatkuvuuteen. Nämä tulisi testata käytännössä ja niitä tulisi noudattaa. Kyberpoikkeamienhallinnan ja liiketoiminnan jatkuvuuden prosessien ja toimintaohjeiden perustana on, että tietoturvavastuullisten roolit ja vastuut on jaettu organisaatiossa selkeästi. (Argaw ym. 2020.)

Tärkeää terveydenhuollon kyberturvallisuudessa on uhkiin liittyvän tiedon jakaminen. Tiedon jakaminen voi liittyä esimerkiksi haitallisen toiminnan tunnistetietojen (IoC) välittämiseen tai tietojen jakamiseen haavoittuvuuksiin, saatuihin kokemuksiin ja häiriöiden lieventämisstrategioihin liittyen. Tietoa tulee välittää julkisen ja yksityisen sektorin sidosryhmien välillä. Tiedon jakaminen helpottaa tilannetietoisuutta ja ymmärrystä uhista ja uhkatoimijoista, heidän motivaatioistaan, kampanjoistaan, taktiikoistaan ja tekniikoistaan. Näin ollen se antaa päättäjille paremman käsityksen organisaation altistumisesta ja yrityksen riskienhallintapolitiikkojen soveltamisesta. (Argaw ym. 2020.) Papastergious ja muut (2020) myös täsmentävät, että kyberuhan kohdistuessa organisaatioon, jotkut tapahtumat voidaan tunnistaa tarkistamalla organisaation verkko tai käyttöjärjestelmät. Tätä toimintaa haitallisen toiminnan tunnistetietojen välittämiseksi voidaan pitää kyberuhkatiedustelun tärkeimpänä ytimenä. Tämän tiedon jakamisen edut ovat erittäin merkittäviä, varsinkin kun toiminnot sekä käsittelyä että jakamista varten voidaan tehdä automatisoidusti koko prosessin nopeuttamiseksi. (Papastergious ym. 2020.)

Kyberhäiriöihin reagointi terveydenhuollossa

Papastergiousin, Mouratidiksen ja Kalogerakin (2020) mukaan kyberhäiriöiden käsittely- ja reagointiprosessin päätavoitteena on määritellä turvallisuusongelmien, tapahtumien ja tapahtumien hallinnan tärkeimmät havainnot tai huolenaiheet. Käytännössä oikean lähestymistavan valinta tapahtumien käsittelyyn osoittautuu kuitenkin

vaikeaksi. Kirjoittajien mukaan nykyiset kyberhäiriötilanteiden torjuntaprosessit ovat liian keskittyneitä häiriöltä suojautumiseen, häiriön hävittämiseen ja häiriöstä palautumiseen liittyviin toimintoihin, eivätkä yleensä huomioi tai keskity muihin tapahtumien hallinnan vaiheisiin, kuten tutkintatoimiin (forensiikkaan). Prosessien ja toimintaohjeiden tulisi painottaa nykyistä enemmän proaktiivista valmistautumista ja reaktiivista oppimista, jotta kyberhäiriöistä voidaan myös oppia. (Papastergious ym. 2020.)

Branchin, Ellerin, Bias, McCawleyn, Myersin & Gerberin (2018) tekemässä tutkimuksessa yksi asia, jonka kukin tutkimukseen osallistunut organisaatio tunnisti auttavan kyberhäiriöihin reagoinnissa ja niiden vaikutusten lieventämisessä, oli tietotekniikan (IT) yksikön henkilöstön nopea tapahtuman tunnistaminen. Jokainen organisaatio ymmärsi olevansa hyökkäyksen kohteena, kun työntekijät soittivat organisaation IT-tukeen ja ilmoittivat ongelmista tiettyjen tietokonesovellusten käytössä. Jokaisen organisaation IT-tuen henkilöstö ymmärsi tämän jälkeen tapahtuneen ja sulki heidän verkkonsa. Yksi vastaajaorganisaatio ilmaisi, kuinka tärkeää oli, että heidän IT-tuen henkilökunnallaan oli valtuudet soittaa puhelu liittyen verkon sulkemiseen. Verkon nopea sulkeminen voi pysäyttää viruksen sivuttaisen leviämisen koko järjestelmässä ja ikään kuin "pysäyttää verenvuodon" järjestelmän vaikutusten kannalta. (Branch ym. 2018, 61–62.)

Toinen tutkimuksen vastauksista selvinnyt merkittävä oivallus oli, kuinka montaa eri sovellusta tai järjestelmää kussakin organisaatiossa käytettiin. Yksi reagoinnin ensimmäisistä vaiheista oli luettelon luominen sovelluksista, joihin vaikutus kohdistui, ja sen jälkeen priorisoinnin teko toiminnan kriittisyysnäkökulmasta. Tämän prosessin aikana jokaisesta organisaatiosta löydettiin sovelluksia, joista komentokeskuksen ihmisillä ei ollut aavistustakaan, ei tiedetty mitä ne olivat tai kuka niitä käytti. (Branch ym. 2018, 68.)

Terveydenhuollon ollessa kyseessä yksi ensimmäisistä kysymyksistä tutkimuksen tapauksissa oli **miten tämä vaikuttaa potilaan hoitoon?** Kaikissa tapauksista organisaatiot pystyivät jatkamaan hoidossa olevien potilaiden hoitoa. Yksi organisaatio asetti

päivystysosastonsa uusiin tiloihin, kunnes he pystyivät paremmin käsittelemään tilannetta. Toisen laitoksen oli peruttava joitakin sinä päivänä suunniteltuja leikkauksia. (Branch ym. 2018, 69.)

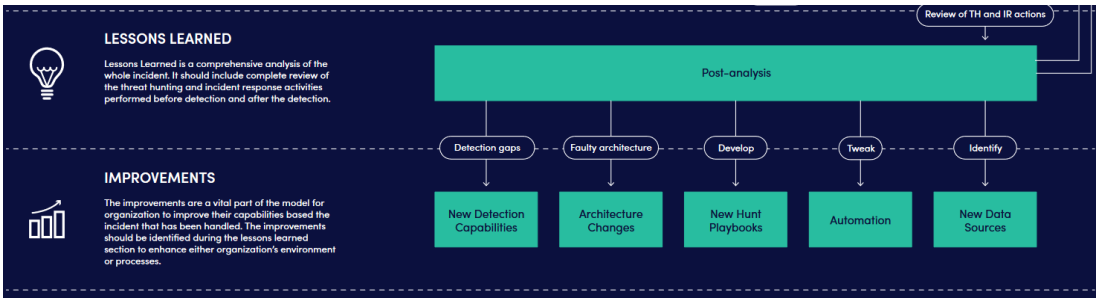
Kyberhäiriöistä palautuminen terveydenhuollossa

Eräässä tutkimuksessa toteutettiin sarja syvällisiä haastatteluita keskeisten sidosryhmien kanssa. Nämä sidosryhmät valittiin tutkimukseen kolmesta kyberhyökkäyksen uhriksi joutuneesta sairaalasta. Tutkimuksen tulosten mukaan kaikissa näissä sairaaloissa organisaation verkot olivat kokonaan pois käytöstä eri mittaisen ajanjakson ajan kyberhyökkäyksen tapahtuessa. Kaksi kolmesta organisaatiosta joutui toimimaan poikkeavissa oloissa yli kuukauden, eivätkä ne toipuneet hyökkäyksestä täysin kuuden kuukauden tai pidemmänkään ajanjakson aikana. Molemmat näistä organisaatioista arvioivat tapauksen maksaneen heille noin 10 miljoonaa dollaria. Palautumisajan pituuden ja hyökkäyksen vaikutusten laajuuden vuoksi molempien sairaaloiden edustajat kokivat, että tämä oli haastavin hätätilanne, jonka he olivat kokeneet sen aikana, kun ovat terveydenhuollossa työskennelleet. Yksi haastatteluissa esiin tulleista pääaiheista oli kyberhyökkäyksen potentiaalinen riski potilaan hoidolle, kun käytössä ei ole digitaalisia laitteita tarkan tiedon ja hoidon varmistamiseksi. (Branch ym. 2018, 56.)

Hyvä kyberhäiriöihin varautuminen ja suunnitelmat auttavat organisaatiota myös kyberhyökkäyksistä palautumisessa. Tulee ymmärtää järjestelmien riippuvuudet, kriisinhallinta ja tapahtumienhallinnan tehtävät. Lisäksi tulee olla järjestelyt vaihtoehtoisille viestintäkanaville, palveluille ja tiloille sekä monia muita liiketoiminnan jatkuvuuden elementtejä. (Bartock, Cichonski, Souppaya, Smith, Witte & Scarfone 2016, 7.)

Yksi erittäin tärkeä seikka kyberhäiriöstä palautumisessa on dokumentoida tarkasti häiriön vaiheet liittyen sen rajaamiseen ja siitä palautumiseen. Lisäksi tulee dokumentoida myös kaikki häiriöön liittyvä todistusaineisto sekä vaarantumisindikaattorit. Nämä toimet auttavat ymmärtämään tapahtunutta ja estämään vastaavanlaisten tilanteiden syntyminen tulevaisuudessa. (JYVSECTEC PHR-model 2020.)

Palautumisprosessin lopussa on tärkeää ottaa tapahtumasta opit talteen. Kuviosta 5 näkee JYVSECTECin PHR-mallin viimeiset vaiheet, joissa olennaista on tunnistaa opitut asiat ja parantaa niiden mukaisesti organisaation toimintaa. Tulee tehdä kattava analyysi koko tapahtumasta. Siihen tulee sisältyä täydellinen tarkastelu ajalta ennen tilanteen havaitsemista ja sen jälkeen suoritetuista uhkiin liittyvistä tapahtumista. Jälkianalyysiä voidaan käyttää esimerkiksi työkaluna organisaation valmiuksien jatkuvaan kehittämiseen tai esimerkiksi haavoittuvuuksien tai vääränlaisen arkkitehtuurin tunnistamiseen. (JYVSECTEC PHR-model 2020.)



Kuvio 5. PHR-mallin viimeiset vaiheet (JYVSECTEC PHR-model 2020)

4 Kehittämisprosessin kuvaus

Tässä luvussa esitellään projektin tuotoksen kehittämisprosessi. Aluksi käydään läpi projektin tavoite ja toimenpiteet projektisuunnitelmaan viitaten. Projektitiimi ja sen jäsenten tehtävät esitellään. Tämän jälkeen käydään läpi projektin alkutilanne ja tilannekartoitusvaihe. Viimeisenä alalukuna on tuotoksen toteuttamisprosessi.

4.1 Projektin tavoite ja toimenpiteet

Projektissa **Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä** oli tarkoituksena kehittää terveydenhuollon ympäristöihin liittyviä kyberpoikkeamienhallinnan prosesseja ja toimintaohjeita, jotta varmistetaan yhteiskunnan kannalta kriittisen terveydenhuollon jatkuvuutta ja toimintakykyä myös ky-

berhyökkäyksien tapahtuessa. Lisäksi yhteistoiminta valtakunnallisella tasolla tiedonjakamisessa sekä tilannekuvassa huomioitiin projektissa. Projekti liittyi kiinteästi koronakriisin aiheuttamien haasteiden ratkaisemiseen, sillä kriisin myötä on syntynyt uudenlaisia uhkia digi- ja tietoturvallisuuden näkökulmasta. Projektin tulokset ovat terveydenhuollon toimijoiden hyödynnettävissä projektin päätyttyä. (Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma 2020, 1.) Projektin toteuttajaorganisaationa toimi JYVSECTEC.

Projektin toimenpiteet oli jaettu kolmeen työpakettiin: tilannekartoitus, prosessit ja ohjeet sekä tietoisuuden lisääminen. Jokaiselle työpaketille oli määriteltynä aikataulu, tulostavoite sekä toimenpiteet tehtävinä. Lisäksi oli määritelty projektin yleiset toimenpiteet. Työpaketti 1 oli nimeltään **tilannekartoitus** ja sen ohjeellinen aikataulu oli 1.8.2020-31.8.2020. Työpaketin tulostavoitteena oli, että terveydenhuollon toimijoiden ohjeet ja prosessit kyberpoikkeamatilanteisiin on kartoitettu. Työpaketti sisälsi kaksi toimenpidettä:

- Kartoitetaan yhteistyökumppaneiden avulla terveydenhuollon toimijoiden voimassa olevat ohjeet ja prosessit kyberpoikkeamatilanteessa.
- Kartoituksen avulla kootaan tiedossa olevat puutteet ja yksityiskohtaiset vaatimukset prosessien sekä toimintaohjeiden parantamiseksi. (Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma 2020, 2.)

Työpaketti 2 oli nimeltään **prosessit ja ohjeet** ja sen ohjeellinen aikataulu oli 1.9.2020-15.12.2020. Työpaketin tulostavoite oli, että uusia ohjeita ja prosesseja kyberpoikkeamatilanteisiin on laadittu. Työpaketti sisälsi kaksi toimenpidettä:

- Kartoitetaan ajankohtaiset terveydenhuollon toimintaan kohdistuvat kyberuhkavektorit, huomioiden koronakriisi.
- Työpaketin 1 tulosten kautta kootun uhkavektoritiedon perusteella laaditaan uusia ohjeita ja prosesseja terveydenhuollon toimijoiden käyttöön kyberpoikkeamatilanteiden ratkaisemiseksi koronapandemian aikana ja sen jälkeen. (Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma 2020, 2.)

Työpaketti 3 oli nimeltään **tietoisuuden lisääminen** ja sen ohjeellinen aikataulu oli 16.12.2020-31.1.2021. Työpaketin tulostavoite oli, että laadittujen ohjeiden ja prosessien käyttöönottamiseksi on toteutettu tietoisuuden lisäämiskampanja. Työpaketti sisälsi kaksi toimenpidettä:

- Tiedotetaan tuloksista terveydenhuollon toimijoita asiantuntijayhteistyönä.
- Toteutetaan tuloksista sosiaalisessa mediassa tiedotuskampanja. (Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma 2020, 2.)

Lisäksi projektisuunnitelmassa oli mainittuna yleiset toimenpiteet, jotka liittyivät kaikkiin projektin tulostavoitteisiin. Näihin sisältyi muun muassa johtaminen, raportointi, projektin seuranta ja hallinnointi sekä projektin toiminnasta tiedottaminen ja loppuraportin laatiminen. (Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma 2020, 2.)

4.2 Projektitiimi ja jäsenten tehtävät

Projektissa pääasiallisina työntekijöinä olivat projektiasiantuntija sekä projektipäällikkö, joiden työpanos oli lähes 100-prosenttisesti allokoitu projektille sen toteutusajanjaksolla. Asiantuntija tutki aihetta ja kirjoitti projektin tuotosta. Projektipäällikkö hoiti kirjoitus- ja tutkimustyön lisäksi muun muassa viestintää yhteistyökumppaneiden suuntaan, palaverien koordinointia sekä yleisiä projektin talouteen ja hallinnointiin liittyviä tehtäviä. Projektipäällikkö ja asiantuntija toimivat työparimaisesti toteuttaen sisältöjä tiiviissä yhteistyössä. Tämän lisäksi käytettiin toteuttajaorganisaation (JYVSECTEC) neljää asiantuntijaa tiettyjen osa-alueiden sisällöntuottajina. Nämä osa-alueet vaativat syvällistä asiantuntijuutta, jota toteuttajaorganisaatiosta löytyi. Aihealueet olivat riskienhallinta, kyberturvallisuussertifikaatit, kyberturvallisuuteen liittyvän tilannetiedon jakaminen sekä kyberhäiriöiden käsittely ja reagointi (sisältäen muun muassa ohjeet kyberhäiriön tekniseen käsittelyyn). Lisäksi projektin kuvituksen toteutti kuvittaja ja taitossa käytettiin visuaalisen suunnittelun asiantuntijaa. Viestintää teki projektiasiantuntijan ja -päällikön lisäksi kaksi toteuttajaorganisaation viestintäasiantuntijaa. Projektin talousraportointia ja arkistointia hoiti projektisihteeri.

4.3 Projektin lähtökohdat ja tilannekartoitus

Projektissa oli tarkoitus kehittää terveydenhuollon ympäristöihin liittyviä kyberpoikkeamienhallinnan prosesseja ja toimintaohjeita. Lähtötilanteena oli terveydenhuollon toimijoiden senhetkiset ohjeet ja prosessit kyberhäiriö- ja poikkeamatilanteisiin. Niitä oli tarkoitus katselmoida projektin alussa. Tämä osoittautui kuitenkin ongelmalliseksi, sillä sairaanhoitopiirien ja muiden terveydenhuollon toimijoiden ohjeet eivät ole julkista tietoa. Yleisessä jaossa olleisiin ohjeisiin kuitenkin perehdyttiin, yhtenä esimerkkinä STM:n vuonna 2019 julkaisema Kyberturvallisuus – ohje sosiaali- ja terveydenhuollon toimijoille. Kyseisen ohjeen tarkoitus on luoda alan kyberturvallisuudesta yleiskuva. Ohje sisältää alaa koskevia periaatteita, jo olemassa olevia ohjeita ja alan suosituksia. Tuotos perustuu Suomen kyberturvallisuusstrategian toimeenpanoohjelmaan. Se ei sisällä yksityiskohtaisia tai teknisiä ohjeita kyberuhan tunnistamiseen tai sen torjuntaan. (Vuorinen 2019.)

Seuraavaksi kartoitettiin ajankohtaiset tarpeet terveydenhuollon kyberturvallisuusprosessien ja toimintaohjeiden kehittämiseen liittyen sekä kyberuhkavektorit erityisesti koronapandemia huomioiden. Tilannekartoitus sisälsi muun muassa Microsoft Teams -palaverin kunkin yhteistyökumppanin kanssa erikseen. Näiden palavereiden kautta saatiin niin sanottua sisäpiirin tietoa terveydenhuoltoalan kyberturvallisuuden puutteista ja ongelmakohdista. Kukin palavereista (joita oli seitsemän) kesti noin tunnin. Palavereissa esiteltiin projekti lyhyesti, ongelma joka projektin aikana oli tarkoitus ratkaista, projektin tavoitteet, toteutus ja tulokset. Suurin osa palaverista käytettiin keskusteluun, minkä tueksi ja avaukseksi oli määritelty seuraavat aiheet:

- Voimassa olevat ohjeet ja prosessit kyberpoikkeamatilanteisiin terveydenhuollossa sekä näiden mahdolliset puutteet (koronakriisi huomioiden).
- Näkemykset ajankohtaisista terveydenhuollon toimintaan kohdistuvista kyberuhkavektoreista, erityisesti koronakriisi huomioiden.

Palavereissa käytetty Microsoft PowerPoint -esitys löytyy tämän työn liitteistä (ks. liite 1). Sekä toteuttajaorganisaation (JYVSECTEC) projektipäällikkö että projektiasian-

tuntija tekijät palavereista pöytäkirjat, ja jokaisen palaverin jälkeen he lisäksi keskustelivat yhdessä tärkeimmistä palavereissa nousseista teemoista. Kun kaikki tilannekartoituspalaverit oli käyty, projektipäällikkö luki pöytäkirjat läpi ja koosti niiden pohjalta yhden dokumentin. Dokumenttiin tiivistettiin jokaisesta palaverista tärkeimmät havainnot. Lisäksi aineistoa luokiteltiin seuraavien otsikoiden alle: kyberuhat koronakriisin aikana, koronakriisin vaikutus terveydenhuoltoalan kyberturvallisuuteen, huomioita koronakriisin ajalta, terveydenhuollon ongelmakohdat kyberturvallisuudessa ja apuvälineitä varautumisen suunnitteluun. Lisäksi listattiin erikseen palavereissa nousseet ongelmat, ratkaisut ja tavoiteltavat asiat. Dokumenttia ei julkaista työssä, sillä sen aineisto ei ole julkista. Palaverit järjestettiin seuraavien yhteistyökumppaniorganisaatioiden kanssa:

- Terveyden- ja hyvinvoinnin laitos
- Huoltovarmuuskeskus (mukana edustajia Digipoolista ja Terveydenhuoltopoolista)
- Liikenne- ja viestintävirasto Traficomin kyberturvallisuuskeskus
- Keski-Suomen sairaanhoitopiiri
- Pirkanmaan sairaanhoitopiiri
- Telia sekä
- Kyber-Terveys-hanke.

Yllä mainittujen yhteistyötahojen lisäksi oltiin vielä sähköpostitse yhteydessä Suomen sairaanhoitopiirien ja sairaaloiden tietohallintovastaaviin ja saatiin muutamilta myös vastauksia ajankohtaisista tarpeista häiriönhallinnan ohjeistusten kehittämisessä. Lisäksi projektipäällikkö ja/tai projektiasiantuntija osallistuivat aiheeseen liittyviin webinaareihin, joista ohessa listaus.

- Tieto20-harjoitus (15.9.2020)
- ENISA eHealth Session 1: Cyber Security in Healthcare in times of a pandemic -webinaari (23.9.2020)
- ERVA Kyber Road Show -seminaari (24.9.2020)
- VAHTI-seminaari johdolle ja asiantuntijoille (14.10.2020)
- ENISA eHealth Session 2: Cyber Security in COVID19 tracing mobile apps -webinaari (23.10.2020)

- Traficomin Kyberturvallisuuskeskuksen webinaari medioille ja sidosryhmille (27.10.2020)
- VAHTI-webinaari (18.11.2020)
- Technopolis Workplace Talks & Networking, F-Secure: Risto Siilasmaa & Mikko Hyppönen: “What business leaders should consider for 2021?” (18.11.2020)
- Cyberwatch-webinaari IT- ja tietoturvapäättäjille (19.11.2020)
- ENISA eHealth Security Conference 2020 - Session 3: Incident response while in crisis (23.11.2020)
- VAHTI-päivä (1.12.2020)
- Tietoturva ja kyberrikollisuus terveydenhuollossa, Diktamen-webinaari (4.12.2020).

Seminaareihin osallistumisen lisäksi projektipäällikkö ja -asiantuntija lukivat aiheesta ajankohtaisia uutisia, raportteja ja tutkimuksia. Näiden toimien kautta muodostui kokonaiskuva kyberhäiriöiden hallinnan prosessien ja toimintaohjeiden puutteista terveydenhuollossa ja näihin puutteisiin lähdettiin kehittämään ratkaisuja.

Projektin aihe muuttui syksyllä 2020 suomalaiseen psykoterapiakeskukseen kohdistuneen laajan tietomurron ja kiristyksen vuoksi entistä ajankohtaisemmaksi. Aiheeseen liittyen käytiin paljon yhteiskunnallista keskustelua ja järjestettiin avoimia webinaareja. Tietoa aiheeseen liittyen oli projektin aikana hyvin saatavilla.

4.4 Projektin tuotoksen toteuttamisprosessi

Tilannekartoituksen jälkeen projektissa muodostettiin kokonaiskuva olemassa olevien terveydenhuollon kyberhäiriöiden prosessien ja toimintaohjeiden puutteista. Puutteiden perusteella päätettiin luoda käsikirja eri kokoisille terveydenhuollon organisaatioille, missä kyberhäiriöiden hallinnan eri vaiheet käsitellään kattavasti ja myös koronakriisin vaikutukset tuodaan esiin. Tilannekartoituksen perusteella ilmeni, että käsikirjan sisältämät prosessit ja ohjeet tulee olla helposti ymmärrettäviä ja käytäntöön sovellettavia. Lisäksi haluttiin luoda tarkistuslistoja häiriönhallinnan eri vaihei-

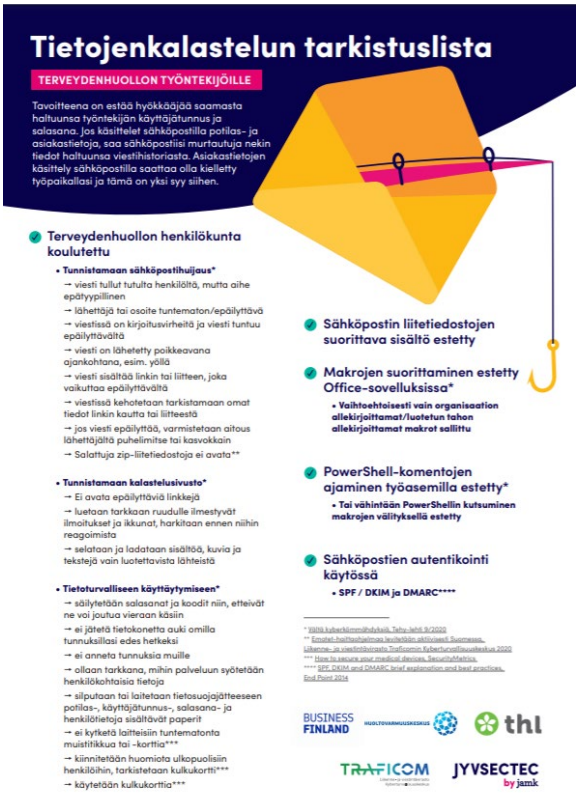
siin, sillä Suomen terveydenhuollon kyberturvallisuuden näkökulmasta niitä ei tiettävästi vielä ole tehty. Tekniset asiasisällöt ja termit päätettiin aukikirjoittaa lukijalle, sillä käsikirjan kohderyhmä määriteltiin melko laajaksi sisältäen kaikki terveydenhuollon toimijat. Tarkemmaksi kohderyhmäksi määriteltiin eri kokoisten terveydenhuollon organisaatioiden kyber- ja digiturvallisuudesta päättävät tahot sekä kyber- ja digiturvallisuudesta vastaavat työntekijät. Täten haluttiin, että teknisemmät termit ovat aukikirjoitettuna ja sisällöt, jotka ovat suunnattu erityisesti teknisemmille kyber- ja digiturvallisuudesta vastaaville työntekijöille, on käsikirjassa ilmoitettu. Tärkeänä huomiona tilannekartoituksissa nousi myös se, että terveydenhuollon kyberturvallisuudessa potilasturvallisuus on aina keskiössä. Kyberturvallisuuden ratkaisuissa on huomioitava potilasturvallisuus.

Lokakuun alussa yhteistyökumppaneihin oltiin sähköpostitse yhteydessä tilannekatsauksen merkeissä. Heille kerrottiin missä vaiheessa projekti on meneillään ja, että sisällysluettelon ensimmäinen versio on valmis. Yhteistyökumppaneille annettiin senhetkinen sisällysluettelo kommentoitavaksi. Lisäksi Kyberturvallisuuskeskukselta pyydettiin kommentteja osioon, jossa esiteltiin kyberturvallisuuden toimijat Suomen terveydenhuollossa, sillä heillä nähtiin roolinsa puolesta olevan osioon annettavaa. Yhteistyökumppaneilta saatiin arvokasta palautetta ja sisältöihin tehtiin palautteiden mukaisesti muutoksia.

Seuraavan kerran yhteistyökumppaneihin oltiin sähköpostitse yhteydessä marraskuun puolivälissä ja heiltä tiedusteltiin halukkuutta lukea käsikirja läpi sekä kommentoida sen sisältöjä. Heille kerrottiin, että kyseessä on noin 50-sivuinen tuotos, joka on vielä luonnosvaiheessa. Aikataulun ollessa projektissa melko tiukka luonnoksen ajateltiin olevan kypsä kommentointia varten. Aikataulutavoitteet (eli saada lopputuotos valmiiksi kuun loppuun mennessä) kerrottiin yhteistyökumppaneille. Heille täsmennettiin myös, että ennen projektin päättymistä käsikirjalle tehdään laadukas taitto ja toteutetaan tietoisuudenlisäämiskampanja. Vain kaksi yhteistyökumppaneista ehti perehtyä tuotokseen. Toinen heistä laati erittäin tarkat kehittämisehdotukset koko lopputuotoksesta. Ne olivat hyödyllisiä ja suurin osa otettiin huomioon käsikirjassa.

Joulukuussa projektin käsikirja oli sisällöllisesti valmis pois lukien pienet viimehetken muutokset ja kieliasuun liittyvät tarkistukset. Tämän jälkeen käynnistyi käsikirjan taitto, jonka toteutti JYVSECTECin visuaalisen suunnittelun ammattilainen konsultoiden projektipäällikköä. Taittotyö oli vaativa ja vei aikaa lähes kuukauden verran. Projektin käsikirja saatiin valmiiksi noin viidessä kuukaudessa. Käsikirja julkaistiin JYVSECTECin Publications-sivustolla 5.1.2021 osoitteessa: https://jyvsectec.fi/2021/01/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille/.

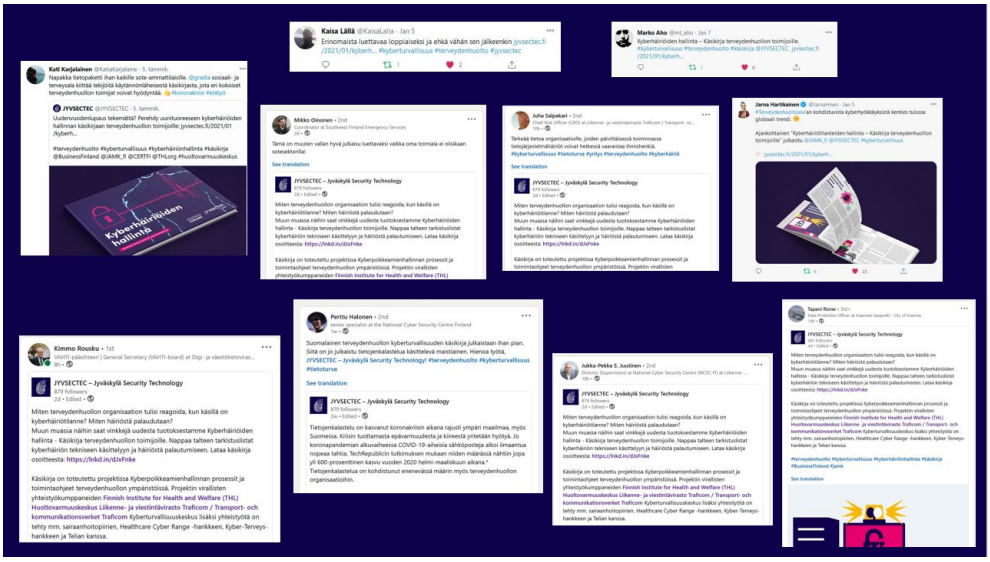
Jo ennen käsikirjan valmistumista projektin etenemisestä viestittiin sosiaalisessa mediassa ja julkaistiin muun muassa ennakkomainoksena ote käsikirjasta (ks. kuvio 6).



Kuvio 6. Tietojenkalastelun tarkistuslista (Vertainen & Suni 2020)

Projektin käsikirjan julkaisun jälkeen käynnistettiin laajamittainen viestintäkampanja, joka alkoi sillä, että JAMK julkaisi tiedotteen käsikirjasta: https://www.epressi.com/tiedotteet/terveys/kasikirja-tukemaan-terveydenhuollon-

kyberturvallisuutta-suomessa-myos-koronakriisin-aikaisia-vaikutuksia-kasitelty.html. Viestintäkampanjan laajempi kohderyhmä olivat kaikki terveydenhuollon toimijat, mutta suppeampi kohderyhmä eri kokoisten terveydenhuollon organisaatioiden kyber- ja digiturvallisuudesta päättävät tahot sekä kyber- ja digiturvallisuudesta vastaavat työntekijät. Sosiaalisen median osalta kampanja toteutettiin JAMKin (Twitter, LinkedIn ja Facebook) sekä JYVSECTECin (LinkedIn ja Twitter) sosiaalisen median kanavissa. JYVSECTECin kanavissa viestintää jatkettiin myös projektin päätymisen (31.1.2021) jälkeen. Sosiaalisen median kampanjointiin osallistuivat JYVSECTECin sekä kumppaniorganisaatioiden lisäksi myös yksityishenkilöt, jotka jakoivat aktiivisesti julkaisuja käsikirjasta omilla tileillään. JYVSECTECin viestintäasiantuntijan mukaan mikään aikaisempi aihe ei ole aiheuttanut näin paljon sosiaalisen median jakoja. Kuviossa 7 on yksittäisten henkilöiden jakamia julkisia julkaisuja sosiaalisen median LinkedIn- ja Twitter-kanavissa. Mukana on valtakunnallisesti merkittäviä kyberturvallisuuden asiantuntijoita, kuten esimerkiksi VAHTI-pääsihteeri Kimmo Rousku.



Kuvio 7. Esimerkkejä yksittäisten henkilöiden tekemistä sosiaalisen median julkaisuista käsikirjaan liittyen

Käsikirjaan liittyen kirjoitettiin myös kaksi blogi-kirjoitusta, joista toinen oli nimeltään: **Ajankohtaiset kyberuhkat terveydenhuollossa**. Kirjoitus löytyy osoitteesta:

https://blogit.jamk.fi/techtothefuture/2021/01/11/ajankohtaiset-kyberuhkat-terveydenhuollossa/. Toinen kirjoitettiin englanniksi tavoitellen kansainvälistä yleisöä. Blogikirjoituksen nimi oli: **Healthcare under attack – Cyber Security Incident Response in Times of Pandemic** ja se löytyy osoitteesta: https://jyvsectec.fi/2021/01/healthcare-under-attack-cyber-security-incident-response-in-times-of-pandemic/.

Yhteistyökumppaneille tarjottiin viestinnän tueksi tiedote, valmiita kuvituskuvia ja sosiaalisen median julkaisuja. Yhteistyökumppanit viestivät käsikirjasta aktiivisesti verkostoissaan, uutiskirjeissään sekä verkkolehdissään. Esimerkkinä, Varmuuden Vuoksi -verkkolehden julkaisu: **Kyber-Terveys -hankkeen Road Show: Digiloikasta turvallisuusloikkaan** osoitteessa: https://www.varmuudenvuoksi.fi/aihe/kyber/534/kyber-terveys_-hankkeen_road_show_digiloikasta_turvallisuusloikkaan. Myös useammassa JAMKin uutiskirjeessä mainittiin käsikirja. Muina viestinnän toimenpiteinä voidaan mainita, että JAMKin hyvinvointiyksikön terveysalan koulutuspäällikkö jakoi tietoa käsikirjasta aktiivisesti terveydenhuollon ammattilaisten verkostoissaan ja JAMKin IT-instituutin johtaja varasi puheenvuoron käsikirjan esittelemiseen Keski-Suomen Turvallisuusfoorumin maaliskuun 2021 kokoukseen.

5 Tutkimuksen tulokset

Tutkimuksen tulokset esitellään tässä luvussa. Projektin tuloksena syntyneen tuotoksen käyttö ja sisältöjen esittely kappaleen jälkeen esitellään tuotoksen pääkappaleet ja niiden sisällöt yksitellen. Kunkin pääkappaleen esittelyn kohdalla avataan myös perusteita sille, miksi kyseinen aihe on valittu tuotoksessa käsiteltäväksi. Luku päättyy kappaleeseen, jossa esitellään tuotoksesta saadut palautteet.

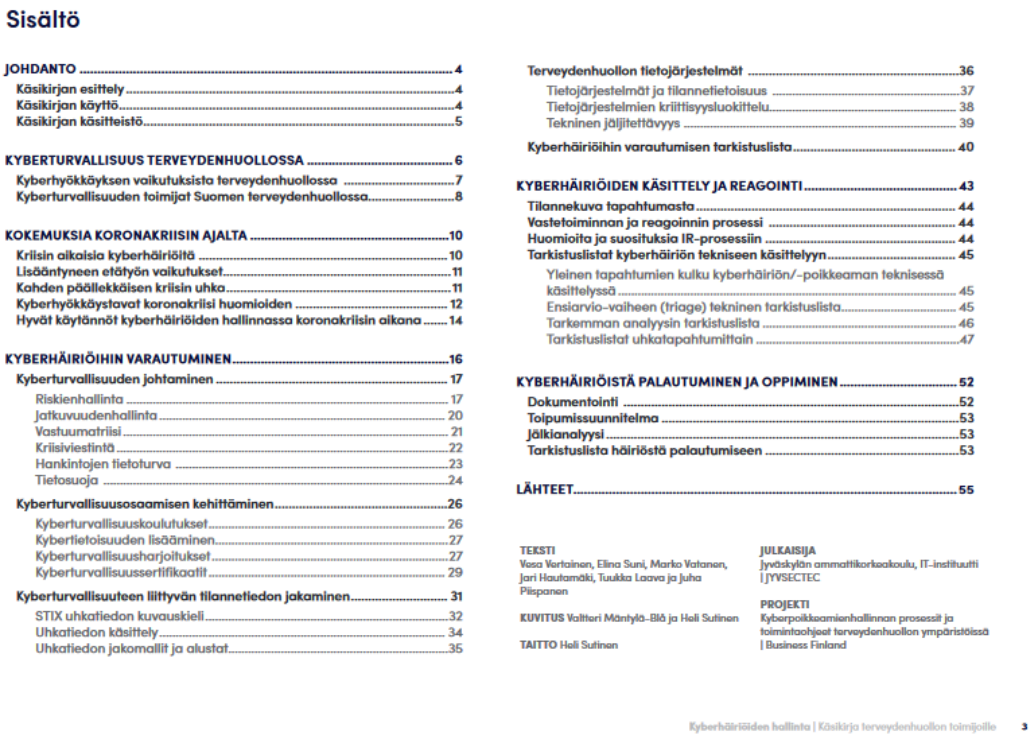
5.1 Projektin tuotoksen käyttö ja sisältöjen esittely

Projektin lopputuotoksena syntyi **Kyberhäiriöiden hallinta – Käsikirja terveydenhuollon toimijoille** teos, joka on julkisesti saatavilla JYVSECTECin

verkkosivuilla. Käsikirjan kohderyhmänä ovat kaikki terveydenhuollon toimijat, mutta erityisesti eri kokoisten terveydenhuollon organisaatioiden kyber- ja digiturvallisuudesta päättävät tahot sekä kyber- ja digiturvallisuudesta vastaavat työntekijät. Käsikirja sisältää muun muassa prosesseja, ohjeita ja tarkistuslistoja terveydenhuollon kyberturvallisuuteen, tarkemmin ottaen kyberhäiriöiden hallintaan liittyen. Nämä on esitetty helposti käytäntöön vietävässä muodossa. Tekniset asiasisällöt ja termit on aukikirjoitettu lukijalle. (Vertainen ym. 2021, 4.)

Käsikirja on tarkoitettu helposti sisäistettäväksi kokonaisuudeksi kyberhäiriöiden hallinnan kehittämiseen nimenomaan terveydenhuollossa. Käsikirjasta saa kattavasti tietoa kybervarautumiseen, joka on erittäin tärkeä osa kyberhäiriöiden hallintaa. Lisäksi käsikirjaa voidaan hyödyntää myös silloin, kun uhka on jo realisoitunut häiriöksi ja vaatii nopeaa reagointia. Käsikirja on myös hyödyllinen jälkianalyysissä, jossa palautuminen normaaliin toimintaan ja häiriöiden välttäminen tulevaisuudessa korostuvat (sekä näiden kahden vaiheen ennakoinnissa). Käsikirja sisältää vinkkejä, linkkejä tiedon lähteille sekä nopeasti hyödynnettäviä tarkistuslistoja kyberhäiriönhallinnan eri vaiheisiin sekä koronakriisin aikana nousseisiin uudenlaisiin uhkatilanteisiin. (Vertainen ym. 2021, 4.)

Käsikirjan **johdannossa** esitellään käsikirja sekä käsikirjassa käytetty käsitteistö. Sen jälkeen lukija johdatellaan aiheeseen **kyberturvallisuus terveydenhuollossa** pääkappaleen kautta, jossa käsitellään kyberhyökkäysten vaikutuksia terveydenhuollolle sekä listataan terveydenhuollon kyberturvallisuuden toimijat Suomessa painottaen lisäksi yhteistyön merkitystä toimijoiden välillä. Toimijoiden välinen yhteistyö nousi tärkeänä teemana esiin lähes kaikissa yhteistyökumppaneiden kanssa käydyissä tilannekartoituspalavereissa. **Kokemuksia koronakriisin ajalta** kappale on nostettu omaksi osiokseen, koska kriisin aikana on syntynyt uudenlaisia uhkaskenaarioita muun muassa etätyön yleistyessä uusilla aloilla. Lisäksi kyberturvallisuusuhat ovat yleisesti lisääntyneet terveydenhuollossa koronakriisin aikana. Käsikirjassa kyberhäiriöiden hallinta on jaettu eri osa-alueisiin, jotka ovat: **kyberhäiriöihin varautuminen**, **kyberhäiriöiden käsittely ja reagointi** sekä **kyberhäiriöistä palautuminen ja oppiminen**. Käsikirjan sisällysluettelo on esitetty kuviossa 8.



Sisältö

TEKSTI
Vesa Vertainen, Elina Suni, Marko Vatanen, Jari Hautamäki, Tuukka Laava ja Juha Pispanen

KUVITUS Valtteri Mäntylä-Blå ja Heli Sutinen

TAITTO Heli Sutinen

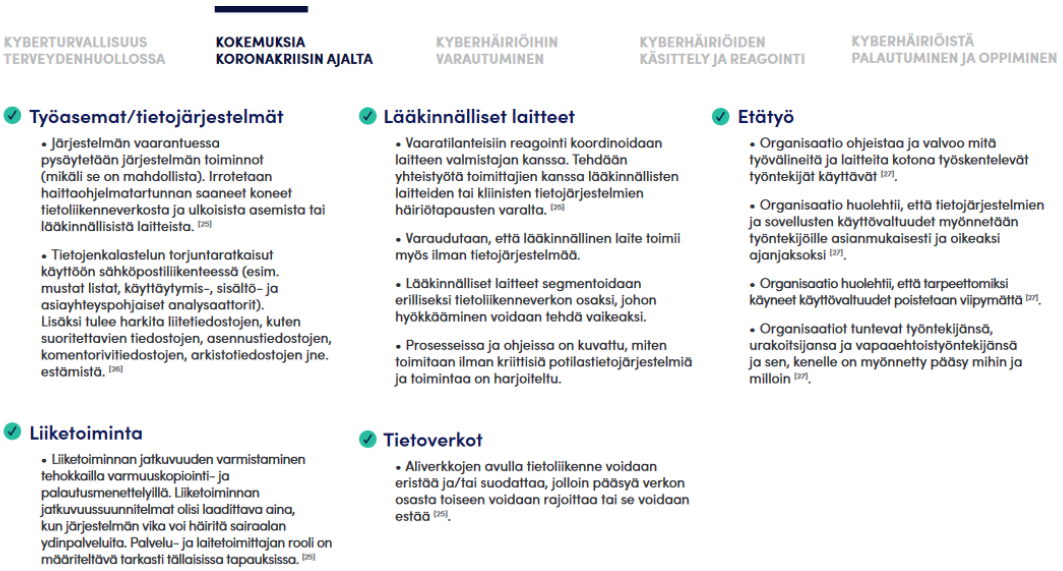
JULKAISIJA
Jyväskylän ammattikorkeakoulu, IT-instituutti | JYVSECTEC

PROJEKTI
Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä | Business Finland

Kuvio 8. Käsikirjan sisällysluettelo (Vertainen ym. 2021, 3)

5.1.1 Kokemuksia koronakriisin ajalta

Kohdennettuja kiristyshaittaohjelmia on nähty koronakriisin aikana ympäri maailmaa, myös Suomessa. Myös tietojenkalastelu on ollut rajussa kasvussa. Kriisin tuottamasta epävarmuudesta ja kiireestä yritetään hyötyä. (Vertainen ym. 2021, 10.) Projektisuunnitelmassa määriteltiin, että ajankohtaiset terveydenhuollon toimintaan kohdistuvat kyberuhkavektorit tulee kartoittaa, erityisesti koronakriisi huomioiden. Täten **kokemuksia koronakriisin ajalta** haluttiin nostaa käsikirjaan omana pääkappaleenaan. Aihe on erittäin ajankohtainen ja sisältää uutta tietoa. Kappaleessa käsitellään kriisin aikaisia kyberhäiriöitä esimerkkien kautta sekä nostetaan esiin eri kyberhyökkäystapoja. Osiossa käsitellään myös lisääntyneen etätyön vaikutuksia kyberturvallisuuden näkökulmasta terveydenhuollossa ja esimerkin kautta kahden päällekkäisen kriisin mahdollisia vaikutuksia. Kappaleen lopussa nostettiin esiin hyviä käytäntöjä kyberhäiriöiden hallinnassa koronakriisin aikana, josta ote kuviossa 9.



Kuvio 9. Ote kappaleesta hyvät käytännöt kyberhäiriöiden hallinnassa koronakriisin aikana (Vertainen ym. 2021, 15)

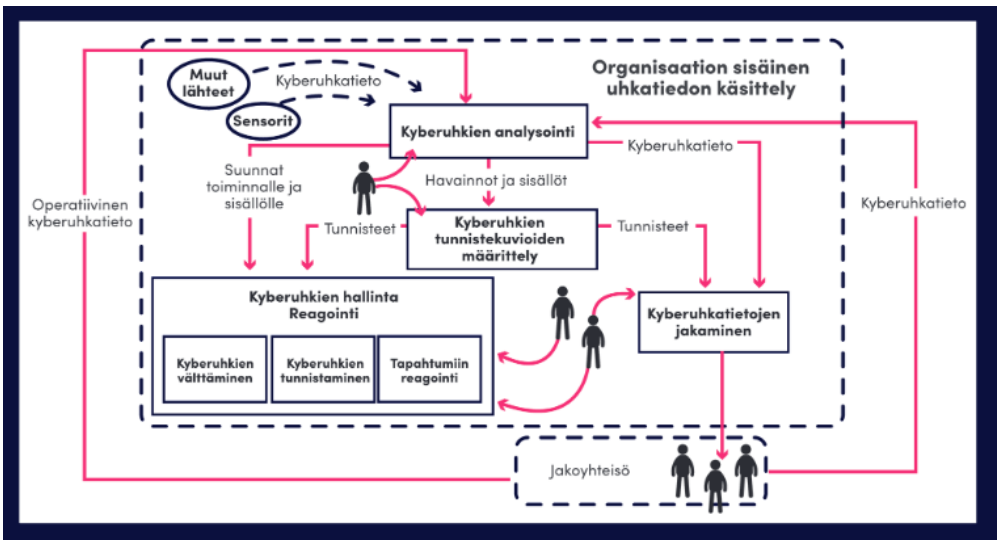
5.1.2 Kyberhäiriöihin varautuminen

Kyberturvallisuuden johtaminen aihe käsiteltiin kyberhäiriöihin varautuminen pääotsikon alla. Valtioneuvosto nimitti vuoden 2020 helmikuussa valtion kyberturvallisuusjohtajaksi Rauli Paanasen. Rauli Paananen on Suomen historian ensimmäinen valtion kyberturvallisuusjohtaja. Liikenne- ja viestintäministeriön mukaan kansallisen tason johtamisen lisäksi tarvitaan organisaatiotasoista kyberturvallisuuden järjestelmällistä johtamista, joka on ensisijaisesti organisaation ylimmän johdon vastuulla. (Liikenne- ja viestintäministeriö 2020.) Yhteistyökumppaneiden kanssa käytyjen tilannekartoituspalavereiden perusteella kyberturvallisuuden johtamisen alla nähtiin tärkeäksi käsitellä myös riskienhallinta, jatkuvuudenhallinta, vastuumatriisi, kriisiviestintä, hankintojen tietoturva ja tietosuoja.

Organisaation työntekijöiden **kyberturvallisuusosaamisen kehittäminen** nousi tärkeäksi osaksi häiriöihin varautumista sekä tilannekartoituspalavereissa että ENISAn järjestämässä webinaarissa (Enisa eHealth Session 1: Cyber Security in Healthcare in ti-

mes of a pandemic -webinaari, 23.9.2020). Sama nousi esiin myös tiivistelmässä kyberturvallisuuden nykytilakartoituksesta eri toimialoilla. Tiivistelmästä selviää, että henkilöstön kyberturvallisuusosaamista olisi syytä lisätä etenkin niillä toimialoilla, joissa se ei kuulu ydinosaamiseen tai henkilöstön vaihtuvuus on suurta. (Huoltovarmuuskeskus, Digipooli & Liikenne- ja viestintäviraston Kyberturvallisuuskeskus 2020, 14.) Terveydenhuoltoon sopii hyvin nämä kuvaukset**.** Kyberturvallisuustietoisuuden lisääminen, kyberturvallisuuskoulutukset ja kyberturvallisuusharjoitukset aiheet valittiin myös käsikirjaan, sillä nekin nousivat esiin yhteistyökumppaneiden kanssa käydyissä tilannekartoituspalavereissa. Kyberturvallisuussertifikaattien tärkeyttä painotettiin muun muassa Diktamenin 4.12.2020 järjestämässä webinaarissa: Tietoturva ja kyberrikollisuus terveydenhuollossa ja täten aihe nostettiin mukaan käsikirjaan.

Tilannekuvan ja tilannetiedon tärkeys nousi esiin yhteistyökumppaneiden kanssa käydyissä tilannekartoituksissa. Tarkka ja oikea-aikainen tilannetieto on hyvin merkittävässä roolissa organisaation sietokyvyn parantamisessa kyberturvahyökkäyksiä vastaan. **Kyberturvallisuuteen liittyvän tilannetiedon jakaminen** nostettiin täten käsiteltäväksi aiheeksi käsikirjaan. Kappaleessa avattiin myös STIX-uhkatiedon kuvauskielen roolia tilannetiedon jakamisessa, uhkatiedon käsittelyä (tiedonjakoverkostossa) sekä uhkatiedon jakomalleja ja alustoja. Näiden kolmen alakappaleen lukijakunnaksi määriteltiin erityisesti kyber- ja digiturvallisuuden parissa työskentelevät asiantuntijat sekä kyberhäiriön teknisestä käsittelystä kiinnostuneet henkilöt. Uhkatiedon käsittelyn osalta avattiin sitä, miten kyberuhkatietoa käsitellään tiedonjakoverkostossa. Tätä on havainnollistettu kuviossa 10.



Kuvio 10. Kyberuhkatietojen käsittely tiedonjakoverkostossa (Vertainen ym. 2021, 34)

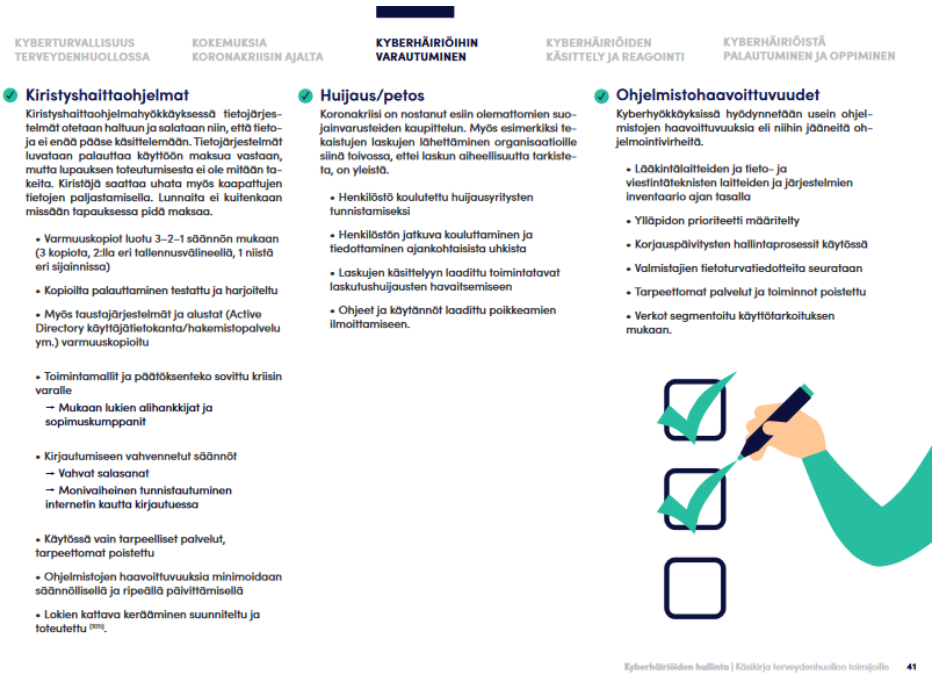
Myös **terveydenhuollon tietojärjestelmät** nähtiin tärkeänä aiheena nostaa käsikirjassa esiin. Moninainen, laaja ja monimutkainen terveydenhuollon organisaatioiden tietojärjestelmäkanta nousi monessa tilannekartoituskeskustelussa esiin kyberturvallisuudesta puhuttaessa. Kartoituksissa nousi esiin muun muassa se, että sairaalan kokoisessa organisaatiossa on haasteita sen kanssa, löytyykö organisaatiosta ketään, kuka tietäisi kaikki organisaation käytössä olevat järjestelmät ja päivittäisi tietoja niiden osalta. Lisäksi monessa aikaisemmassa tutkimuksessa ja raportissa käsiteltiin terveydenhuollon monimutkaista tietojärjestelmäarkkitehtuuria järjestelmähäiriöihin ja kyberturvallisuuteen liittyen.

Kyberhäiriöihin varautumiseen liittyen on tärkeää, että terveydenhuollon tietojärjestelmäarkkitehtuuri on suunniteltu hyvin. Tietojärjestelmäarkkitehtuurilla tarkoitetaan kuvausta organisaation tai toimialan keskeisistä tietojärjestelmistä, niiden keskinäisistä suhteista ja ominaisuuksista. Esimerkkejä sairaalan kriittisistä tietojärjestelmistä on kuviossa 11.

Kuvio 11. Sairaalan kriittisiä järjestelmiä (Vertainen ym. 2021, 36)

Myös tietojärjestelmät ja tilannetietoisuus ovat tärkeä osa aihetta. Organisaation tietojärjestelmistä, niiden kriittisyydestä ja järjestelmien välisistä riippuvuussuhteista tulee pitää kirjaa ja arvioida, mitkä ovat kunkin järjestelmän riskit, miten järjestelmät vaikuttavat toisiinsa sekä mitä tapahtuu, jos jokin näistä ei enää toimi (Vertainen ym. 2021, 37). Tietojärjestelmien kriittisyysluokittelu on olennainen osa häiriöihin varautumista ja kokonaiskuvan hahmottamista, joten myös se käsiteltiin osiossa. Tekninen jäljitettävyys nostettiin esiin, sillä lokit eli organisaation järjestelmistä kerättävät tapahtumatiedot (joista nähdään esimerkiksi, milloin ja kuka on kirjautunut tietojärjestelmään ja mitä tietoja on muutettu) ovat hyödyksi häiriötilanteiden selvittämisessä. Niiden seuranta auttaa tilanteen ymmärtämisessä, mutta myös korjaustoimenpiteissä ja häiriötilanteista palautumisessa. (Vertainen ym. 2021, 37.)

Kyberhäiriöihin varautuminen -pääkappale päättyi **kyberhäiriöihin varautumisen tarkistuslistaan**. Tarkistuslistaan koottiin keinoja ennakoida terveydenhuoltoon kohdistuvia, erityisesti kriisin aikana esiin nousseita yleisimpiä uhkia ja häiriöitä (Vertainen ym. 2021, 37). Ote tarkistuslistasta on kuviossa 12.



KYBERTURVALLISUUS TERVEYDENHUOLLOSSA | KOKEMUKSIA KORONAKRIISIN AJALTA | **KYBERHÄIRIÖIHIN VARAUTUMINEN** | KYBERHÄIRIÖIDEN KÄSITTELY JA REAGOINTI | KYBERHÄIRIÖISTÄ PALAUTUMINEN JA OPPIMINEN

Kiristyshaittaohjelmat

Kiristyshaittaohjelmahyökkäyksessä tietojärjestelmät otetaan haltuun ja salataan niin, että tieto- ja ei enää pääse käsittelemään. Tietojärjestelmät luvataan palauttaa käyttöön maksua vastaan, mutta lupauksen toteutumisesta ei ole mitään takeita. Kiristäjä saattaa uhata myös kaapattujen tietojen paljastamisella. Lunnaita ei kuitenkaan missään tapauksessa pidä maksaa.

- Varmuuskopiot luotu 3–2–1 säännön mukaan (3 kopiota, 2:lla eri tallennusvälineellä, 1 niistä eri sijainnissa)
- Kopioilta palauttaminen testattu ja harjoiteltu
- Myös taustajärjestelmät ja alustat (Active Directory käyttäjätietokanta/hakemistopalvelu ym.) varmuuskopioitu
- Toimintamallit ja päätöksenteko sovittu kriisin varalle
  - → Mukaan lukien alihankkijat ja sopimuskumppanit
- Kirjautumiseen vahvennetut säännöt
  - → Vahvat salasanat
  - → Monivaiheinen tunnistautuminen internetin kautta kirjautuessa
- Käytössä vain tarpeelliset palvelut, tarpeettomat poistettu
- Ohjelmistojen haavoittuvuuksia minimoidaan säännöllisellä ja ripeällä päivittämisellä
- Lokien kattava kerääminen suunniteltu ja toteutettu [105].

Huijaus/petos

Koronakriisi on nostanut esiin olemattomien suojainvarusteiden kaupittelun. Myös esimerkiksi tekaistujen laskujen lähettäminen organisaatioille siinä toivossa, ettei laskun aiheellisuutta tarkisteta, on yleistä.

- Henkilöstö koulutettu huijausyritysten tunnistamiseksi
- Henkilöstön jatkuva kouluttaminen ja tiedottaminen ajankohtaisista uhkista
- Laskujen käsittelyyn laadittu toimintatavat laskutushuijausten havaitsemiseen
- Ohjeet ja käytännöt laadittu poikkeamien ilmoittamiseen.

Ohjelmistohaavoittuvuudet

Kyberhyökkäyksissä hyödynnetään usein ohjelmistojen haavoittuvuuksia eli niihin jääneitä ohjelmointivirheitä.

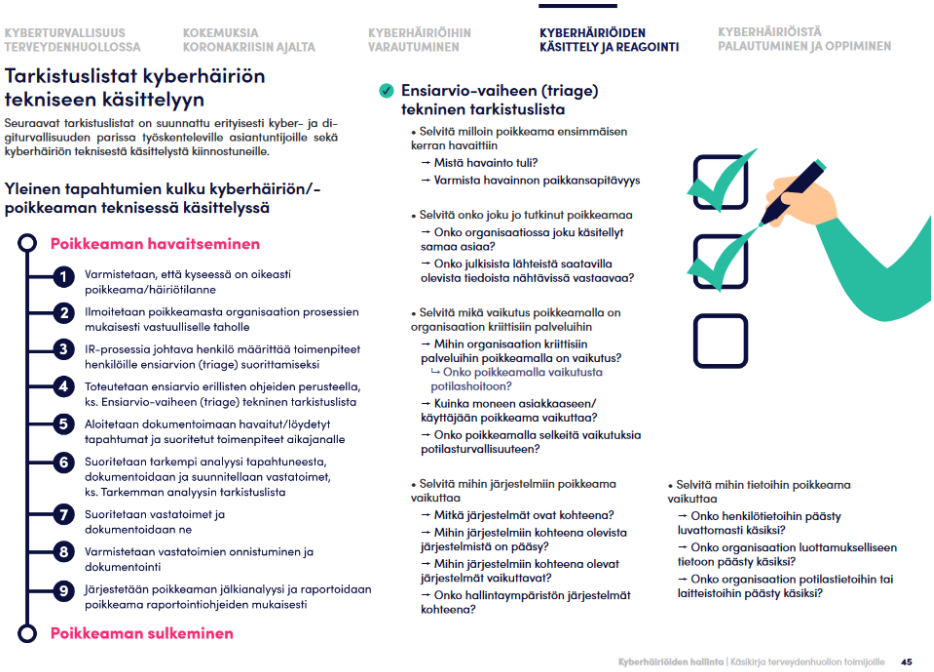
- Lääkintälaitteiden ja tieto- ja viestintäteknisten laitteiden ja järjestelmien inventaario ajan tasalla
- Ylläpidon prioriteetti määritelty
- Korjauspäivitysten hallintaprosessit käytössä
- Valmistajien tietoturvatiedotteita seurataan
- Tarpeettomat palvelut ja toiminnot poistettu
- Verkot segmentoitu käyttötarkoituksen mukaan.

Kuvio 12. Ote kyberhäiriöihin varautumisen tarkistuslistasta (Vertainen ym. 2021, 41)

5.1.3 Kyberhäiriöiden käsittely ja reagointi

Kyberhäiriöön varautuminen ei välttämättä riitä estämään kaikkia häiriö- tai poikkeamatilanteita esimerkiksi silloin, kun sairaalaan tai terveydenhuollon organisaatioon kohdistetaan hyökkäys kyvykkään uhkatoimijan toimesta (Vertainen ym. 2021, 41). Tällöin kyberhäiriöön reagointi on tärkeää. Tilannekartoituspalavereissa nousi esiin käytännön keinojen tarve reagointiin liittyen. Aiheesta käytiin myös paljon yhteiskunnallista keskustelua ja uutisoitiin laajasti psykoterapiakeskukseen kohdistuneen tietomurron seurauksena. Kyberhäiriötilanteiden käsittely on käsikirjassa jaettu osa-alueisiin, joita ovat valmistautuminen, vaste ja ensiarvio, eristäminen ja palautuminen sekä jälkianalyysi (Vertainen ym. 2021, 41). Kappaleessa käytiin läpi myös tilannekuva tapahtumasta, vastetoiminnan ja reagoinnin prosessi sekä huomioita ja suosituksia IR-prosessiin. Osio sisältää kattavan **tarkistuslistan kyberhäiriön tekniseen käsittelyyn** liittyen. Tarkistuslistan sisällön teknisemmän näkökulman vuoksi osion lukijakunnaksi määriteltiin erityisesti kyber- ja digiturvallisuuden parissa työskentelevät asiantuntijat sekä kyberhäiriön teknisestä käsittelystä kiinnostuneet henkilöt. Kuviossa 13 on ote tarkistuslistasta, jossa näkyy tapahtumien yleinen kulku ky-

berhäiriön ja -poikkeaman teknisessä käsittelyssä sekä ensiarviovaiheen tekninen tarkistuslista. Kuten varautuminen niin reagointikin tulee suunnitella ennakkoon ja harjoitella ennen kuin tilanteeseen joudutaan. Tätä painotetaan myös käsikirjassa.

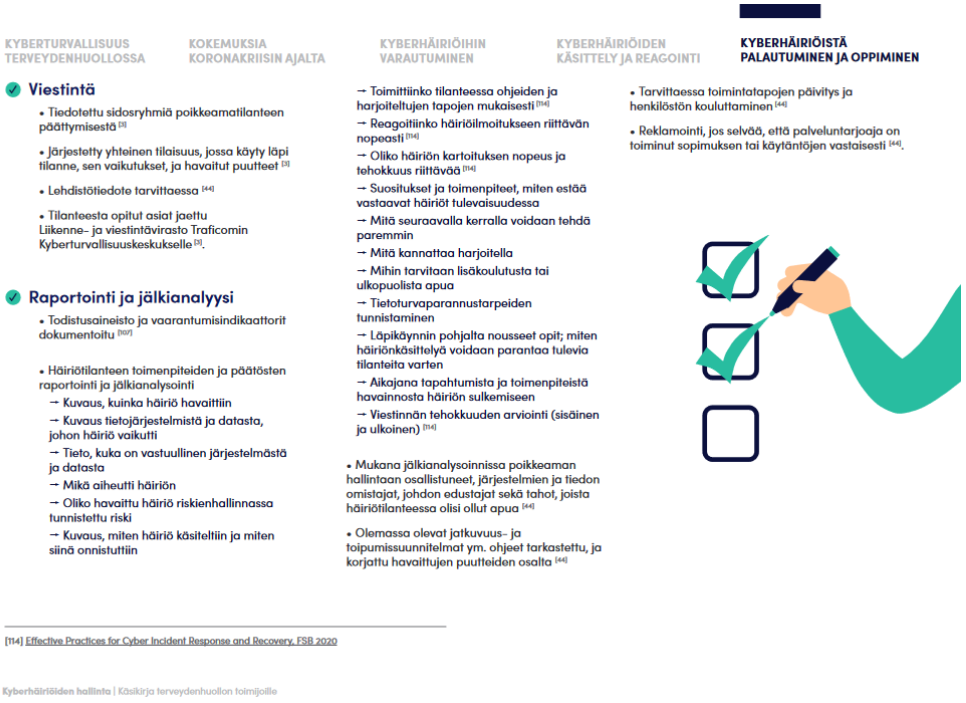


Kuvio 13. Ote tarkistuslistasta kyberhäiriön tekniseen käsittelyyn liittyen (Vertainen ja muut 2021, 45)

5.1.4 Kyberhäiriöistä palautuminen ja oppiminen

Alustava kyberhäiriöstä palautuminen on aloitettava jo silloin, kun havaittua häiriötä epäillään kyberhäiriöksi. Tämä saattaa tarkoittaa esimerkiksi varajärjestelmän ottamista käyttöön. Lähtökohtana on turvata toiminnan jatkuvuus sekä tietojen luottamuksellisuus ja eheys. (Vertainen ym. 2021, 45.) Opit kyberhyökkäyksestä on syytä ottaa talteen, jotta vastaavalta vältytään tulevaisuudessa. Tämän vuoksi kappaleessa käsiteltiin dokumentointi ja jälkianalyysi omina osioinaan. Dokumentoinnin tärkeys nousi esiin useamman yhteistyökumppanin nostamana tilannekartoituspalavereissa. Lisäksi kappale sisältää tietoa järjestelmien ja prosessien toipumissuunnitelmista. Osio päättyy **häiriöistä palautumisen tarkistuslistaan**, joka sisältää toipumisessa,

viestinnässä, raportoinnissa ja jälkianalyysissä huomioitavia asioita. Ote tästä tarkistuslistasta kuviossa 14.



KYBERTURVALLISUUS TERVEYDENHUOLLOSSA | KOKEMUKSIA KORONAKRIISIN AJALTA | KYBERHÄIRIÖIHIN VARAUTUMINEN | KYBERHÄIRIÖIDEN KÄSITTELY JA REAGOINTI | **KYBERHÄIRIÖISTÄ PALAUTUMINEN JA OPPIMINEN**

Viestintä

- Tiedotettu sidosryhmiä poikkeamatilanteen päättymisestä [3]
- Järjestetty yhteinen tilaisuus, jossa käyty läpi tilanne, sen vaikutukset, ja havaitut puutteet [3]
- Lehdistötiedote tarvittaessa [44]
- Tilanteesta opitut asiat jaettu Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle [3].

Raportointi ja jälkianalyysi

- Todistusaineisto ja vaarantumisindikaattorit dokumentoitu [107]
- Häiriötilanteen toimenpiteiden ja päätösten raportointi ja jälkianalysointi
  - → Kuvaus, kuinka häiriö havaittiin
  - → Kuvaus tietojärjestelmistä ja datasta, johon häiriö vaikutti
  - → Tieto, kuka on vastuullinen järjestelmästä ja datasta
  - → Mikä aiheutti häiriön
  - → Oliko havaittu häiriö riskienhallinnassa tunnistettu riski
  - → Kuvaus, miten häiriö käsiteltiin ja miten siinä onnistuttiin

- → Toimittiinko tilanteessa ohjeiden ja harjoiteltujen tapojen mukaisesti [114]
- → Reagoitiinko häiriöilmoitukseen riittävän nopeasti [114]
- → Oliko häiriön kartoituksen nopeus ja tehokkuus riittävää [114]
- → Suositukset ja toimenpiteet, miten estää vastaavat häiriöt tulevaisuudessa
- → Mitä seuraavalla kerralla voidaan tehdä paremmin
- → Mitä kannattaa harjoitella
- → Mihin tarvitaan lisäkoulutusta tai ulkopuolista apua
- → Tietoturvaparannustarpeiden tunnistaminen
- → Läpikäynnin pohjalta nousseet opit; miten häiriönkäsittelyä voidaan parantaa tulevia tilanteita varten
- → Aikajana tapahtumista ja toimenpiteistä havainnosta häiriön sulkemiseen
- → Viestinnän tehokkuuden arviointi (sisäinen ja ulkoinen) [114]

- Mukana jälkianalysoinnissa poikkeaman hallintaan osallistuneet, järjestelmien ja tiedon omistajat, johdon edustajat sekä tahot, joista häiriötilanteessa olisi ollut apua [44]
- Olemassa olevat jatkuvuus- ja toipumissuunnitelmat ym. ohjeet tarkastettu, ja korjattu havaittujen puutteiden osalta [44]

- Tarvittaessa toimintatapojen päivitys ja henkilöstön kouluttaminen [44]
- Reklamointi, jos selvää, että palveluntarjoaja on toiminut sopimuksen tai käytäntöjen vastaisesti [44].

[114] Effective Practices for Cyber Incident Response and Recovery, FSB 2020

54 Kyberhäiriöiden hallinta | Käsikirja terveydenhuollon toimijoille

Kuvio 14. Ote häiriöstä palautumisen tarkistuslistasta (Vertainen ja muut 2021, 54)

5.2 Tuotoksesta saatu palaute

Yhteistyökumppaneilta kerättiin projektin lopussa palaute Webropol-kyselyohjelmiston kautta. Palautekysely lähetettiin tilannekartoituksiin osallistuneille seitsemälle organisaatiolle ja siihen vastasi kolmen organisaation edustajat. Kyselyaineistoa käsiteltiin luottamuksellisesti projektin sisällä ja se on arkistoitu asianmukaisesti. Jälkikäteen pyydettiin erikseen lupa käyttää koostetta anonyymeistä palautteista tässä työssä. Kyselylomakkeen pohja löytyy työn liitteistä (ks. liite 2). Asteikkona kyselyssä oli: 1 täysin eri mieltä, 2 jokseenkin eri mieltä, 3 ei eri, eikä samaa mieltä, 4 jokseenkin samaa mieltä ja 5 täysin samaa mieltä. Seuraavaksi esitellään kyselyaineiston perusteella tehdyt johtopäätökset ja keskiarvot tuloksista.

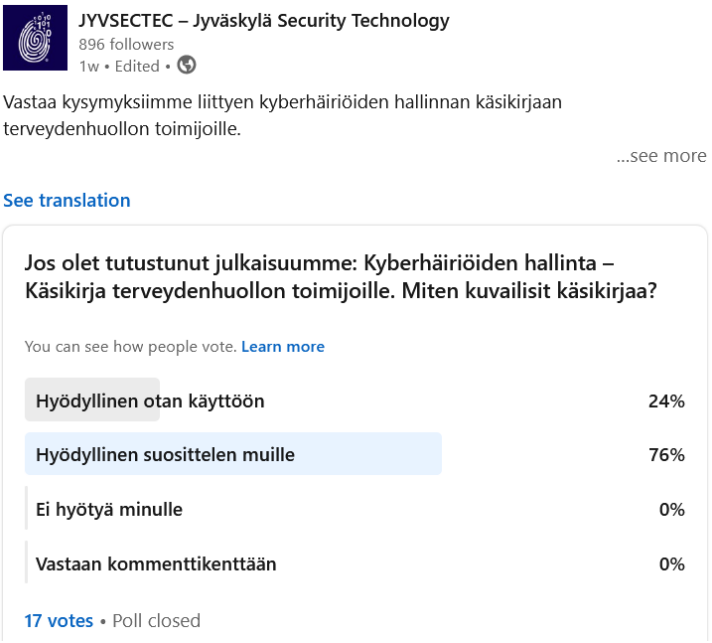
Vastaajat kokivat, että projektin toteuttaja kertoi selkeästi projektin tavoitteista (5,0) ja, että he saivat riittävästi tietoa projektin etenemisestä (4,7). Yhteistyön sujuvuuteen oltiin tyytyväisiä (4,7) ja yhteistyö nähtiin melko hyödyllisenä (4,3). Vastaajat haluavat tehdä yhteistyötä JAMKin kanssa myös tulevaisuudessa (5,0). Omaa osallistumista arvioitiin seuraavasti: osallistuin projektiin niin aktiivisesti kuin olin ennakkoon suunnitellut (3,7), projektin toteuttaja tarjosi riittävästi mahdollisuuksia osallistua projektiin (4,7) ja mahdollisuuksia vaikuttaa projektin tuloksiin (4,7). Yksi vastaajista lisäsi, että valitettavasti ei pystynyt juurikaan osallistumaan alkua pidemmälle, eli välivaiheen osiot jäivät häneltä pois töiden aiheuttaman kiireen vuoksi. Alkuhaastattelu ja tiedon keräämisen vaihe olivat kuitenkin hänen mielestään onnistuneita.

Projektin tuotoksena syntyneestä käsikirjasta nähtiin olevan hyötyä terveydenhuollolle (5,0) ja siihen oltiin melko tyytyväisiä (4,3). Vastaajille annettiin myös mahdollisuus kertoa ajatuksiaan käsikirjasta. Yksi vastaaja piti käsikirjaa hyvänä, mutta olisi halunnut, että käsikirjan kaikki tekninen sisältö olisi aukikirjoitettu ei-teknisille lukijoille (käsikirjassa oli kaksi teknisempää osiota, joiden alussa kohderyhmä oli määritelty). Toinen vastaaja sanoi, että käsikirjaan on koostettu hyvin käsitteistöä, perusperiaatteita ja toimintamalleja, joilla pääsee aloittamaan toiminnalle sopivan mallin mietintää ja rakentamista. Ehdotuksena jatkoa ajatellen yksi vastaajista mainitsi, että vastaavia oppaita voisi kirjoittaa muillekin toimialoille (mm. vesihuoltoon ja logistiikkasektorille). Lisäksi yksi vastaajista toivoi vielä pidemmälle vietyjä malleja mm. kriittisyyden arviointiin, viestintäohjeisiin ja riskimatriisiin.

Sisältöpalautteiden lisäksi käsikirjan visuaalisuus on saanut yhteistyökumppaneilta sekä muilta viranomaisilta vapaamuotoista hyvää palautetta. Etenkin laadukasta ja ammattimaista taittoa sekä nokkelia kuvituskuvia on kehuttu. Kuviossa 15 näkyy taiton tyyliä ja yksi kuvituskuvista esimerkkinä.

Kuvio 15. Kuva havainnolistamaan taittoa ja visuaalista ilmettä (Vertainen ja muut 2021, 16)

Kolme viikkoa käsikirjan julkaisun jälkeen JYVSECTECin LinkedIn-tilin kautta tehtiin julkaisu, jossa käsikirjaan tutustuneita pyydettiin kertomaan, onko käsikirja vastaajalle hyödyllinen ja aikooko hän ottaa sen käyttöön, onko se hyödyllinen ja hän suosittelee sitä muille vai onko hän sitä mieltä, että käsikirjasta ei ole hänelle hyötyä. Annettiin myös vaihtoehto omin sanoin kommentoida ajatuksia käsikirjasta julkaisun alle. Julkaisuun sai vastata viikon ajan. 17 ihmistä vastasi julkaisun kyselyyn ja heistä 24 % koki käsikirjan hyödylliseksi ja aikoo ottaa sen käyttöön. Loput 76 % koki, että käsikirja on hyödyllinen ja he suosittelevat sitä muille. Kuviossa 16 on nähtävissä tämän julkisen kyselyn tulokset.



Kuvio 16. LinkedIn-kyselyn tulokset

Sairaanhoitopiirien edustajien ja eri viranomaisten kautta sekä toteuttajaorganisaation sisältä saatu vapaamuotoinen palaute on ollut erittäin positiivista. On muun muassa nähty, että ajankohtaiseen tarpeeseen on kyetty vastaamaan hyvin. Lisäksi on koettu, että käsikirja on napakka tietopaketti siitä, mitä kaikenkokoiset toimialan organisaatiot voivat tehdä kyber- ja digiturvallisuutensa parantamiseksi. Käsikirjan kokonaisuutta kehuttiin. Nähtiin, että käsikirja on toteutettu erityisesti terveydenhuollon tarpeisiin, mutta sisältävän myös tärkeitä yleisesti huomioitavia asioita muidenkin alojen näkökulmasta.

6 Yhteenveto

Häiriöherkkyytensä sekä koronakriisin aiheuttaman tiukan resurssitilanteen vuoksi terveydenhuolto on erityisen haavoittuvainen kyberhäiriöille sekä kaikille toiminnan häiriöille. Terveydenhuollon organisaatioiden on nyt erittäin tärkeää varautua kyberhäiriöihin ja suunnitella reagoinnin sekä palautumisen prosessit huolellisesti. On

myös huomioitava mitä uudenlaisia uhkavektoreita koronakriisi on synnyttänyt. Resurssien ollessa terveydenhuollossa tiukoilla on helposti käytäntöön vietäville prosesseille, ohjeille, vinkeille ja tarkistuslistoille suuri tarve. Tämä selvisi tilannekartoituspalavereista. Lisäksi selvisi, että prosessit ja ohjeistukset olisi hyvä aukikirjoittaa niin, että ne ovat muidenkin kuin teknisimpien asiantuntijoiden hyödynnettävissä. Täten tietoisuus kyberturvallisuusasioista lisääntyy laajemmin organisaatioissa.

6.1 Vastaus tutkimuskysymykseen

Konstruktiivisessa tutkimusotteessa pyritään ratkaisemaan reaalimaailman ongelmia (Lukka n.d). Tämän työn lähtökohtana oli reaalimaailman ongelma, joka puettiin tutkimuskysymykseksi muotoon, **miten terveydenhuollon organisaatioissa tulee varautua kyberhäiriöihin sekä reagoida ja palautua niistä?** Tätä täsmennettiin vielä alakysymyksellä, **mitä uudentyyppisiä kyberuhkia koronakriisi on aiheuttanut terveydenhuoltoalalle?** Tutkimuskysymyksiin vastattiin kehittämällä laaja (60-sivuinen) käsikirja kyberhäiriöiden hallintaan terveydenhuollon toimijoille. Käsikirja syntyi työssä kuvatun kehittämisprosessin mukaisesti. Projektin ja tämän työn tavoitteisiin sekä tilannekartoituksessa selvinneisiin tarpeisiin pystyttiin lopputuotoksen osalta vastaamaan erittäin hyvin. Käsikirja on kattava, mutta myös napakka tietopaketti siitä, mitä terveydenhuollon organisaatiot voivat tehdä kyber- ja digiturvallisuutensa parantamiseksi. Lukija johdatetaan tiedon ja erilaisten ratkaisumallien lähteille. Erityisesti viime vuoden aikana kyberrikollisuus on suuntautunut huomattavassa määrin terveydenhuollon toimijoihin, mikä osaltaan lisää tarvetta ja kiinnostusta käsikirjaan.

Prosessissa oli vahvasti konstruktiivinen ote. Konstruktiolla, kuten tämänkin työn lopputuloksena syntyneellä käsikirjalla, on loputon määrä mahdollisia toteutumia. Niille tunnusomaista on se, että ne keksitään ja kehitetään eli niitä ei ole mistään löydetty. Kehittämällä kaikesta jo olemassa olevasta poikkeava konstruktio, kehitetään uutta todellisuutta. (Lukka n.d.) Konstruktiivisen tutkimusprosessin mukaisesti työtä tehtiin läheisessä yhteistyössä käytännön edustajien (yhteistyökumppaneiden) kanssa sekä tiimin kesken. Näihin seikkoihin perustuen voidaan todeta, että tähän laadullisen tutkimukseen sopi hyvin konstruktiivinen tutkimusote.

Konstruktiivisen tutkimuksessa tutkija on itse tekemässä uutta konstruktiota omaan ongelmaansa, kuten tässä tutkija eli projektin projektipäällikkö. Tutkimuksessa oli tarkkaan pohdittava sitä, miten työn lopputuotoksena syntynyt käsikirja olisi mahdollisimman puolueeton ja riippumaton projektipäällikön henkilökohtaisesta näkemyksestä tai asenteesta. Asia huomioitiin tutkimuksessa siten, että projektipäällikön lisäksi tuotoksen tekoon osallistuivat projektiasiantuntija sekä neljä muuta asiantuntijaa, jotka oman kirjoitustyönsä lisäksi lukivat ja kommentoivat tuotosta. Aihesisällöt tuotokseen valikoituivat pääosin yhteistyökumppaneiden kanssa käydyistä tilannekartoituspalavereista. Lisäksi projektipäällikkö ja -asiantuntija seurasivat aihealueen ajankohtaisia webinaareja ja asiantuntijaluentoja. Niistä tehtyjen muistiinpanojen ja huomioiden perusteella arvioitiin, onko aihe tärkeä nimenomaan Suomen terveydenhuollossa. Yhteistyökumppaneille annettiin mahdollisuus kommentoida projektipäällikön ja asiantuntijan kokoamaa sisällysluetteloehdotusta. Lisäksi asiantuntijaverkostolla oli mahdollisuus kommentoida lähes valmista käsikirjaa. Kommentit, ideat ja muutosehdotukset huomioitiin tuotoksessa. Näiden seikkojen kautta pyrittiin varmistamaan käsikirjan objektiivisuus.

6.2 Tulosten ja tietoperustan välinen suhde

Kirjallisuuskatsaus tuki tutkimuksen tuloksia. Tutkimuksen tulosten ja tietoperustan välistä suhdetta tarkastellessa voidaan nostaa esiin seuraavia asioita. Käsikirjan pääkappaleessa **Kokemuksia koronakriisin ajalta** käsiteltiin lisääntyneen etätyön vaikutuksia terveydenhuollossa (kyberturvallisuuden näkökulmasta). Tämä haaste nousi esiin myös kirjallisuuskatsauksen luvussa 3.1 Williamsin ja muiden (2020) nostamana.

Käsikirjan pääkappaleessa **Kyberhäiriöihin varautuminen** käsiteltiin tärkeää aihetta, kyberturvallisuuteen liittyvän tilannetiedon jakamista. Aihe nousi esiin yhteistyökumppaneiden kanssa käydyissä tilannekartoituksissa. Myös kirjallisuuskatsauksen luvussa 3.2 Argaw ja muut (2020) painottivat, että tiedon jakaminen helpottaa tilannetietoisuutta, ymmärrystä uhista ja uhkatoimijoista sekä heidän motivaatioistaan, kampanjoistaan, taktiikoistaan ja tekniikoistaan. Näin ollen se antaa päättäjille paremman käsityksen organisaation riskienhallintapolitiikkojen soveltamisesta. Samoin

Papastergious ja muut (2020) korostivat, että haitallisen toiminnan tunnistetietojen välittämistä voidaan pitää kyberuhkatiedustelun tärkeimpänä ytimenä.

Kyberhäiriöihin varautuminen pääkappaleessa käsiteltiin terveydenhuollon tietojärjestelmät. Aihe nousi eri näkökulmista esiin useamman kerran tilannekartoituspalavereissa. Myös kirjallisuuskatsauksen luvussa 3.2 Argaw ja muut (2020) korostivat, että terveydenhuollon organisaatioiden tietojärjestelmien on oltava laadukkaita sekä sovelluskannan ja IT-infrastruktuurin vakaata, jotta tietoturvan tason on riittävä.

Gyunkan ja Christianan (2017, 10) mukaan hyökkääjät hyödyntävät tehokkaasti Ihmisen manipulointiin suunniteltuja hyökkäystekniikoita. Tutkimuksen tulokset paljastivat, että inhimilliset tekijät ovat syynä 95 prosentissa kaikista kyberhäiriötapauksista. **Kyberhäiriöihin varautuminen** kappaleeseen nostettiin tämä sama aihe eli kyberturvallisuusosaamisen kehittäminen ja tietoisuuden lisääminen mukaan käsikirjaan. Aihetta käsiteltiin tilannekartoituspalavereissa, Enisan webinaarissa (23.9.2020) ja Kyberturvallisuuden nykytilakartoituksesta eri toimialoilla.

Käsikirjassa reagointi, kuten varautuminenkin, on ennalta suunniteltua toimintaa, jota on harjoiteltu ennen, kuin tilanteeseen todellisuudessa joudutaan. Papastergious ja muut (2020) painottivat myös kirjallisuuskatsauksen luvussa 3.2. proaktiivista valmistautumista ja reaktiivista oppimista.

Kirjallisuuskatsauksen luvussa 3.2 mainitaan, että kyberhäiriöstä palautumisvaiheessa on erittäin tärkeää dokumentoida tarkasti häiriön vaiheet liittyen muun muassa sen rajaamiseen. Tulee myös dokumentoida kaikki siihen liittyvä todistusaineisto sekä vaarantumisindikaattorit. Näin ymmärretään tapahtunutta ja estetään vastaavanlaisten tilanteiden syntyminen tulevaisuudessa. (JYVSECTEC PHR-model 2020.) Dokumentointi ja jälkianalyysi nostettiin myös esiin käsikirjan pääkappaleessa **Kyberhäiriöistä palautuminen ja oppiminen**.

6.3 Tulosten hyödyt ja yhteiskunnalliset vaikutukset

Projektin käsikirja voi lisätä liiketoimintaa terveydenhuollon kyberturvallisuuteen liittyen. Käsikirja on aiheen parissa liiketoimintaa suunnittelevien ja tekevien yritysten ja organisaatioiden avoimesti hyödynnettävissä. Käsikirjaa voidaan käyttää yritysten ja organisaatioiden palveluliiketoiminnan tuotteissa. Teos on myös projektin kumppaniorganisaatioiden terveydenhuollon kyberturvallisuuteen liittyvän liiketoiminnan hyödynnettävissä.

Lisäksi käsikirja on eri kokoisten Suomen terveydenhuollon organisaatioiden hyödynnettävissä kyberhäiriöiden prosessien ja toimintaohjeiden kehitystyön osalta. Käsikirjan merkitys käytännönläheisenä teoksena, jollaista ei aikaisemmin ole Suomen terveydenhuollon alalla julkaistu, on merkittävä. Teoksessa on huomioitu teknisten sisältöjen selittäminen lukijalle. Täten kohderyhmä on pystytty pitämään laajana, joka osaltaan auttaa tietoisuuden lisäämisessä.

Kirjoittaja oppi henkilökohtaisesti paljon terveydenhuollon alaa ohjaavista säädöksistä ja prosesseista sekä kyberturvallisuuden tilasta terveydenhuollon alalla. Lisäksi kirjoittaja oppi uutta kyberturvallisuudesta yleisesti sekä koronakriisin aiheuttamista kyberuhkista. Kirjoittaja sai kokemusta ja osaamista projektipäällikkönä toimimisesta, sillä aikaisemmin hän on toiminut TKI-projekteissa muissa tehtävissä (sisällön asiantuntijana, viestinnän ja talouden sekä hallinnollisen raportoinnin tehtävissä). Kirjoittajan ammatillinen yhteistyöverkosto laajentui projektin aikana, mikä on ammatillisesti merkittävä asia.

Käsikirjan teema muuttui psykoterapiakeskukseen kohdistetun tietomurron myötä entistä ajankohtaisemmaksi ja aiheeseen liittyen käytiin paljon yhteiskunnallista keskustelua. Moni terveydenhuollon organisaatio on herännyt miettimään kyberturvallisuutta ja tarkastelemaan prosessejaan ja toimintaohjeitaan. Uutisointi psykoterapiakeskuksen tietomurron ympärillä on mahdollisesti heikentänyt kansalaisten luottamusta sosiaali- ja terveydenhuollon palveluihin muun muassa henkilötietojen turvallisen käsittelyn osalta. Tämän vuoksi on erittäin tärkeää tuoda käsikirjaa esiin,

jotta pystytään näyttämään, että tukea alan organisaatioille on tarjolla ja kyberturvallisuuden eteen tehdään töitä monella sektorilla. Tämä voidaan nähdä työn yhteiskunnallisena vaikutuksena.

Mikäli käsikirjan prosessien ja ohjeiden avulla yksikin terveydenhuollon organisaatio välttäisi kyberhyökkäyksen, voitaisiin ajatella, että työllä on ollut merkittävä hyöty potilasturvallisuuden näkökulmasta. Työllä olisi myös merkittävä rooli, mikäli yksikin terveydenhuollon organisaatio pystyisi palautumaan kyberhäiriöstä nopeammin käsikirjan sisältämien ohjeiden avulla. Käsikirjan hyödyllisyys korostuu huomioiden, että terveydenhuollon organisaation joutuessa kyberhyökkäyksen kohteeksi vaikutukset voivat olla hyvin laajoja, koskien muun muassa potilasturvallisuutta, organisaation mainetta, taloutta ja toimintakykyä. Käsikirjalla pyritään osaltaan vaikuttamaan Suomen kansalliseen kyberresilienssiin.

6.4 Toimeksiantajan saamat hyödyt

Työn toimeksiantaja JYVSECTEC hyötyy tämän työn tuloksena syntyneestä käsikirjasta profiloituen entistä vahvemmin terveydenhuollon kyberturvallisuuteen. Käsikirja on lisäksi JYVSECTECin Healthcare Cyber Range -hankkeen hyödynnettävissä muun muassa sen tulevassa kyberturvallisuusharjoituksessa. Lisäksi toimeksiantaja voi hyödyntää käsikirjaa muissakin kyberturvallisuusharjoituksissaan. Toimeksiantaja voi myös myydä käsikirjaan pohjautuvia palveluliiketoiminnan koulutustuotteita.

Toimeksiantaja voi tulevaisuudessa hyötyä uusien TKI-projektien muodossa käsikirjasta, sillä sen kautta on syntynyt idea tehdä muillekin huoltovarmuuskriittisille aloille vastaavia tuotoksia. Yhden kumppanin kanssa on lisäksi syntynyt suunnitelmia liittyen uuteen yhteistyömahdollisuuteen tutkimus- ja kehitystoiminnan saralla. Yhteistyö projektin kumppaneiden kanssa oli erittäin hyödyllistä toimeksiantajan näkökulmasta.

Tieto käsikirjasta on levinnyt laajasti sosiaalisen median kampanjoinnin avulla, jossa Jyväskylän ammattikorkeakoulun ja JYVSECTECin lisäksi yhteistyökumppanit ja yksi-

tyishenkilöt aktivoituivat jakamaan tietoa asiasta. Verkostoyhteistyö käsikirjan viestinnässä on ollut erittäin hyvää. Käsikirjaan liittyvä viestintä kokonaisuudessaan on lisännyt toimeksiantajan näkyvyyttä.

6.5 Haasteet ja kehittämisehdotukset

Mikäli projekti olisi kestänyt pidempään kuin kuusi kuukautta, olisi siinä ollut mahdollisuus vielä tarkempaan tutkimustyöhön ja laajempien kyberhäiriöihin liittyvien mallien luomiseen terveydenhuollolle. Koronakriisi myös aiheutti sen, että yhteistyökumppanit olivat melko kiireisiä. Lisäksi osalla heistä oli muitakin työkuormaa lisääviä tekijöitä, kuten psykoterapiakeskukseen kohdistunut tietomurto, koronavilkku-sovelluksen julkaisu ja kehitys sekä keskussairaalan muutto. Mikäli yhteistyökumppanit eivät olisi olleet niin kiireisiä, he olisivat ehkä voineet osallistua myös käsikirjan sisältöjen tuottamiseen yhdessä toteuttajaorganisaation kanssa sekä laajempaan sisältöjen kommentointiin. Pidempi projekti olisi myös mahdollistanut esimerkiksi kyselytutkimusten teon prosessien ja ohjeiden tarpeista laajalle joukolle kohderyhmää. Koronakriisin vallitessa tämä olisi kuitenkin ollut haastavaa resurssien ollessa tiukilla. Tarkkoja terveydenhuollon organisaatioiden olemassa olevia kyberhäiriöiden hallinnan prosesseja ja toimintaohjeita ei ollut julkisesti saatavilla, mikä myös aiheutti haasteita aiheeseen perehtymisessä.

6.6 Mahdollisia jatkotutkimusaiheita

Jatkotutkimusaihe työlle on, että vastaavia kyberhäiriöiden hallinnan prosessien ja toimintaohjeiden kehitysprojekteja voisi toteuttaa myös muille huoltokriittisille aloille. Tämä jatkotoimenpide-ehdotus tuli yhteistyökumppanilta palautekyselyn vastauksena. Lisäksi Huoltovarmuuskeskuksen yhteistyössä Digipoolin ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen kanssa tekemän **Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot** julkaisun perusteella media-ala, elintarvikeala ja logistiikka voivat hyötyä vastaavantyyppisestä kehitysprojektista, sillä nämä alat jäivät kypsyystasoltaan alhaisimmiksi kartoituksessa. (Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot 2020, 8.)

Toinen jatkotutkimusaihe on, että tiettyjen käsikirjan aihealueiden osalta toteutetaan yksityiskohtainen malli tai ohje. Tämä nousi jatkotoimenpide-ehdotuksena palautekyselyssä ja lisäksi samaa aihetta käsiteltiin kahden eri kumppanin kanssa käydyssä sähköpostikeskustelussa. Kumppaneiden kanssa mietittiin, että aihealueen parissa riittäisi töitä niin paljon, kun tekijöitä on. Etenkin julkisella sektorilla hyödyttäisiin ohjeista, sillä ohjeiden laatimista varten joudutaan usein palkkaamaan ulkopuolisia tekijöitä. Esimerkkinä voidaan mainita viestintä. Kehitetään tarkka malli, miten terveydenhuollon organisaation tulee toimia jouduttuaan tietomurron kohteeksi. Malli voi sisältää tarkat kuvaukset siitä, miten organisaation tulee kommunikoida rikollisen toimijan, median, viranomaisten ja muiden organisaatioiden kanssa. Toisena tarkemman mallin esimerkkinä voi olla työkalu (kuten tietojärjestelmä) terveydenhuollon tietojärjestelmien kriittisyysluokittelun tekemiseen. Tilannekartoituksen perusteella tietojärjestelmien kriittisuusluokittelun tukena on tällä hetkellä käytössä Excel-pohjainen malli.

Kolmas jatkotutkimusaihe on toteuttaa vastaavantyyppinen käsikirja jollekin toiselle maalle tai yleisempi teos englanniksi, mikä on laajemmin eri maiden hyödynnettävissä. Euroopan näkökulmasta samantyyppinen teos olisi hyvä tehdä yhteistyössä Euroopan unionin verkko- ja tietoturvavirasto ENISA:n kanssa.

Liikenne- ja viestintäministeriö asetti ajalle 9.11.2020 – 31.1.2021 työryhmän selvittämään tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla. Alat, joiden osalta selvitystä tehtiin, olivat terveydenhuolto, energiahuolto, vesihuolto, liikenne, rahoitusala ja digitaalinen infrastruktuuri. Selvitystyön motivaationa oli loppuvuodesta 2020 ilmi tullut psykoterapiakeskukseen kohdistettu tietomurto. Työryhmän loppuraportissa esitetään lainsäädännön muutostarpeita ja muita toimenpiteitä tietoturvan ja tietosuojan parantamiseksi valituilla toimialoilla. Erityisesti viranomaisten entistä tehokkaampaa ja järjestäytyneempää yhteistyötä painotetaan tuloksissa. Tätä yhteistyötä tukee ja vahvistaa kyberturvallisuuskeskus. Yhteistoiminnan merkitys nousi esiin myös tilannekartoituspalavereissa. Neljäs mahdollinen jatkotutkimusaihe on terveydenhuollon kyberturvallisuuden toimijoiden yhteistyön kehit-

täminen kansallisella tasolla. Käsikirjassa esiteltyjä kyberturvallisuuteen liittyvän uhkatiedon jakomalleja ja alustoja voi hyödyntää pohjana. (Lehtilä, Nyström, Ronikonmäki & Sirviö 2021.)

Lähteet

Argaw, ST., Troncoso-Pastoriza, JR., Lacey, D., Florin, MV., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J-M., O'Leary, C., Eshaya-Chauvin, B., Flahault, A. 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 146. Viitattu 30.12.2020. https://doi.org/10.1186/s12911-020-01161-7

Bartock, M., Cichonski, J., Souppaya, M., Smith, M., Witte, G. & Scarfone, K. 2016. Guide for Cybersecurity Event Recovery. NIST Special Publication 800-184. Viitattu 21.1.2021. https://doi.org/10.6028/NIST.SP.800-184

Biswas, R., Fidalgo, E. & Alegre, E. 2017. Recognition of Service Domains on TOR Dark Net using Perceptual Hashing and Image Classification Techniques. IET Digital Library. Viitattu 28.1.2021. http://gvis.unileon.es/wp-content/uploads/2018/09/Recognising-Illegal-Services-on-the-Dark-Net-using-Perceptual-Hashing-and-Image-Classification-Techniques_Published.pdf

Branch, L., Eller, W., Bias, T., McCawley, M., Myers, D. & Gerber, B. 2018. Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective Preparedness Perspective. West Virginia University. Viitattu 8.1.2021. https://researchrepository.wvu.edu/cgi/viewcontent.cgi?article=4749&context=etd#page=62

CYBERDI Tietojenkalastelu. N.d. Jyväskylän ammattikorkeakoulu. Viitattu 28.1.2021. https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/tietopankki/infokortit/tietojenkalastelu/

Evans, M., Maglaras, L., He Y. & Janicke. H. 2016. Human behaviour as an aspect of cybersecurityassurance. School of Computer Science and Informatics, De Montfort University, Leicester, U.K. Viitattu 15.1.2021. https://onlinelibrary.wiley.com/doi/pdf/10.1002/sec.1657

Gyunka, BA. & Christiana, AO. 2017. Analysis of Human Factors in Cyber Security: A Case Study of Anonymous Attack on Hbgary. Viitattu 18.1.2021. http://jandmparker.net/research/Analysis%20of%20Human%20Factors%20in%20Cyber%20Security%20-%20A%20Case%20Study%20of%20Anonymous%20Attack%20on%20Hbgary.pdf

Healthcare Cyber Range (HCCR). 2020. HCCR-hankkeen verkkosivut. Jyväskylän ammattikorkeakoulu. Viitattu 22.1.2021. https://jyvsectec.fi/2019/01/healthcare-cyber-range-hccr/

Hesse-Biber, S.N. & Leavy, P. 2011. The Practice of Qualitative Research. 2. p. Thousand Oaks: SAGE Publications.

Huoltovarmuuskeskus. 2021. Organisaation verkkosivut. Viitattu 24.1.2021. https://www.huoltovarmuuskeskus.fi/organisaatio/huoltovarmuuskeskus/

Huoltovarmuuskeskus. 2020. Uutisarkisto -sivusto. Viitattu 14.12.2020. https://www.huoltovarmuuskeskus.fi/terveydenhuollossa-varaudutaan-kyberuhkia-vastaan/

Huoltovarmuuskeskus Sektorit ja poolit. 2021. Organisaation verkkosivut. Viitattu 24.1.2021. https://www.huoltovarmuuskeskus.fi/organisaatio/sektorit-ja-poolit/

Huoltovarmuuskeskus Terveydenhuolto. 2021. Organisaation verkkosivut. Viitattu 24.1.2021. https://www.huoltovarmuuskeskus.fi/toimialat/terveydenhuolto/

Huusko, J. 2020. Helsingin Sanomat ulkomaat ja tietoturva -sivusto. Viitattu 14.12.2020. https://www.hs.fi/ulkomaat/art-2000006707701.html

Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. 2012. Tutkimuseettinen neuvottelukunta. Viitattu 9.1.2021. https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

Hämäläinen, V-P. & Kallunki, E. 2020. Yle uutiset. Viitattu 27.12.2020. https://yle.fi/uutiset/3-11642774

Hämäläinen, V-P & Rummukainen, A. 2020. Yksi heistä on kiristäjä. Viitattu 27.12.2020. https://yle.fi/uutiset/3-11616210

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. N.d. Digi- ja väestötietoviraston verkkosivut. Viitattu 8.2.2021. https://dvv.fi/vahti

JYVSECTEC by Jamk About Us. 2020. Jyväskylän ammattikorkeakoulu. Viitattu 11.12.2020. https://jyvsectec.fi/about

JYVSECTEC kyberharjoitus esitysdiat. N.d. Jyväskylän ammattikorkeakoulu.

JYVSECTEC PHR-model. 2020. Jyväskylän ammattikorkeakoulu. Viitattu 21.1.2021. https://github.com/JYVSECTEC/PHR-model

Kananen, J. 2017. Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylän ammattikorkeakoulu. Viitattu 21.1.2021. https://janet.finna.fi/, Booky.fi.

Kananen, J. 2015. Online research for preparing your thesis: a guide for conducting qualitative and quantitative research online. Jyväskylä: JAMK University of Applied Sciences. Viitattu 12.12.2020. https://janet.finna.fi/, Booky.fi.

Keränen, T. 2017. WannaCry-haittaohjelma löytyi TYKS:sta. Lääkärilehti. Viitattu 27.12.2020. https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/

Kruse, C., Frederick, B., Jacobson, T., & Monticone, K. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Journal of Technology and Health Care, 25, 1, 1-10. Viitattu 30.12.2020. https://content.iospress.com/articles/technology-and-health-care/thc1263

Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä. 2020. Jyväskylän ammattikorkeakoulu. Viitattu 12.12.2020. https://www.jamk.fi/fi/reportronic-project/?projectnum=101019

Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektisuunnitelma. 2020. Jyväskylän ammattikorkeakoulu.

Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot. 2020. Huoltovarmuuskeskus, Digipooli ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskus. Pohjautuu Digipoolin teettämään selvitykseen, jonka teki KPMG. Viitattu 22.1.2021. https://cdn.huoltovarmuuskeskus.fi/app/uploads/2020/10/05091400/Kyberturvallisuuden-nykytila-eri-toimialoilla.pdf

Kyberturvallisuuden tähden. 2018. Huoltovarmuuskeskus. Viitattu 21.1.2021. https://www.varmuudenvuoksi.fi/aihe/huoltovarmuus/375/kyberturvallisuuden_tahden

Lehtilä, O., Nyström, P., Ronikonmäki, N-M. & Sirviö, T-H. 2021. Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla. Työryhmän loppuraportti. Valtioneuvosto. Viitattu 3.2.2021. http://urn.fi/URN:ISBN:978-952-243-614-6

Liikenne- ja viestintäministeriö. 2020. Tiedote. Viitattu 20.1.2021. https://valtioneuvosto.fi/-/valtion-kyberturvallisuusjohtaja-on-nimitetty

Lukka, K. N.d. Konstruktiivinen tutkimusote. Metodix - metoditietämystä kaikille -sivusto. Viitattu 13.12.2020. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Martin, G., Martin, P., Hankin, C., Darzi, A. & Kinross, J. 2017. Cybersecurity and healthcare: how safe are we? BMJ. Viitattu 12.12.2020. https://doi.org/10.1136/bmj.j3179

Papastergiou, S., Mouratidis, H. & Kalogeraki, E-M. 2020. Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures. Evolving systems. Viitattu 10.1.2021. https://doi.org/10.1007/s12530-020-09335-4

Swasey, K. 2020. Insufficient Healthcare Cybersecurity Invites Ransomware Attacks and Sale of PHI on the Dark Web. Center for Anticipatory Intelligence Student Research Reports. Viitattu 11.12.2021. https://www.usu.edu/cai/files/studentpaper-swasey.pdf

Tiedonhallinta sosiaali- ja terveysalalla. 2020. Terveyden ja hyvinvoinnin laitoksen verkkosivu. Viitattu 24.1.2021. https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/tiedonhallinnan-ohjaus

Tietoturva tuottaa ratkaisuja hyvinvointiin. 2020. Artikkeli Telian verkkosivuilla. Viitattu 24.1.2021. https://www.telia.fi/yrityksille/artikkelit/artikkeli/tietoturva-tuottaa-ratkaisuja-hyvinvointiin

Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Cert 2020. Organisaation verkkosivut. Viitattu 24.1.2021. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert

Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Kybersää Maaliskuu 2020. 2020. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 21.1.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kybers%C3%A4%C3%A4_maaliskuu_2020.pdf

Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Kybersää Syyskuu 2020. 2020. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Viitattu 22.1.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4-syyskuu2020.pdf

Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus NCSA. 2021. Organisaation verkkosivut. Viitattu 24.1.2021. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa

Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus Tilannekuva ja verkostojohtaminen 2021. Organisaation verkkosivut. Viitattu 24.1.2021. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen

Vertainen, V., & Suni, E. 2020. Tietojenkalastelun tarkistuslista. Viitattu 12.1.2021. https://jyvsectec.fi/wp-content/uploads/2020/12/TerveydenhuollonTietojenkalastelunTarkistuslista-JYVSECTEC.pdf

Vertainen, V., Suni, E., Vatanen, M., Hautamäki, J., Laava T. & Piispanen J. 2021. Kyberhäiriöiden hallinta Käsikirja terveydenhuollon toimijoille. Jyväskylän ammattikorkeakoulu. Viitattu 20.1.2021. https://jyvsectec.fi/2021/01/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille/

Virtanen, A. 2006. Ammattikasvatuksen aikakauskirja, Ajankohtaisia teemoja ammattikasvatuksesta. Artikkeli: Konstruktiivinen tutkimusote, Miten koulutus ja elinkeinoelämänodotukset kohtaavat ammattikorkea-koulun opinnäytetöissä 46–52. Viitattu 7.1.2021. https://akakk.fi/wp-content/uploads/Aikak_2006_1_lehti.pdf#page=47

Vuorinen, S. 2019. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja. Viitattu 15.1.2021. http://urn.fi/URN:ISBN:978-952-00-4085-7

Williams, CM., Chaturvedi, R. & Chakravarthy, K. 2020. Cybersecurity Risks in a Pandemic. Journal of Medical Internet Research (JMIR) Publications, 22, 9. Viitattu 30.12.2020. https://www.jmir.org/2020/9/e23692/

Liitteet

Liite 1. Tilannekartoituspalavereissa käytetty Microsoft PowerPoint -esitys

Ongelma

- Koronakriisin keskellä terveydenhuollon organisaatioihin kohdistuneet kyberhyökkäykset lisääntyneet maailmalla
- Hyökkääjä voi olettaa lunnasvaatimusten maksun olevan todennäköisempää kriisin aikana
- Myös muita motiiveja hyökkäykselle (esim. henkilötietojen myyminen eteenpäin)

jamk

Tavoitteet

- Kehittää terveydenhuollon ympäristöihin liittyviä kyberpoikkeamienhallinnan *prosesseja* ja *toimintaohjeita* varmistamaan yhteiskunnan kannalta kriittisen terveydenhuollon toimintojen jatkuvuutta myös kyberhyökkäysten tapahtuessa
- Yhteistoiminta valtakunnallisella tasolla tiedonjakamisessa ja tilannekuvassa
- Mahdollistaa uuden liiketoiminnan syntyminen ja vakiintuminen myös koronakriisin jälkeen

jamk

Toteutus

- Katselmoidaan terveydenhuollon tämänhetkiset ohjeet ja prosessit kyberpoikkeamatilanteisiin (yhteistyökumppaneiden ja saatavilla olevan tiedon avulla)
- Kartoitetaan ajankohtaiset kyberuhkavektorit, erityisesti liittyen koronakriisiin
- Kootaan tiedossa olevat puutteet ja laaditaan vaatimukset prosessien ja toimintaohjeiden parantamiseksi
- Tiedotetaan tuloksista terveydenhuollon toimijoita asiantuntijayhteistyönä, ja tiedotuskampanjan avulla sosiaalisessa mediassa

jamk

Tulokset

- Uudet kehitetyt prosessit ja toimintaohjeet ovat terveydenhuollon toimijoiden käytössä
- Kriittisen terveydenhuollon jatkuvuus turvataan kyberpoikkeamatilanteessa myös kriisin aikana
- Aktiivista tiedottamista kehitetyistä prosesseista jatketaan projektin jälkeenkin, jolla varmistetaan liiketoimintahyötyjen jatkojalostaminen sekä yksityisellä että julkisella sektorilla
- Tuloksia hyödynnetään myös mm. JAMK:in Health Care Cyber Range (HCCR) – hankkeessa

jamk

Keskustelua

- **voimassa olevat ohjeet ja prosessit kyberpoikkeamatilanteissa terveydenhuollossa**
  --> näiden mahdolliset puutteet (koronakriisi huomioiden)
- **näkemyksenne ajankohtaisista terveydenhuollon toimintaan kohdistuvista kyberuhkavektoreista, erityisesti koronakriisi huomioiden (lisääntyneen etätyön vaikutukset?)**

jamk

Liite 2. Projetin yhteistyökumppaneille lähetetty kyselylomake

Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektin palautekysely yhteistyökumppaneille

Pakolliset kentät ovat merkattu asteriskilla (*) ja ne pitää täyttää lomakkeen lähettämiseksi.

Tämä kysely on projektin yhteistyökumppaneille.
Olet saanut tämän kyselyn, sillä olet ollut mukana Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektissa. Tällä kyselyllä kerätään tietoa projektin toteutuksesta, vastaukset ovat anonyymejä.

Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä
Toteutusaika: 1.8.2020 - 31.1.2021
Rahoitus: Business Finland

Projektin tavoite on kehittää terveydenhuollon ympäristöihin liittyviä kyberpoikkeamienhallinnan prosesseja ja toimintaohjeita parantamaan ja varmistamaan yhteiskunnan kannalta kriittisen terveydenhuollon jatkuvuutta myös kyberhyökkäyksien tapahtuessa.

1. Yhteistyö *

Arvioi alla olevia väittämiä asteikolla 1-5

1 = täysin eri mieltä
2 = jokseenkin eri mieltä
3 = ei eri, eikä samaa mieltä
4 = jokseenkin samaa mieltä
5 = täysin samaa mieltä

	1	2	3	4	5
Projektin toteuttaja (JAMK) kertoi selkeästi projektin tavoitteista	○	○	○	○	○
Sain riittävästi tietoa projektin etenemisestä projektin toteuttajalta (JAMK)	○	○	○	○	○
Yhteistyö projektin toteuttajan (JAMK) kanssa oli sujuvaa	○	○	○	○	○
Projektin yhteistyöstä on ollut hyötyä minulle ja/ tai organisaatiolleni	○	○	○	○	○
Toivon tekeväni tulevaisuudessakin yhteistyötä projektin toteuttajan (JAMK) kanssa	○	○	○	○	○

2. Oman osallistumisen arviointi *

Arvioi alla olevia väittämiä asteikolla 1-5

1 = täysin eri mieltä
2 = jokseenkin eri mieltä
3 = ei eri, eikä samaa mieltä
4 = jokseenkin samaa mieltä
5 = täysin samaa mieltä

	1	2	3	4	5
Osallistuin projektiin niin aktiivisesti kuin olin ennakkoon suunnitellut	○	○	○	○	○
Projektin toteuttaja (JAMK) tarjosi riittävästi mahdollisuuksia osallistua projektiin	○	○	○	○	○
Projektin toteuttaja (JAMK) tarjosi riittävästi mahdollisuuksia vaikuttaa projektin tuloksiin	○	○	○	○	○

3. Kerro omin sanoin aktiivisuudestasi/ osallistumisestasi projektiin

4. Projektin tulosten arviointi *

Arvioi alla olevia väittämiä asteikolla 1-5

1 = täysin eri mieltä
2 = jokseenkin eri mieltä
3 = ei eri, eikä samaa mieltä
4 = jokseenkin samaa mieltä
5 = täysin samaa mieltä

	1	2	3	4	5
Projektin tuotoksesta (käsikirja) on hyötyä terveydenhuollolle	○	○	○	○	○
Olen tyytyväinen projektin tuloksena syntyneeseen käsikirjaan	○	○	○	○	○

5. Kerro ajatuksistasi projektin tuloksena syntyneestä käsikirjasta.

6. Kerro mikäli sinulle on syntynyt jatkoprojekti-ideoita aiheeseen liittyen.

7. Ehdotuksia projektin tuloksena syntyneen käsikirjan viestintään

Aktiivinen tiedottaminen käsikirjasta jatkuu projektin päättymisen jälkeenkin, kerro mikäli sinulla on ehdotuksia viestinnän kehittämiseksi.

8. Terveiset projektin toteuttajalle (JAMK)

9. Tämä kysely kerää tietoja Kyberpoikkeamienhallinnan prosessit ja toimintaohjeet terveydenhuollon ympäristöissä -projektin loppuraporttia varten. Tietojasi ei käytetä muihin tarkoituksiin ja niitä käsittelevät ainoastaan projektin toteuttajaorganisaation (JAMK) työntekijät. Kyselyn vastaukset ovat anonyymejä. Tietojesi käsittelyyn liittyen voit tarvittaessa olla yhteydessä elina.suni@jamk.fi *

- ◯ Annan luvan tietojeni käsittelyyn.