

Eerika Kauppinen

TIETOVERKKOON LIITETTYJEN FYY- SISTEN LÄÄKETIETEELLISTEN LAIT- TEIDEN KYBERTURVALLISUUS TER- VEYDENHUOLLOSSA

Lääketieteellisten laitteiden kyberturvallisuuden ny-
kytila terveydenhuollon organisaatioissa

Johtamisen ja talouden tiedekunta
Diplomityö
Ilona Ilvonen
Samuli Pekkola
Toukokuu 2023

TIIVISTELMÄ

Eerika Kauppinen: Tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuus terveydenhuollossa
Tampereen yliopisto
Tietojohdamisen tutkinto-ohjelma
Diplomityö
Toukokuu 2023

Terveydenhuollon toimialan digitalisoitumisen myötä terveydenhuollon organisaatioilla on halussaan luottamuksellista, digitaalisessa muodossa olevaa tietoa ja dataa. Digitalisaation ja nopeasti kasvavan ja kehittyvän teknologian myötä haasteena on tuottaa vaatimusten mukaisesti kyberturvallisia palveluita terveydenhuollon toimialalla. Luottamuksellisen tiedon turvaamiseksi terveydenhuollon organisaatioiden on otettava kyberturvallisuus huomioon kokonaisvaltaisesti toiminnassaan. Älysairaaloiden ja terveydenhuollon toimialan kehittymisen myötä myös lääketieteellisten laitteiden ominaisuudet ovat kehittyneet ja monilla laitteilla on kyky muodostaa yhteys tietoverkkoihin. Tietoverkkojen ja niihin kytkettävien älykkäiden lääketieteellisten laitteiden muodostama kokonaisuus luo tarpeen varmistua toiminnallisuuden luotettavuudesta ja turvallisuuden huomioinnista kokonaisvaltaisesti.

Tutkimuksessa on keskitytty tutkimaan lääkinnällisistä laitteista fyysisiä lääketieteellisiä laitteita, joilla on kyky muodostaa yhteys tietoverkkoihin. Rajauksen tarkoituksena on tutkia lääkinnällisten laitteiden laajasta joukosta laitteita, joiden kyberturvallisuutta voidaan arvioida erityisesti tietoverkkoon liitettävien ominaisuuksien näkökulmasta teoreettisten taustojen avulla. Tutkimuksen tarkoituksena on tutkia fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuuden nykytilaa. Tutkimuksessa selvitetään, minkälaisia kyberturvallisuusriskejä näihin laitteisiin liittyy ja kuinka organisaatiot hallitsevat ja hallinnoivat näitä riskejä toiminnassaan. Tutkimuksessa aihetta on tarkasteltu kyberturvallisuusriskien ja riskienhallinnan, riskien arvioinnin, hallinnan ja valvonnan, laitteisiin liittyvän yhteistyön ja hankintojen, sekä vastuiden ja seurannan teemojen kautta. Tutkimuksessa keskitytään fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuuden tarkasteluun käyttäjäorganisaatioiden näkökulmasta.

Tutkimuksessa käytettiin kvalitatiivista tutkimusmenetelmää ja tutkimusstrategiana tapaustutkimusta. Tutkimuksessa haastateltiin terveydenhuollon organisaatioista lääkintätekniikan ja tietohallinnon asiantuntijoita. Haastattelut toteutettiin kolmesta eri organisaatiosta ja viiden eri asiantuntijan kanssa puolistrukturoituina haastatteluina. Haastattelujen analysointiin käytettiin temaatista analyysiä aineistojen käsittelyssä. Haastatteluiden avulla selvitettiin tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuusriskejä ja niiden hallintatapoja organisaatioissa.

Tutkimusaineiston perusteella tietoverkkoon liitettäviin fyysisiin lääketieteellisiin laitteisiin kohdistuvat kyberturvallisuusriskit ovat lisääntyneet näiden laitteiden yleistyessä ja hoitotapojen sekä terveydenhuollon toimialan kehittyessä. Kyberturvallisuus on otettava huomioon lääketieteellisten laitteiden koko elinkaaren ajan laitevalmistajien ja terveydenhuollon käyttäjäorganisaatioiden taholta. Laitevalmistajien vahvojen laitevastuiden myötä käyttäjäorganisaatioiden on huomioitava toiminnassaan yhä enemmän kyberturvallisuutta tukevia parhaita käytäntöjä.

Tutkimuksesta käy ilmi, että kyberturvallisuuden huomiointi terveydenhuollon organisaatioissa ja lääketieteellisten laitteiden käytössä on merkityksellistä ja organisaatiot kokevat aiheen tärkeäksi. Terveydenhuollon organisaatioissa lääketieteellisten laitteiden riskejä hallitaan ja hallinnoidaan riskienhallinnan, tietoliikenteen ja -yhteyksien turvallisuudesta huolehtimalla, valitsemalla turvallisia ja luotettavia palveluntarjoajia, hankintaprosessissa vaatimusten mukaisilla laitehankinnoilla sekä organisaation sisäisillä prosessilla ja suunnitelmilla. Terveydenhuollon organisaatioiden pakollisten vastuiden ja toimintojen toteuttamisen lisäksi kokonaisvaltaisella suunnittelulla ja kolmansien osapuolien kanssa tehdyllä yhteistyöllä voidaan tukea laitteiden kyberturvallisuutta.

Avainsanat: kyberturvallisuus, lääkinnällinen laite, lääketieteellinen laite, tietoverkko, terveydenhuolto, terveydenhuollon digitalisaatio, älysairaala

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

ABSTRACT

Eerika Kauppinen: Cyber security of networked physical medical devices in healthcare
Tampere University
Information and Knowledge Management
Master's Thesis
May 2023

With the digitalization of the healthcare industry, healthcare organizations have access to confidential, digital information and data. Digitalization and rapidly growing and developing technology is causing challenges to produce cyber secure services in the healthcare industry in accordance with the requirements. To be able to secure confidential information, healthcare organizations have to take cybersecurity into account holistically in their operations. Combination of information networks and networked medical devices have created a need to ensure the reliability of functionality and the consideration of safety in a comprehensive manner.

Research has focused on the study of medical devices that are physical and have ability to connect to information networks. The purpose of the demarcation is to study a wide range of medical devices, the cybersecurity of which can be assessed, from the point of view of the characteristics to be connected to the network, using theoretical backgrounds. The purpose of the study is to define the current state of cybersecurity of physical networked medical devices. The study explores the types of cybersecurity risks associated with these devices and how healthcare organizations manage these risks in their operations. In the research, the topic has been examined through the themes of cybersecurity risks and risk management, risk assessment and validation, cooperation and procurement, and responsibilities and monitoring. The research focuses on examining the cybersecurity of physical networked medical devices from the perspective of healthcare user organizations.

The study used a qualitative research method and a case study as a research strategy. The study interviewed professionals in medical technology and information management from national healthcare organizations. The interviews were conducted from three different organizations and with five experts as semi-structured interviews. For the analysis of the interviews, thematic analysis was used in the processing of the data. The interviews were used to define the cybersecurity risks of networked physical medical devices and how to manage them in different healthcare organizations.

According to the research, cybersecurity risks to physical networked medical devices have increased as these devices have become more common and treatment methods and the healthcare industry have evolved. Cybersecurity must be considered throughout the life cycle of medical devices by device manufacturers and healthcare user organizations. With the strong device responsibilities of device manufacturers, user organizations must increasingly take into account best practices that support cybersecurity in their operations.

The study shows that the cybersecurity in healthcare organizations and the use of medical devices are significant and important topics in healthcare industry. In healthcare organizations, medical device risks are mostly managed by ensuring the security of risk management, network communications and connections, selecting secure and reliable service providers, in the procurement process through compliant equipment procurement, and through the organization's internal processes and plans. In addition to the mandatory responsibilities and functions of healthcare organizations, holistic planning and cooperation with third parties can support the cybersecurity of devices.

Keywords: cyber security, medical device, networked medical device, connected medical device, healthcare, healthcare digitalization, smart hospital

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

ALKUSANAT

Diplomityö toteutettiin yhdessä Deloitteen kanssa vuoden 2021 syksystä alkaen vuoden 2022 syksyyn saakka. Diplomityön tekemisen tukena on ollut monia merkityksellisiä henkilöitä, joita haluan kiittää korvaamattomasta avusta. Kiitän Deloitteen Cyber-tiimiä ja erityisesti Hannu Kasasta työn ohjaamisesta. Lisäksi haluan kiittää Tampereen yliopiston puolelta Ilona Ilvosta suuresta avusta ja arvokkaista neuvoista työn edistämiseksi diplomityöprosessin aikana. Kiitän myös suuresti diplomityöni haastatteluihin osallistujia.

Lopuksi haluaisin muistaa ja kiittää myös perhettäni saamastani avusta. Lisäksi kiitän ystäviäni koko opiskeluaikana saamastani tuesta ja kannustuksesta. Erityiset kiitokset kuuluvat puolisololleni Eerolle ja isälleni Tuomakselle, jotka ovat jaksaneet kannustaa ja tukea minua työni ohella toteutetusta diplomityöstä.

Tampereella, 12.5.2023

Eerika Kauppinen

SISÄLLYSLUETTELO

1. JOHDANTO	1
1.1 Tutkimuksen lähtökohdat ja tausta	1
1.2 Tutkimusongelman rajaus ja tutkimuskysymykset	2
1.3 Tutkimuksen rakenne	4
2. KYBERTURVALLISUUS SOSIAALI- JA TERVEYDENHUOLLOSSA	5
2.1 Terveydenhuollon organisaatioiden toimiala	5
2.2 Terveydenhuollon tietojärjestelmät	7
2.3 Kyberturvallisuus terveydenhuollossa	7
2.4 Kyberturvallisuuden haavoittuvuuksia, hyökkäyksiä ja uhkia terveydenhuollossa	9
2.5 Toteutuneita kyberriskejä ja -uhkia terveydenhuollon toimintaympäristössä	15
2.5.1 Haittaohjelmat	15
2.5.2 Tietomurrot	16
2.5.3 Palvelunestohyökkäykset	17
2.5.4 Tietojenkalastelut	18
3. LÄÄKINNÄLLISTEN JA LÄÄKETIETEELLISTEN LAITTEIDEN KYBERTURVALLISUUS	20
3.1 Lääkinnälliset laitteet terveydenhuollossa	21
3.2 Lääketieteellisten laitteiden elinkaari ja kunnossapito	23
3.3 Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet terveydenhuollossa	24
3.4 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kyberturvallisuushat ja -haavoittuvuudet	27
3.5 Toteutuneita hyökkäyksiä fyysisiin tietoverkkoon liitettyihin lääketieteellisiin laitteisiin	30
3.5.1 Haittaohjelmat	30
3.5.2 Verkkoyhteyttä käyttävät kyberhyökkäykset	31
3.5.3 Laitevarkaudet	32
3.6 Lääketieteellisten laitteiden riskit, riskienhallinta ja uhkilta suojaaminen 33	
3.6.1 Kyberturvallisuuden tilannekuvat, prosessit ja politiikat	38
3.6.2 Laitevalmistajien ja muiden sidosryhmien välinen yhteistyö	39
3.6.3 Tekniset turvatoimenpiteet ja yhteydet	41
3.6.4 Tietoturva- ja virustentorjuntaohjelmat sekä laitepäivitykset	42
3.6.5 Ihmisten käyttäytyminen ja koulutus	43
3.6.6 Fyysinen turvallisuus ja laitteiden suojaaminen	45
4. TUTKIMUSMENETELMÄ	47
4.1 Tutkimusasetelma	47

4.1.1	Tutkimusfilosofia: Interpretivismi	48
4.1.2	Lähestymistapa: Induktio	48
4.1.3	Tutkimusmetodologia: Laadullinen tutkimus.....	49
4.1.4	Tutkimusstrategia: Tapaustutkimus.....	49
4.1.5	Aikahorisontti: Poikittaistutkimus	50
4.2	Tapaustutkimuksen menettelytavat – kirjallisuuskatsaus ja haastattelututkimus.....	51
4.2.1	Kirjallisuuskatsaus	51
4.2.2	Puolistrukturoitu haastattelu.....	53
4.2.3	Tutkimuksen luotettavuus ja tiedon laadukkuus	54
4.3	Haastattelujen tiedonkeruu, kysymykset ja haastateltavat.....	56
4.4	Haastatteluaineiston analysointi.....	58
5.	KYBERTURVALLISUUDEN NYKYTILA TIETOVERKKOON LIITETTÄVISSÄ FYYSSISISSÄ LÄÄKINNÄLLISISSÄ LAITTEISSA.....	61
5.1	Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet ja niihin liittyvät riskit ja riskienhallinta.....	61
5.2	Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arviointi, valvonta ja hallinta	73
5.3	Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hankinnat ja niissä tehtävä yhteistyö.....	87
5.4	Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuut ja seuranta	94
6.	TULOSTEN ANALYSOINTI: KYBERTURVALLISUUDEN KEHITYSTARPEET JA TAVOITETILAN SAAVUTTAMINEN TIETOVERKKOON LIITETTÄVISSÄ FYYSSISISSÄ LÄÄKINNÄLLISISSÄ LAITTEISSA	102
6.1	Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet ja niihin liittyvät riskit ja riskienhallinta.....	102
6.2	Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arviointi, valvonta ja hallinta	110
6.3	Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hankinnat ja niissä tehtävä yhteistyö.....	118
6.4	Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuut ja seuranta	122
7.	JOHTOPÄÄTÖKSET	126
7.1	Yhteenveto.....	126
7.2	Tutkimuksen arviointi	131
7.3	Opinnäytetyöprosessin ja oman oppimisen arviointi.....	135
7.4	Tutkimuksen merkitys ja jatkotutkimuskohteet.....	136
	LÄHTEET.....	139

LIITE 1: TUTKIMUSTIEDOTTEEN POHJA HAASTATELTAVILLE TERVEYDENHUOLLON ORGANISAATIOILLE	145
LIITE 2: TUTKITTAVAN SUOSTUMUS.....	148
LIITE 3: HAASTATELUKYSYMYKSET JA -RUNKO	149

KUVALUETTELO

<i>Kuva 1. Piggin (2017) mukainen kuvaus terveydenhuollon toimintaympäristöstä.....</i>	<i>20</i>
<i>Kuva 2. Saundersin et al. (2019) sipulimallia käyttäen esitetyt tutkimusmetodologiset valinnat.</i>	<i>48</i>
<i>Kuva 3. Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteisiin liittyvät riskit ja riskienhallinta.</i>	<i>72</i>
<i>Kuva 4. Yhteenveto haastateltavien nostamista aiheista tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arvioinnista, valvonnasta ja hallinnasta.....</i>	<i>87</i>
<i>Kuva 5. Yhteenveto haastateltavien nostamista aiheista tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hankintaprosessista ja laitevalmistajien kanssa tehtävästä yhteistyöstä.....</i>	<i>94</i>
<i>Kuva 6. Yhteenveto haastateltavien nostamista aiheista tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuista ja seurannasta.....</i>	<i>101</i>
<i>Kuva 7. Haastatteluista ja kirjallisuudesta nostetut isoimmat ja merkittävimmät riskit fyysisissä tietoverkkoon liitettävissä lääketieteellisissä laitteissa.....</i>	<i>103</i>

TAULUKKOLUETTELO

<i>Taulukko 1. Pigin (2017) mukainen taulukko kyberhyökkäysten aiheuttamista uhista terveydenhuollon organisaatioissa.</i>	10
<i>Taulukko 2. Libickin (2007) kybermaailman rakennetta mukaileva viisikerroksinen malli terveydenhuollon toimintaympäristöstä.</i>	12
<i>Taulukko 3. Kyberturvallisuuden merkittävimmät riskit lääketieteellisille laitteille mukainen Deloitte Center for Health Solutions (2013), Pigin (2017) ja Csulak et al. (2017).</i>	35
<i>Taulukko 4. Hakulausekkeiden osumien määrä tutkimuskäsitteistä valikoiduissa tietokannoissa.</i>	52
<i>Taulukko 5. Tutkimukseen osallistuneet haastateltavat henkilöt ja viittaustapa heihin tutkimuksessa.</i>	56
<i>Taulukko 6. Haastateltavien vastauksista kootut merkittävimmät tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kyberturvallisuusriskit.</i>	63
<i>Taulukko 7. Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kohdistuvien riskien potentiaaliset vaikutukset riskien toteutuessa.</i>	66
<i>Taulukko 8. Haastateltavien organisaatioiden riskienhallintaan ja sen prosesseihin liittyvät havainnot.</i>	67
<i>Taulukko 9. Haastateltavien päänostot ja -havainnot kyberriskeiltä ja -uhilta suojautumiseen.</i>	71
<i>Taulukko 10. Haastateltavien päähavainnot ja -nostot laitteiden turvallisuuden arviointitavoista ja -käytännöistä.</i>	77
<i>Taulukko 11. Haastateltavien päähavainnot ja -nostot haavoittuvuuksien hallinnasta.</i>	79
<i>Taulukko 12. Haastateltavien päähavainnot ja -nostot pääsynhallinnan ja -valvonnan keinoista.</i>	83
<i>Taulukko 13. Haastateltavien päähavainnot ja -nostot tietoturvapoikkeamien hallinnoimisesta.</i>	85
<i>Taulukko 14. Haastateltavien päähavainnot ja -nostot laitevalmistajien kanssa tehdystä yhteistyöstä ja siihen liittyvistä haasteista.</i>	90
<i>Taulukko 15. Haastateltavien päähavainnot ja -nostot kyberturvallisuusriskien huomioinneista hankinnoissa.</i>	93
<i>Taulukko 16. Haastateltavien päähavainnot ja -nostot turvallisuuteen liittyvistä vastuista lääketieteellisten laitteiden osalta.</i>	98
<i>Taulukko 17. Haastateltavien päähavainnot ja -nostot informoimisen vastuista hoitohenkilökunnalle ja potilaille kyber- ja tietosuojariskeistä.</i>	99
<i>Taulukko 18. Haastateltavien päähavainnot lääketieteellisten laitteiden rekistereistä ja niiden tiedoista.</i>	100
<i>Taulukko 19. Vertailu kirjallisuudessa ja haastatteluissa mainituista kyberturvallisuusriskienhallinnasta, riskeistä sekä niiltä suojautumisesta.</i>	110
<i>Taulukko 20. Vertailu kirjallisuudessa ja haastatteluissa mainituista kyberturvallisuuteen liittyvästä arvioinnista ja hallinnoinnista lääketieteellisissä laitteissa.</i>	118
<i>Taulukko 21. Vertailu kirjallisuudessa ja haastatteluissa mainituista kyberturvallisuuteen liittyvien lääketieteellisten laitteiden hankinnoista.</i>	122
<i>Taulukko 22. Laitevalmistajan ja käyttäjäorganisaatioiden vastuut lääketieteellisistä laitteista laitteiden elinkaaren aikana.</i>	124

1. JOHDANTO

Tämä diplomityö tarkastelee fyysisten tietoverkkoon kytkettyjen lääketieteellisten laitteiden kyberturvallisuuden nykytilaa terveydenhuollon organisaatioissa. Nykytilan lisäksi tutkimuksessa selvitetään, miten erilaisia fyysisten tietoverkkoon kytkettyjen lääketieteellisten laitteiden kyberriskejä ja -uhkia hallinnoidaan, ja kuinka vastuut näiden laitteiden kyberturvallisuudesta on jaettu organisaatioissa. Tässä luvussa lukija johdatellaan tutkimuksen kohteena olevaan aiheeseen esittelemällä aluksi yleisesti kyberuhkia ja -riskejä sekä niiden mahdollisia vaikutuksia terveydenhuollon alalla, joka näkyy poikkileikkauksella myöhemmin esitettyjen tutkimuksen tavoitteiden ja rajauksen käsittelyssä. Tavoitteiden ja tutkimusrajan lisäksi esitellään tutkimusrakenne. Muut tutkimuksen rajaukseen ja valinnat esitellään tarkemmin tutkimusmetodologian luvussa.

1.1 Tutkimuksen lähtökohdat ja tausta

Tutkimuksen aihe valikoitui kyberturvallisuuden parista omasta mielenkiinnostani terveydenhuollon alaa kohtaan sekä toimeksiantajayrityksen tarpeesta tunnistaa terveydenhuollon kyberturvallisuuden nykytilaa liittyen lääketieteellisiin laitteisiin. Terveydenhuollon toimiala on kiinnostanut minua teknologisesta näkökulmasta jo opintojen alusta alkaen, jolloin diplomityön aihe on itselleni mielenkiintoinen. Oman mielenkiinnon lisäksi aihe on myös yhteiskunnallisesti ajankohtainen ja tärkeä, sillä tietoturvatapausten määrä on kasvanut vuosi vuodelta ja kyberturvallisuus koskettaa yhä useamman ihmisen arkea eri digitalisoituneiden kanavien ja palveluiden kautta (Traficom 2021). Digitaalisten järjestelmien ja sähköisten palveluiden kautta myös kyberhyökkäyksistä on tullut todellinen uhka terveydenhuoltoalalla. Kyberhyökkäysten yleistyessä terveydenhuollon organisaatioihin, voidaan tässä nähdä jonkinlaista globaalin trendin kehittymistä. (Pulliainen 2020) Teknologian ja digitalisaation kehittymisen myötä terveydenhuoltoon on avautunut mahdollisuus tuottaa sairaalapalveluita aiempaa laajemmin tietoverkkoja käyttämällä. Teknologisen kehityksen myötä tietoverkkojen ja niihin kytkettävien älykkäiden laitteiden muodostama kokonaisuus luo huolen toiminnan luotettavuudesta ja tietojenkäsittelyn turvallisuudesta. Kyberturvallisuuden osalta riskejä luovat haavoittuvat laitteet ja ohjelmistosovellukset, joita käytetään osana hoidossa käytettävää verkottunutta toimintaympäristöä ja tätä kautta myös kyberfyysisiä järjestelmiä. (Lehto et al. 2019, s.9)

Diplomityön tarkoituksena on tutustua kirjallisuusosiossa lääketieteellisiin laitteisiin terveydenhuollon toimialan ympäristössä sekä tarkastella kyberturvallisuuden nykytilaa ja kehitystä terveydenhuollon näkökulmasta. Lääketieteellisistä laitteista rajataan tutkimukseen tietoverkkoon kytkettävät fyysiset lääketieteelliset laitteet kokonaisvaltaiseen tarkasteluun, jolloin rajauksen ulkopuolelle jäävät esimerkiksi tietojärjestelmät ja ohjelmit. Rajaus on perusteltua tarkemman tutkittavan kohderyhmän tekemiseksi sekä kyberturvallisuuden näkökulmasta siksi, että näillä fyysisillä laitteilla, kuten esimerkiksi kuvantamisen laitteilla, on yhtenäisiä ominaisuuksia, jolloin tutkimusaineiston analysointi ja siitä tehtävät johtopäätökset ovat yleistettävämpiä. Rajaukseen sisällytettiin lääketieteellisten laitteiden osalta myös tietoverkkoon kytkettävyys, jonka tarkoituksena oli rajata pois lääkinnälliset laitteet, joissa ei ole ominaisuutta yhdistyä tietoverkkoon. Tällaisia lääkinnällisiä laitteita ovat esimerkiksi piilolinssi, kylmägeeli, sairaalasänky ja laastari (Fimea 2022).

Haastatteluiden avulla pyritään selvittämään, miten kyberturvallisuuden riskit on tunnistettu ja miten kyberturvallisuutta, sen riskejä ja haavoittuvuuksia hallitaan. Lisäksi haastatteluilla pyritään selvittämään ja siten tutkimaan, miten ja kenelle kyberturvallisuuteen liittyvät vastuut on jaettu sekä kuinka vastuiden jakamistavat eroavat terveydenhuoltoalan eri organisaatioiden välillä. Haastatteluiden ja kirjallisuuskatsauksen avulla pyritään selvittämään minkälaisia uhkia ja riskejä näihin laitteisiin ja miten niitä vastaan tulisi suojautua. Tutkimusta tehdään lääketieteellisten laitteiden käyttäjäorganisaatioiden näkökulmasta, jolloin valmistajien näkökulma kyberturvallisuudesta rajataan tutkimuksen ulkopuolelle. Tutkimushaastattelut sisältävät kuitenkin kysymyksiä valmistajien ja terveydenhuolto-organisaatioiden välisestä yhteistyöstä ja vuorovaikutuksesta.

Diplomityön tutkimuksen tulosten myötä toimeksiantajaorganisaatiolla voidaan nähdä olevan parempi käsitys terveydenhuollon kyberturvallisuuteen ja lääketieteellisiin laitteisiin liittyen. Uuden tutkimustiedon avulla voidaan kohdistaa ja tarjota erilaisia kyberturvallisuuden palveluita terveydenhuollon organisaatioihin sekä ymmärtää minkälaisia haasteita ja tarpeita organisaatioilla on terveydenhuollon alalla. Tunnistettujen tietojen valossa toimeksiantajalla on mahdollisuus vahvistaa aiempia asiakassuhteita sekä tarjota kyberturvallisuuden palveluita potentiaalisille asiakkaille ymmärtämällä alalle merkittävistä riskeistä, uhkista ja haavoittuvuuksista.

1.2 Tutkimusongelman rajaus ja tutkimuskysymykset

Tutkimuksen tavoitteena on tutkia kyberturvallisuuden nykytilaa tietoverkkoon liitettyjen fyysisten lääkinnällisten laitteiden osalta kansallisissa terveydenhuollon organisaatioissa.

tioissa. Tutkimuksessa halutaan tunnistaa miten eri terveydenhuollon organisaatiot hallitsevat ja jakavat vastuita tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuuden osalta. Tutkimuksen tavoitteiden pohjalta on luotu diplomityön päätutkimuskysymys, johon tutkimuksella pyritään vastaamaan. Päätutkimuskysymyksen lisäksi on muodostettu alatutkimuskysymyksiä, jotka pyrkivät avustamaan päätutkimuskysymykseen vastaamisessa.

Tutkimuksen päätutkimuskysymys:

1. Miten tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberriskit ja -uhkat ovat otettu huomioon terveydenhuollon organisaatioissa kyberturvallisuuden hallitsemiseksi ja hallinnoimiseksi?

Diplomityön tarkoituksena on vastata tähän pääkysymykseen tutkimalla kokonaisvaltaisesti lääketieteellisten laitteiden kyberturvallisuuden nykytilaa ja haastateltavien organisaatioiden vastuunjakoa, hallintaa ja seurantaan liittyen kyberriskeihin ja -uhkiin. Aihe on rajattu lääketieteellisten laitteiden osalta tietoverkkoon liitettyihin fyysisiin laitteisiin, jotta aihe saataisiin rajattua tarpeeksi tiiviiksi ja kyberturvallisuuden näkökulmasta näillä laitteilla on tietynlaisia ominaisuuksia, joihin kohdistuu erilaisia riskejä ja uhkia. Pääkysymyksen lisäksi on kehitetty alatutkimuskysymyksiä, jotka auttavat vastaamaan päätutkimuskysymykseen.

Tutkimuksen alakysymykset:

1. Minkälaisia kyberuhkia ja -riskejä tietoverkkoon liitettyihin fyysisiin lääketieteellisiin laitteisiin kohdistuu ja miten niitä on pyritty tunnistamaan?
2. Minkälaista kyberturvallisuuteen liittyvää yhteistyötä tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden osalta toteutetaan hankintojen osalta terveydenhuollon organisaatioissa?
3. Miten tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuutta hallitaan ja miten vastuut kyberturvallisuudesta on jaettu?

Kyberturvallisuuden yleisen huomioimisen ja hallinnoimisen lisäksi diplomityössä selvitetään, minkälaisia kyberuhkia ja -riskejä tietoverkkoon liitettäviin fyysisiin lääketieteellisiin laitteisiin kohdistuu. Lisäksi tutkitaan, miten niitä hallitaan terveydenhuollon organisaatioissa. Kyberriskien ja -uhkien lisäksi diplomityössä tutkitaan kyberturvallisuuden hallintaan ja vastuiden jakamisiin liittyviä valintoja lääketieteellisten laitteiden suhteen.

Diplomityön tutkimusongelma on rajattu sosiaali- ja terveydenhuollon alalta kansallisiin terveydenhuoltoon ja sen julkisiin organisaatioihin. Tutkimuksen rajaus kansallisiin, jul-

kisten terveydenhuollon organisaatioihin on tehty tutkimushaastatteluaineiston paremman vertailtavuuden ja samankaltaisten lääketieteellisten laitteiden käyttöympäristön kautta. Lääketieteellisten laitteiden suhteen tutkimuksessa on rajattu käsittelemään tietoverkkoon liitettäviä fyysisiä lääketieteellisiä laitteita, jolloin ulkopuolelle jäävät esimerkiksi lääkinnälliset ohjelmistot ja tietojärjestelmät.

1.3 Tutkimuksen rakenne

Tämä tutkimus koostuu johdannosta, kirjallisuuskatsauksesta, tutkimusmetodologian valinnasta ja empiirisestä osuudesta, jossa analysoidaan aineistoa, sekä johtopäätöksistä. Kirjallisuuskatsausta pidetään osana tapaustutkimuksen aineistoa yhdessä tapaustutkimuksen empiirisen osion kanssa. Kirjallisuudesta ja empiirisestä osuudesta saatavaa tietoa ja aineistoa käytetään analyysissä yhdessä kokonaisvaltaisen kuvan ja käsityksen luomiseen. Viimeisenä kohtana tutkimuksessa luodaan johtopäätöksiä aineiston analyysin pohjalta.

Diplomityö alkaa aiheeseen tutustuttavalla johdannolla. Tämän jälkeen toisessa ja kolmannessa kappaleessa käsitellään kirjallisuusosuuksien avulla ensin kyberturvallisuutta terveydenhuoltoalalla ja sen jälkeen kolmannessa luvussa lääkinnällisiä laitteita ja lääkinnällisten laitteiden kyberturvallisuutta terveydenhuoltoalalla. Neljännessä kappaleessa esitetään tutkimuksen metodologisia valintoja ja menetelmiä. Viidennessä kappaleessa käsitellään tapaustutkimuksen empiiristä osuutta, jossa haastatteluaineistot analysoidaan ja tuodaan esille kyberturvallisuuden näkökulmasta tietoverkkoon kytkettävien fyysisten lääkinnällisten laitteiden uhista, riskeistä ja riskienhallinnasta, sekä niihin liittyvistä hallinta- ja vastuumalleista. Tämän jälkeen kuudennessa kappaleessa haastatteluaineistoa ja teoriaa vertaillaan toisiinsa ja käydään lävitse yhtäläisyyksiä ja erilaisuuksia. Viimeisessä eli seitsemännessä luvussa vedetään tutkimuksen pääpiirteitä yhteenvedoksi sekä tuodaan esille johtopäätökset tutkimuksen pääteemoista tutkimuksen pää- ja alatutkimuskysymysten avulla. Lisäksi seitsemännessä kappaleessa arvioidaan tutkimuksen onnistumista ja jatkotutkimuskohteita.

2. KYBERTURVALLISUUS SOSIAALI- JA TERVEYDENHUOLLOSSA

Kyberturvallisuuden merkitys organisaation tietojen turvaamiseksi ja toiminnan takaamiseksi on kasvanut viime aikoina. Teknologisen murroksen myötä terveydenhuollon organisaatiot muodostavat suotuisan ympäristön mahdollisille kyberhyökkäyksille (Seale et al. 2018). Erilaiset kyberhyökkäykset ovat moninaistuneet ja moninkertaistuneet, mikä tarkoittaa organisaatioille jatkuvaa tarvetta suojautua näiltä hyökkäyksiltä. Terveysthuollon digitalisoitumisen myötä terveydenhuollon organisaatioilla on hallussaan luottamuksellista tietoa ja dataa digitaalisessa muodossa esimerkiksi erilaisissa tietojärjestelmissä, mikä luo haasteita tietojenkäsittelyyn, tallennukseen ja käsittelyyn datan kasvun, tiedonkäsittelyn nopeuden, tietorakenteiden ja arvonalisäyksen suhteen (Zhang et al. 2017, s.88). Terveysthuollon haavoittuvuudet voivat potentiaalisesti vaikuttaa negatiivisesti kliniseen hoitoon ja potilasturvallisuuteen (Lehto et al. 2019, s.9). Näin kyberturvallisuudesta huolehtiminen koskettaa kaikkia terveydenhuollon organisaatioita ja on yhteiskunnallisesti merkityksellistä.

Tässä luvussa tutustutaan tarkemmin terveydenhuollon toimialaan ja kyberturvallisuuden alan organisaatioissa. Lopuksi käsitellään tarkemmin terveydenhuollon toimintaympäristöön liittyvistä kyberriskeistä ja -uhista. Luvun tarkoituksena on syventyä ja tutustua kyberturvallisuuden terveydenhuollossa ja luoda ymmärrystä pohjaksi lääketieteellisten laitteiden kyberturvallisuuden paremmaksi ymmärtämiseksi.

2.1 Terveysthuollon organisaatioiden toimiala

Terveysthuollolla on suuri rooli suomalaisen yhteiskunnan toimivuudessa ja se luokitellaan osaksi turvallisuusstrategian elintärkeitä toimintoja (Norri-Sederholm et al. 2019). Terveysthuoltoalalla hyödynnetään jokapäiväisesti digitaalisia palveluita, jotka perustuvat tieto- ja viestintäteknologiaan. Tällaisiin teknologioihin luetaan muun muassa mobiiliteknologia, pilvipalvelut ja tekoälytoiminta. Terveysthuollossa kerätään dataa ja tietoja tyypillisesti paljon, mutta niiden käsittelyyn ja hyödyntämiseen tarvitaan yhteistyötä, jotta tiedot eivät vaarantuisi ja ammattilaisten työ ei vaikeutuisi tai keskeytyisi. (Sosiaali- ja terveystministeriö 2019)

Terveysthuollon arkaluontoisten asiakas- ja potilastietojen käsittely asettaa toimijoille erityisiä vaatimuksia. Arkaluonteisuuden ja luottamuksellisen luonteen vuoksi näitä tietoja on suojattava asiakkaiden ja potilaiden yksityisyyden takaamiseksi. Tämän lisäksi

on suojattava tietojen eheyttä, saatavuutta ja luotettavuutta. Potilaan ja asiakkaan palveluiden täytyy perustua oikean henkilön oikeisiin tietoihin, jotka on yhdistetty oikeaan potilaaseen. Toisaalta taas tietojen tulee olla käytettävissä, kun siihen on tarve. (Sosi- aali- ja terveysministeriö 2019)

Luottamuksellisuutta, saatavuutta ja eheyttä voidaan kuvata CIA-mallilla (eng. CIA-Model), joka esiteltiin vuonna 1991. CIA-mallin tarkoituksena on kuvata tietoturvaa luokittelumallilla luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta ja parantaa näin ohjelmistojen ja tietojärjestelmien tietoturvallisuutta. (Hafiz & Johnson 2007) Luottamuksellisuudella (eng. confidentiality) tarkoitetaan sitä, että vain valtuutetut tahot käsittelevät tietoja. Tiedon eheydellä (eng. integrity) pyritään siihen, ettei tieto muuttuisi hallitsemattomasti tai tahattomasti teknisestä syystä tai ihmisen tekemänä. Saatavuudella tarkoitetaan tiedon saatavuutta juuri silloin, kun tietoa tarvitaan. (Andress 2019)

Terveydenhuollossa luottamuksellisuudella, eheydellä ja saatavuudella on kaikilla suuri vaikutus ja merkitys potilasturvallisuuden rakentamisessa ja lääketieteellisissä järjestelmissä ne eroavat toisistaan käyttötarkoitusten mukaan (Pöyhönen et al. 2019). Luottamuksellisuus näkyy tietojen käsittelyn luottamuksellisuudessa ja siinä, että terveystietoja voivat käsitellä vain terveydenhuollon ammattilaiset, joilla on lain kautta muodostuva hoitosuhde tai muu syy tietojen käsittelyyn (Andreasson et al. 2013). Luottamuksellisuus ja sen varmistaminen terveydenhuollon sairaalajärjestelmissä on ensisijainen tavoite ja tarkoitus tietomurtojen ja kiristyshaittaohjelmilta suojautumisessa (Pöyhönen et al. 2019). Terveydenhuollossa työskenteleville salassapito on yksi tärkeimmistä asioista potilashoidossa, jonka päämääränä on hoidon onnistumisen turvaaminen ja luottamuksellisen hoitosuhteen yksilön suojaaminen (Andreasson et al. 2013).

Saatavuudella on puolestaan iso merkitys ja rooli, kun on tarve saada tietää potilaan aiempia hoitokertomuksia ja -tietoja ja leikkauksessa annettujen lääkkeiden ja määrien tiedot. Asiakas- ja potilastyöhön liittyvät tiedot tulee olla ammattilaisten saatavilla digitaalisesti, mutta myös kansalaisille tulee mahdollistaa pääsy omiin terveystietoihin. (Sosi- aali- ja terveysministeriö 2019) Tiedon saatavuuden varmistamisella voidaan huolehtia, että potilaat saavat tarvitsemaansa hoitoa myös lääketieteellisten laitteiden ollessa osana hoitoa (Pöyhönen et al. 2019). Myös tiedon eheys ja siihen luottaminen on erityisen tärkeää, sillä terveydenhuollossa tietoa käytetään muun muassa hoidon päätöksenteon tukena (Andress 2019). Potilastietojen ollessa digitaalisessa muodossa on tärkeää varmistaa potilastietojärjestelmien toimivuus ja tietojen onnistunut tallentaminen. Terveydenhuollossa tietojen saatavuutta ovat heikentäneet esimerkiksi palvelunestohyökkäykset, joiden määrä terveydenhuollon toimijaorganisaatioihin kohdistuen on noussut.

2.2 Terveydenhuollon tietojärjestelmät

Terveydenhuollon tietojärjestelmien toimivuus on hyvän potilashoidon lähtökohta. Terveydenhuolto on yksi suurimmista toimijoista, jotka käyttävät tietojärjestelmiä. Tietojärjestelmien avulla pyritään parantamaan palvelua, mutta myös vähentämään lääketieteellisten virheiden määrää paremmalla tietojen saatavuudella (LeRouge et al. 2017). Terveydenhuollossa potilaan tietoja on mahdollista käyttää vain terveydenhuollon asiantuntija, jolla on hoitosuhde potilaaseen. Hoitavalla henkilökunnalla on tällöin oikeus nähdä potilaskertomus hoitoa vaativilta osilta ja toisaalta myös velvollisuus kirjata oma merkintä potilaskertomukseen. (Sosiaali- ja terveysministeriö 2019)

Terveydenhuollossa käytössä on kansallisia, alueellisia ja paikallisia järjestelmiä, jotka muodostavat tietojärjestelmäarkkitehtuurin. Tietojärjestelmien yksi keskeisin toimintaympäristö terveydenhuollossa on sairaala. Kansallisten tietojärjestelmien tarkoituksena on huolehtia tietojen varastoinnista ja jakelusta, kun taas paikalliset ja alueelliset järjestelmät ovat tarkoitettuja operatiiviseen käyttöön jokapäiväisessä toiminnassa. (Sosiaali- ja terveysministeriö 2019) Suomessa käytössä oleva kansallinen terveydenhuollon tietojärjestelmä on esimerkiksi kansallinen potilastiedon arkisto Kanta, jota käytetään sosiaali- ja terveydenhuollon ammattilaisten ja kansalaisten keskuudessa. Paikallinen terveydenhuollon tietojärjestelmä on esimerkiksi potilastietojärjestelmä, jolla hallitaan potilaiden tietoja ja terveydenhuollon ammattilaisen työtä. Potilastietojärjestelmät ovat liittyneitä kansallisiin palveluihin, jolloin potilastietoja saadaan päivitettyä Kanta-palveluun. Potilastietojärjestelmiä ja rekisterin pitäjiä on monia erilaisia ja niiden välinen kommunikointi perustuu potilaan kieltoon tai suostumukseen tietojensa näkymiseen toisissa rekistereissä. (Sosiaali- ja terveysministeriö 2019)

2.3 Kyberturvallisuus terveydenhuollossa

Suomi tunnetaan kansainvälisesti digitalisaation hyödyntämisestään. Digitalisaation ja nopeasti kasvavan ja kehittyvän teknologian myötä muodostuu myös haasteelliseksi tuottaa vaatimusten mukaisesti tieto- ja kyberturvallisia palveluita. (Sosiaali- ja terveysministeriö 2019) Terveydenhuollon toimivien tietojärjestelmien takaaminen on yksi merkittävimmistä toimivuuden turvaamisen osista yhteiskunnassamme. Tietojärjestelmien toimivuuden suojaaminen on myös osa turvallisuusstrategiaan liittyvää talouden, infrastruktuurin ja huoltovarmuuden varmistamista. (Norri-Sederholm et al. 2019) Suomen kyberturvallisuusstrategiassa mainitaan kansallinen terveydenhuolto toimeenpano-ohjelmassa, jossa yhtenä kohtana käsitellään tieto- ja kyberturvallisuuden varmistamista

(Turvallisuuskomitea 2013). Turvallisuuden kokonaiskuvan näkökulmasta on merkittävää huomioida myös kyberturvallisuus ja siihen liittyvät riskit sekä uhkat terveydenhuoltoalalla (Norri-Sederholm et al. 2019).

Kyberturvallisuus terveydenhuollossa on tärkeänä osana yhteiskunnan varautumista, kun kyseessä on elintärkeiden toimintojen turvaaminen normaali- ja kriisitilanteessa. Kyberturvallisuutta on priorisoitava ja siihen kiinnitettävä huomiota terveydenhuollossa, sillä terveydenhuoltoala kiinnostaa kyberrikollisia ja on sijoittuneena ensimmäiseksi kyberhyökkäysten listalla. Terveystoimiala on ensimmäisenä top-5-listalla kyberhyökkäysten suhteen yhdessä valmistuksen ja tuotannon, pankki- ja rahoitustoimialan, julkishallinnon sekä liikenne- ja kuljetustoimialan kanssa. (Norri-Sederholm et al. 2019).

Kyberturvallisuuden avulla voidaan lisätä luottamuksellisuutta tietojenkäsittelyyn terveydenhuollossa (Sosiaali- ja terveysministeriö 2019). Terveydenhuoltoalalla kyberturvallisuudessa erityisen tärkeätä on pystyä suojaamaan ja huomioimaan asiakas- ja potilastiedot, sekä kansallisten sosiaali- ja terveydenhuollon tietovarannot ja digitaaliset diagnostiset palvelut ja verkkoihin kytketyt laitteet. Kyberhyökkäysten kohteena on erityisesti potilastiedot, joita vuonna 2015 varastettiin arviolta satamiljoonaa. Potilastiedot kiinnostavat entistä enemmän kyberrikollisia, sillä potilastiedot sisältävät luottamuksellista tietoa, kuten luottokorttinumeroita, sähköpostiosoitteita sekä sairausvakuutus-, työnantaja- ja sairaushistoriatietoja. (Norri-Sederholm et al. 2019)

Asiakas- ja potilastietojen suojaamisen lisäksi kyberturvallisuuden huomiointia tarvitaan terveydenhuollon toimintaympäristössä erilaisiin järjestelmiin, laitteisiin ja rakennuksiin (Sosiaali- ja terveysministeriö 2019). Terveydenhuollossa kyberturvallisuus tulee ottaa huomioon esimerkiksi erilaisissa järjestelmissä niin kansallisesti kuin paikallisestikin. Sairaalassa tai terveydenhuollon suorassa ympäristössä olevien järjestelmien, kuten kliinisen hoidon tietojärjestelmien, lisäksi on huolehdittava muun muassa etähoidon järjestelmien ja potilaiden tunnistamiseen käytettävien järjestelmien kyberturvallisuudesta.

Terveydenhuollon tietojärjestelmien turvallisuudesta huolehditaan erilaisin teknisin tavoin ja prosessein. Tietojärjestelmien tulee läpäistä sertifiointiprosessi sisältäen tietoturvallisuuden auditoinnin, mikäli järjestelmät halutaan liitettävän Kanta-palveluihin (Sosiaali- ja terveysministeriö 2019). Kansallisen tason järjestelmässä on kyberturvallisuudesta pyritty huolehtimaan hyvällä suojauksella ja valvonnalla. Järjestelmien välinen tietoliikenne kulkee pääosin erillisissä verkoissa, mutta erityisesti pienet toimijat voivat käyttää palveluita julkisessa verkossa altistaen palvelut mahdollisille verkon häiriöille. Julkista verkkoa käyttävät järjestelmät ovat näkyviä ja siksi myös alttiita hyökkäyksille, mutta

usein tällaiset järjestelmät eivät ole kriittisiä järjestelmiä. (Sosiaali- ja terveysministeriö 2019)

Tietojärjestelmien lisäksi terveydenhuollon kyberturvallisuudessa tulee huomioida myös erilaiset verkkolaitteet, mobiilipäätelaitteet ja niiden sovellukset, tietosisällöt ja verkotetut lääkinnälliset laitteet. Verkkolaitteilla tarkoitetaan laitteita, jotka mahdollistavat etälaitteiden, kuten älyrannekkeiden ja biometrinen skannereiden, liittämisen terveydenhuollon toimijan järjestelmiin. Mobiilipäätelaitteet kattavat puolestaan laitteet, jotka mahdollistavat tiedon tallettamisen ja kuljettamisen terveydenhuollon hoitohenkilökunnan mukana sijainnista riippumatta. Lääkinnällisistä laitteista puolestaan verkotetut laitteet vaativat erityistä kyberturvallisuuden arviointia, sillä ne ovat yhteydessä tietoverkkoihin ja sitä kautta kommunikoivat muiden laitteiden ja järjestelmien kanssa. Verkottuneita lääkinnällisiä laitteita ovat esimerkiksi puettavat teknologiset laitteet, avustavat robotit ja kannettavat päätelaitteet. Myös tietosisällöt on otettava huomioon erityisellä tavalla kyberturvallisuuden näkökulmasta, sillä ne sisältävät sensitiivistä tietoa henkilökunnasta, sairaalasta, tutkimuksista ja potilaista. (Sosiaali- ja terveysministeriö 2019).

Tietojärjestelmien, laitteiden ja tietosisältöjen lisäksi sairaalaympäristössä täytyy suojata kiinteistörakennukset ja suoraan terveydenhuollon hoitotapahtumaan liittymättömät, mutta toimintaa tukevat toimistolaitteet. Rakennusten turvallisuuden turvaamiseen voi liittyä esimerkiksi kiinteistöautomaatiota, joka mahdollistaa automaattiovien, älykkäiden lukitus- ja LVIS-järjestelmien sekä hoitotilanteisiin liittyvien automaattisten järjestelmien käytön. Kyberturvallisuuden suhteen on osattava myös ottaa huomioon perinteisinä nähdyt toimistolaitteet, jotka kuuluvat osaksi ympäristöä (Sosiaali- ja terveysministeriö 2019).

2.4 Kyberturvallisuuden haavoittuvuuksia, hyökkäyksiä ja uhkia terveydenhuollossa

Terveydenhuollon kyberturvallisuudessa on huolehdittava haavoittuvuuksien, hyökkäyksien ja uhkien suhteen ylläpitämällä teknisiä keinoja esimerkiksi erilaisten palomuurien, salausten ja virusten torjuntaohjelmien kautta. Teknisten keinojen lisäksi on huolehdittava myös ihmisten käytöksestä ja toiminnasta, sillä ihmistä voidaan pitää tietoturvan heikoimpana osapuolena. Terveydenhuollon työntekijöiden, kuten muidenkin ihmisten, työssä tapahtuvat huolimattomuudet tietoturvassa ja ihmisten profilointi luovat mahdollisuuksia kyberhyökkäysten alueille. (Norri-Sederholm et al. 2019)

Kyberuhat voivat muodostua toteutuneista kyberturvauhkista vaarantamalla tietojärjestelmien oikeanmukaisuutta tai tarkoitettua toimintaa, tai digitaalisissa ympäristöissä toteutettavia turvallisuuteen negatiivisesti vaikuttavista teoista (Turvallisuuskomitea 2018).

Kyberuhat voivat olla itsenäisiä, tapahtua samanaikaisesti tai jatkumoina toisista tapahtumista (Lehto 2015). Kyberuhkia ovat esimerkiksi kybervandalismi, -rikollisuus, -vakoilu, -terrorismi ja -operaatiot osana kybersodankäyntiä. (Norri-Sederholm et al. 2019) Kyberuhkat terveydenhuollossa liittyvät pääasiallisesti terveydenhuollon, etähallittaviin sekä mobiililaitteisiin, ohjelmistoihin ja ihmiseen toimintaan esimerkiksi salasanojen ja järjestelmien käytön kautta (Kyberturvallisuuskeskus 2016).

Terveydenhuollon organisaatioihin voi kohdistua kyberturvallisuuteen liittyviä uhkia esimerkiksi kyberturvallisuushyökkäysten kautta. Kyberhyökkäyksistä voi aiheutua uhkia hoidon tai palveluiden häiriönä, henkilöstölle kohdistettuina huijaussähköposteinä tai väärennetyinä verkkosivustoina, potilastietojen menetyksenä, tietomurtoina, tietojen vuotamisena, arvon menetyksenä, kiristyksenä, immateriaalioikeuksien varastamisena tai tahattomana tai tarkoituksellisena sisäpiiriläisen uhkana. (Piggin 2017, s.5) Kyberhyökkäyksien aiheuttamat uhkat terveydenhuollossa Piggin (2017) mukaan on listattuna taulukkoon 2.

Terveydenhuollon organisaatioiden kyberhyökkäysten aiheuttamia uhkia
Hoidon tai palvelun häiriöt
Henkilöstölle kohdistetut huijaussähköpostit ja kirjautumistunnuksia kalastelevat huijausverkkosivustot
Potilastietojen menetykset mukaan lukien sähköiset terveystiedot
Tietomurrot, tietojen vuotamiset ja arvon menetykset
Kiristykset esimerkiksi arkaluontoisien terveystietojen avulla
Immateriaalioikeudet
Tahaton tai tarkoituksenmukainen sisäpiiriläisen uhka luottamuksellisen aseman avulla organisaatiossa

Taulukko 1. *Piggin (2017) mukailen taulukko kyberhyökkäysten aiheuttamista uhista terveydenhuollon organisaatioissa.*

Norri-Sederholmin et al. (2019) mukaan terveydenhuollon kyberturvallisuusuhkiin kuuluvat erilaiset potilaiden hoitoon tai sen toimenpiteisiin sekä palveluihin kohdistuvat häiriöt. Näiden potilashoitoon liittyvien häiriöiden vaikutukset voivat olla todella mittavat, sillä vakavat ja pitkään jatkuvat häiriöt voivat johtaa jopa potilaan kuolemaan. Potilaiden hoitoon liittyy myös uhkat potilastietojen menetyksestä erityisesti digitaalisessa muodossa ja elektronisesti turvattuna (Norri-Sederholm et al. 2019).

Potilashoidon uhkien lisäksi kyberturvallisuusuhkia muodostavat erilaiset tietomurrot, kiristykset ja immateriaalioikeuksien varastamiset. Tietomurroissa, tietojen vuotamisissa ja arvon menetyksissä kaikissa on yhtenäisenä uhkana arvokkaan ja usein luottamuksellisen tiedon menettäminen, joissa uhreina voivat olla niin organisaatiot kuin henkilötkin. Myös kiristykset ja arkaluontoisten tietojen vuotamisella uhkailu ja pakottaminen ovat todellisia kyberuhkia, joissa hyödynnetään ihmisten luottamuksellisia tietoja ja niiden jakamista kiristyksen kohteena. (Norri-Sederholm et al. 2019)

Kyberuhkia luovat myös erilaiset ihmisiin liittyvät ja kohdistuvat huijaukset ja sosiaaliset manipuloinnit. Kyberuhkia terveydenhuollossa liittyen ihmisen toimintaan ovat Norri-Sederholmin et al. (2019) mukaan henkilöstön harhauttaminen huijaussähköposteilla tai väärennetyillä verkkosivustoilla henkilökohtaisten tietojen saamiseksi tai haittaohjelmien levittämiseksi. Ihmisten kautta voidaan toteuttaa myös niin kutsuttua sisäpiiriläisten uhkaa tahattomasti tai tarkoituksellisesti. Sisäpiiriläisen uhalla tarkoitetaan uhkaa liittyen sisäpiiriläisten luottamukselliseen asemaan ja statukseen organisaatioissa. (Norri-Sederholm et al. 2019)

Kyberhyökkäyksiä, -haavoittuvuuksia ja -uhkia voidaan tarkastella viisikerroksisen kybermaailman hierarkkisen verkostomallin mukaisesti. Hierakkinen verkostomalli sisältää fyysisen, syntaktisen, semanttisen, palvelun ja kognitiivisen kerroksen. (Norri-Sederholm et al. 2019) Tämä viisikerroksinen malli perustuu Libickin (2007) nelikerroksiseen malliin kybermaailman rakenteesta hyödyntäen OSI-mallia (Open Systems Interconnection Reference Model) (Libicki 2007). Taulukossa 1 viisikerroksista mallia kybermaailmasta on sovellettu terveydenhuollon toimintaympäristön ja siinä olevien uhkien kuvaamiseen muokaten Norri-Sederholm et al. (2019) taulukkoa.

Fyysinen kerros

- Sisältö: Tiedonsiirtoverkko ja kytketyt laitteet, kiinteät ja langalliset yhteydet
- Hyökkäykset: Laitteiden varkaudet, katoamiset ja tuhoamiset sekä komponenttitason saastutus

Syntaktinen kerros

- Sisältö: Järjestelmien ohjaus- ja hallintalaitteet, liityntäteknologiat ja verkkoprotokollat
- Hyökkäykset: Laitteiden haltuunotot ja saastutukset haittaohjelmilla

Semanttinen kerros

- Sisältö: Informaatio- ja tietosisällöt käyttäjien hallitsemana ja järjestelmän toimintojen ohjaus
- Hyökkäykset: Tietojen varastus, tuhoamiset, saastutukset, väärentämiset sekä tiedon luottamuksellisuuden, eheyden ja saatavuuden estäminen ja lunnashaittaohjelmat

Palvelukerros

- Sisältö: Kaupalliset ja julkiset verkkopalvelut ja kansalaisten palvelut
- Hyökkäykset: Palvelunestohyökkäykset, palvelusivustojen saastutus

Kognitiivinen kerros

- Sisältö: Inhimillinen ongelmanratkaisu- ja tulkintaympäristö sekä informaation merkityssisällön ymmärtäminen ja tulkinta
- Hyökkäykset: Tietojen kalastelu, pelotteluohjelmat ja identiteettivarkaudet

Taulukko 2. Libickin (2007) kybermaailman rakennetta mukaileva viisikerroksinen malli terveydenhuollon toimintaympäristöstä.

Fyysinen kerros voidaan ajatella kattavan tiedonsiirtoverkon ja siihen kytketyt laitteet sekä kiinteät ja langattomat yhteydet (Norri-Sederholm et al. 2019). Fyysisen kerroksen haavoittuvuudet liittyvät muun muassa puutteelliseen fyysiseen suojaukseen, suojaamattomiin WLAN-verkkoihin ja laitteisiin sekä verkkosalauksien puutteisiin (Lehto 2017). Fyysisen kerroksen haavoittuvuuksia on lisännyt terveydenhuollon vahva suuntautuminen paperittomiin materiaaleihin ja tietosisältöjen liikkuminen digitaalisesti yli organisaatiorajojen, millä on voitu edistää potilaan hoitoa ja turvallisuutta. Samalla kuitenkin terveydenhuollon laitteiden määrä on noussut ja laitteet ovat kehittyneet teknisiltä ominai-

suuksilta. Laitteiden kehityksen myötä ne ovat myös yhä enenevässä määrin tietoverkkoon liitettävissä ja niillä on potilastietojärjestelmiin integraatorajapintoja. (Norri-Sederholm et al. 2019)

Fyysisessä kerroksessa tapahtuneet raportoidut hyökkäykset ovat laitevarkauksia ja kiinteistä tuhoamista (Norri-Sederholm et al. 2019). Laitevarkauksia on tapahtunut ympäri maailmaa ja kohdistuen monenlaisiin laitteisiin. Hakkeroinnit ovat myös osana fyysisen kerroksen hyökkäyksiä ja ovat olleet yleisimpiä hyökkäystapoja terveydenhuollon organisaatioihin. (Lehto & Lehto 2017) Hakkerointien tarkoituksena on saada potilastiedoista henkilökohtaisia tietoja ja tunnuksia sekä terveys- ja luottotietoja muun muassa identiteettivarkauksiin (Norri-Sederholm et al. 2019).

Syntaktiseen kerrokseen kuuluvat erilaiset järjestelmien ohjaus- ja hallintalaitteet, liityntäteknologiat ja verkkoprotokollat (Norri-Sederholm et al. 2019). Syntaktisessa kerroksessa tapahtuvat haavoittuvuudet ovat useimmiten seurausta puutteellisista valvontajärjestelmistä, vajavaisesta tai epätarkasta kokonaiskuvasta kyberturvallisuuden tilanekuvasta ja järjestelmien heikoista suojaustasoista (Lehto 2017). Terveydenhuollon organisaation tietoverkoille on tyypillistä, että niihin on liitettynä työasemia, palvelimia sekä terveydenhuollon laitteita. Norri-Sederholmin et al. (2019) mukaan erityisesti terveydenhuollon laitteet aiheuttavat kyberturvallisuuden uhkia, joka johtuu etäyhteyksien käytöstä, käyttöoikeuksien epäselvyydestä ja tietosuojan edellyttämistä toimista. Lisäksi uhkien olemassaoloa lisää heikosti suojatut yhteydet ja käyttäjien tunnistamiset (Kyberturvallisuuskeskus 2016). Virustentorjunnan näkökulmasta terveydenhuollon laitteet ovat haasteellisia, sillä Williamsin & Woodwardin (2015) mukaan niitä ei voida asentaa osaan laitteista ollenkaan ja Vartiaisen (2017) mukaan osaan laitteista voidaan asentaa vain laitevalmistajan hyväksymiä tietoturvaohjelmia.

Semanttisen kerroksen sisältöön kuuluvat käyttäjien hallitsemat informaatio- ja tietosivallöt sekä järjestelmän toimintojen ohjaus (Norri-Sederholm et al. 2019). Semanttisen kerroksen uhkat muodostuvat puutteellisesta tai heikosta tietosuojauksesta, varmuuskopioinneista ja ohjelmistosuunnittelusta ja -tuotannosta (Lehto 2017). Tämän kerroksen haavoittuvuuksia hyödyntämällä kyberrikolliset voivat suorittaa mielivaltaisesti erilaisia komentoja, levittää haittaohjelmia ja vuotaa salatuiksi tiedoiksi luokiteltuja tietoja (Norri-Sederholm et al. 2019). Haavoittuvuuksia on mahdollista hyödyntää haittaohjelmien käytössä, jonka avulla on mahdollista saada haltuunsa jopa korotettuja käyttöoikeuksia (Lehto & Lehto 2017).

Semanttisen kerrokset tyypilliset uhkat liittyvät haittaohjelmiin, joita pyritään levittämään esimerkiksi sähköpostien kautta. Olemassa olevien uhkien vuoksi on merkityksellistä

varmuuskopioida tiedostoja ja tietoja säännöllisesti, sillä uhkissa korostuvat tietojen tuhoamiset sekä vääristämiset ja kiristyshaittaohjelmat. (Norri-Sederholm et al. 2019) Semanttisen kerroksen uhkat ja haavoittuvuudet ovat kyberrikollisille erityisen kiinnostavia terveydenhuollossa, sillä onnistuessaan ne luovat vaikuttavat merkittävästi terveydenhuollon organisaatioiden toimintaan (Lehto & Lehto 2017). Esimerkiksi kiristyshaittaohjelmat onnistuessaan vaikuttavat vahvasti toimintaan terveydenhuollon organisaatioiden nojatessa käytännössä kokonaan sähköisiin potilasjärjestelmiin ja tietoihin sekä työasemiin ja laitteisiin (Norri-Sederholm et al. 2019).

Palvelukerroksessa käsitellään julkisia ja kaupallisia verkkopalveluita sekä kansalaisten palveluita (Norri-Sederholm et al. 2019). Kerros sisältää kyberturvallisuuteen liittyvän johtamisen ja hallinnoinnin sekä ohjelmistotuotannon ja turvallisuusprosessit (Lehto 2017). Terveydenhuoltoon ja sen toimintaan liittyy monenlaisia palveluita kansalaisille ja julkisia verkkopalveluita kuten esimerkiksi Kanta-palvelut sisältäen kaikkien terveydenhuollon toimijoiden potilaskertomukset ja OmaKanta-palvelu, jossa kansalaiset pääsevät käsiksi omiin potilas- ja terveystietoihinsa (Norri-Sederholm et al. 2019).

Palvelukerroksen uhkat muodostuvat suoraan palveluiden kyberturvajohtamisen ja -hallinnoinnin, ohjelmistotuotannon sekä turvallisuusprosessien puutteista (Lehto 2017). Kyberturvallisuuden johtamisessa uhkana on hajautettu terveydenhuolto, joka toteutuu eri yksiköissä ja organisaatioissa (Soininen 2016). Palveluiden kokonaisuhkakuvassa esiintyy myös organisaatioiden liian positiivinen näkemys suojauksen tasosta kyberturvallisuuden suhteen (Norri-Sederholm et al. 2019). Palvelukerroksen hyökkäykset voivat olla esimerkiksi palvelunestohyökkäyksiä, joiden tarkoituksena on kuormittaa verkkoliikennettä niin paljon, että palveluiden käyttö hidastuu merkittävästi tai ne eivät toimi ollenkaan (Lehto & Lehto 2017).

Kognitiivisessa kerroksessa tarkastellaan inhimillistä ongelmanratkaisu- ja tulkintaympäristöä sekä informaation merkityssisällön ymmärtämistä ja tulkintaa. Norri-Sederholm et al. (2019) mukaisesti kerros sisältää tiedon, osaamisen ja kompetenssin puutteet sekä vajavaisen kybertilannetietoisuuden. Kognitiivisessa kerroksessa korostuvat terveydenhuollon ammattilaisten ja muiden työntekijöiden kohdistuvat kyberhyökkäykset kalasteluviestien kautta. Kalasteluviestejä voidaan lähettää terveydenhuollon työntekijöille sähköpostitse ja haittaohjelmia voidaan levittää sähköpostin lisäksi verkkosivustojen ja -mainosten sekä sosiaalisen median kautta (Piggin 2017). Kognitiivisen kerroksessa korostuvan ihmisen toiminnan myötä uhkat muodostuvat organisaatioille ihmisten huonosta ja vajavaisesta kyberturvakäyttäytymisestä sekä -kouluttamattomuudesta (Williams & Woodward 2015).

2.5 Toteutuneita kyberriskejä ja -uhkia terveydenhuollon toimintaympäristössä

Terveydenhuollon ja sen alan organisaatioiden on kriittisinä kansallisina toimijoina suojauduttava ja varauduttava erilaisiin kyberuhkiin ja -riskeihin kokonaisvaltaisesti ja kattavasti (Norri-Sederholm et al. 2019). Identiteettivarkaudet, lunnasohjelmat ja valtiollisiin toimiin kohdistetut hakkeroinnit osoittavat, että terveydenhuollossa käsiteltävät tiedot ovat haavoittuvaisia (Csulak et al. 2017). Kyberturvallisuuden sanaston (2018) mukaisesti kyberturvallisuuteen kuuluvat ne toimenpiteet, joilla voidaan hallita ja tarvittaessa myös sietää kyberuhkia ja niistä mukana tulevia vaikutuksia. Kyberturvallisuuden voidaan nähdä perustuvan haavoittuvuuksien ymmärtämiseen tieto- ja tietoliikennejärjestelmissä ja integroiduissa informaatioteknologiaa sisältävissä järjestelmissä. Nämä eri järjestelmät puolestaan sisältävät toimijaorganisaation toimintaa edellyttäviä, kriittisiä tietoja ja toiminnallisuuksia. (Remedyi & Wilson 2018)

Kyberriskien määrä on noussut terveydenhuollossa. Vuoden 2015 KPMG:n teettämän kyberturvallisuuteen liittyvän kyselyn mukaan yli 80% terveydenhuollon organisaatioista oli ollut kyberhyökkäyksen uhrina kahden viimeisen vuoden aikana. Samassa kyselyssä ilmeni myös, että vain puolet kohteeksi joutuneista organisaatioista olivat varautuneet kyberhyökkäykseen riittävällä tasolla. (Piggin 2017) Potilashoidon mahdollistamiseksi ja kehittämiseksi kerättyjä tietoja voidaan käyttää rikollisiin tarkoituksiin esimerkiksi petosten, identiteettivarkauksien ja toimitusketjujen häiriöihin (Csulak et al. 2017). Kyberhyökkäysten ja kyberrikollisten suurimpana intressinä on saada mahdollisimman paljon potilastietoja esimerkiksi kiristyshaittaohjelmien avulla sekä saada potilastietojen palauttamisesta maksuja. Tällaisia kyberhyökkäyksiä on tapahtunut sairaaloissa ja muissa terveydenhuollon organisaatioissa esimerkiksi Yhdysvalloissa, Isossa-Britanniassa ja Australiassa. (Piggin 2017) Merkityksellisin seuraus kyberhyökkäyksistä ja -rikoksista on potilashoidon häiriintyminen (Csulak et al. 2017).

Myös terveydenhuollon järjestelmiin on kohdistunut hyökkäyksiä yleisesti julkisen verkon käytössä tai paikallisissa järjestelmissä. Tällöin hyökkäykset eivät ole vaikuttaneet suuresti kansallisiin palveluihin. Ulkopuoliset kyberhyökkäykset ovat usein olleet palvelunestohyökkäyksiä ja ne ovat kohdistuneet muun muassa Kanta-palveluihin, verkon kriittisiin palveluihin tai julkisen verkon kautta yhteyksiä käyttävien palveluntarjoajien toimintaan. (Sosiaali- ja terveystieteiden ministeriö 2019)

2.5.1 Haittaohjelmat

Terveydenhuollon toimijoihin on kohdistunut viime vuosina kyberrikollisten suosimia kyberhyökkäyksiä muun muassa kiristyshaittaohjelmien kautta. Aikaisemmin kiristyshaittaohjelmien kohderyhminä ovat olleet lähinnä palvelu-, teollisuus- ja pankkialojen toimijoita, mutta terveydenhuollon toimijat ovat tulleet yhä enemmän ja enemmän kiinnostavimmiksi kyberrikollisille suurten tietomassojen myötä. (Sosiaali- ja terveysministeriö 2019) Kiristyshaittaohjelmilla tehdyt hyökkäykset ovat osoittaneet, että tietoverkkojen ja laitteiden haavoittuvuuksia käytetään yhä laajemmin hyödyksi myös terveydenhuollon toimialalla (Csulak et al. 2017). Kiristyshaittaohjelmien kohderyhminä ovat niin yksityishenkilöt kuin organisaatiotkin ja ne aiheuttavat globaalisti jopa satojen miljoonien dollarien tappioita. Haittaohjelmien tarkoituksena on saastuttaa kohteen tietokone ja sen jälkeen salaamaan koneen tiedostot. Tämän jälkeen tiedostojen salauksen purkamisesta ja palauttamisesta vaaditaan tyypillisesti lunnaita. Haittaohjelmilla voidaan myös kuormittaa kohteena olevan tietokoneen resursseja, jolloin terveydenhuollon toimintaan liittyvät järjestelmät eivät toimi normien mukaisesti tai siinä esiintyy hidastumista. (Sosiaali- ja terveysministeriö 2019) Lisäksi haittaohjelmat voivat aiheuttaa potilashoitoon keskeytyksiä järjestelmän murtautumisten myötä (Csulak et al. 2017).

Yhtenä esimerkkinä kiristyshaittaohjelmasta terveydenhuoltoon kohdistuneena on WannaCry, joka aiheutti laajasti eri toimialojen organisaatioihin kansainvälisesti haittaa vuonna 2017. Iso-Britanniassa haittaohjelma vaikutti kansallisessa National Health Service -järjestelmässä laajasti vähäisen tietoverkkosegmentoinnin ja päivittämättömien tietokoneiden vuoksi. (Sosiaali- ja terveysministeriö 2019) Haittaohjelma ja hyökkäys käytti Windows-järjestelmän haavoittuvuutta ja se levisi erityisesti vanhentuneiden työasemien kautta (Norri-Sederholm et al. 2019). WannaCry-kiristyshaittaohjelma levisi työasemille, jossa se lukitsi käyttäjiä ulos ja lukitsi tiedostoja (Clarke & Youngstein 2017). Myös Suomessa Turun yliopistollinen sairaala joutui WannaCryn uhriksi ja lääkinnällisten, kuvantamisen laitteiden tietokoneet saastuivat haittaohjelmasta. WannaCry aiheutti potilashoidon viivästymistä ja jopa estämistä (Sosiaali- ja terveysministeriö 2019).

Kiristyshaittaohjelmien lisäksi haittaohjelmia on käytetty Lahden kaupungin tietoverkossa ulkopuolisen tahon tarpeisiin, jonka myötä kaupungin tietokoneiden laskentateho väheni ja häyttasi yli viikon ajan kaupungin tietoverkkoon liittyvää toimintaa. Haittaohjelma Wannaminen tarkoituksena oli käyttää tietokoneita kryptovaluutan louhimiseen. Laskentatehon laskemisen takia potilasjärjestelmät olivat poissa käytöstä eikä potilaiden tietoihin ollut pääsyä. (Vaarama 2019)

2.5.2 Tietomurrot

Norri-Sederholm et al. (2019) mukaan tietomurrot ovat olleet yleisimpiä terveydenhuoltoon kohdistuvia hyökkäyksiä erityisesti potilas- ja henkilötietojen varastamiseksi. Tietomurtojen yleistymistä selittää järjestelmien valtaviin henkilökohtaisten tietojen, nimien, henkilötunnusten ja maksutietojen määrä. Näitä tietoja voidaan käyttää muun muassa identiteettivarkauksissa ja tietojenkalasteluissa. (Norri-Sederholm et al. 2019).

Tietomurtoja on tapahtunut hakkereiden tekemänä sairaaloihin ja muihin terveydenhuollon toimijaorganisaatioihin ympäri maailmaa. Vuonna 2022 marraskuussa hakkerit keräsivät varastaneensa lokakuussa tehdyssä tietomurrossa lähes 270 000 potilaan henkilötietoja ja sosiaaliturvatunnuksia Yhdysvalloissa, Louisianan Lake Charliessa olevasta sairaalasta (Kullas 2022). Singaporessa vuonna 2018 tapahtui hakkerointi terveydenhoitoalan instituutioiden isoimpaan tietokantajärjestelmään ja 1,5 miljoonan potilastiedot varastettiin sis. osoitteita, syntymäaikoja. Erityisen tästä tietomurrosta teki hakkereiden yritys saada erityisesti pääministeri PM Leen ja muiden ministerien terveystietoja käsiinsä. (Tham et al. 2018)

Suomessa yksi isoimmista tietomurroista terveydenhuollon toimialalla tapahtui vuonna 2020 syksyllä Vastaamon tietomurrossa. Vastaamon tietomurron seurauksena yksityisen psykoterapiakeskuksen potilas- ja henkilötietoja vuodettiin asiakkaista. Vastaamon tapaus toimii varoittavana esimerkkinä terveydenhuollon toimialan kiinnostavuudesta kyberrikollisten näkökulmasta. Potilas- ja henkilötietojen turvaamisessa tulisi huolehtia riittävällä kyberturvallisuuden tasolla ja tietosuojaa parantavilla keinoilla. (Kortesoja 2022)

2.5.3 Palvelunestohyökkäykset

Kybermaailman mallin palvelukerroksessa hyökkäykset on yleisesti toteutettu palvelunestohyökkäyksinä (Norri-Sederholm et al. 2019). Palvelunestohyökkäyksessä tavoitteena on kohdistaa tietokoneilta mahdollisimman paljon liikennettä niin, että verkon toimintaa saadaan mittavasti häirittyä tai keskeytettyä (Vaarama 2019). Palvelunestohyökkäyksissä ei suoranaisesti ole tarkoituksena saada potilastietoja haltuun, jolloin potilasturvallisuus ei ole vaarassa tietojen suhteen (Norri-Sederholm et al. 2019). Palvelunestohyökkäyksissä potilasturvallisuus voi kuitenkin sivullisesti vaarantua pidentyneiden odotusten ja tietojen saatavuuden heikentyessä järjestelmien ollessa kaatuneina.

Palvelunestohyökkäyksiä on tehty Suomessa terveydenhuoltoalan organisaatioihin ja esimerkiksi Pohjois-Karjalan sairaanhoitopiirissä vuonna 2015 palvelunestohyökkäys kohdistui ajanvarauksiin ja verkkosivustot eivät pyörineet. Palvelunestohyökkäyksessä tavoitteena oli kohdistaa tietokoneilta mahdollisimman paljon liikennettä niin, että verkon toiminta saatiin keskeytettyä. Tämä palvelunestohyökkäys on tulkittu jälkikäteen olleen

kiusantekoa, sillä tietoja ei informoitu varastetuiksi tai rahaa kiristettäväksi. (Vaarama 2019) Sairaaloiden lisäksi myös Kanta-palveluihin on kohdistunut useita palvelunestohyökkäyksiä. Esimerkiksi vuoden 2017 palvelunestohyökkäyksen takia tietoihin ei päästy käsiksi Kanta.fi, OmaKanta- ja Kelain-palveluissa. Näiden hyökkäysten vaikutukset eivät usein vaikuta kaikkiin Kanta-palveluihin ja esimerkiksi osa apteekkeista pystyi toimimaan tavanomaisesti vuoden 2017 palvelunestohyökkäyksen aikana. (Rautio 2017)

2.5.4 Tietojenkalastelut

Tietojenkalasteluyritykset ovat yleinen ja suosiossa oleva huijaustapa saada tietoja yksityisiltä henkilöiltä ja organisaatioilta (Sosiaali- ja terveysministeriö 2019). Tietojenkalastelulla tarkoitetaan erilaisia tapoja, joilla käyttäjältä pyritään saamaan henkilökohtaisia tai henkilötietoja käyttämällä huijaukseen sähköpostia, valheellisia verkkosivustoja ja haittaohjelmia. Tietojenkalastelussa hyödynnetään manipulatiivisia ja teknisiä keinoja. (Hahnagy, Fincher & Dreeke 2015).

Myös terveydenhuollon organisaatioissa henkilökunta voi saada esimerkiksi sähköpostitse tietojenkalasteluviestejä, mutta kalasteluviestejä ilmenee myös puhelimitse niin puheluilla kuin tekstiviesteilläkin. Tietojenkalastelu hyödyntää ihmisen inhimillisyyttä ja voi käyttää psykologista manipulointia toteuttaakseen hyökkäyksen (Hahnagy, Fincher & Dreeke 2015). Tietojenkalasteluviestejä lähetetään usein jonkin auktoriteetin, esimerkiksi tunnetun yrityksen, kuten Microsoftin, tai henkilön nimissä ja tarkoituksena on saada vastaanottaja syöttämään omia tietoja esimerkiksi linkin kautta päätyvälle sivustolle, jossa pyydetään kirjautumistietoja. Uhrin täyttämien tietojen avulla huijari voi saada organisaation sähköpostitilin käyttöön ja näin esimerkiksi käytettyä tiliä muihin huijausviesteihin, väärennetyjen laskujen eteenpäinviemiseen, saastuneiden materiaalien levittämiseen tai identiteettihuijauksiin. (Sosiaali- ja terveysministeriö 2019)

Tietojenkalastelu on yleinen tapa saada tietoja kaikilla eri toimialoilla ja organisaatioissa, mutta terveydenhuoltoalasta on tullut viime vuosina yhä kiinnostavampi kohde sen sisältämien suurien tietovarastojen myötä kyberrikollisille. Esimerkiksi Terveystaloon kohdistui vuonna 2020 tietojenkalastelu verkkoajanvarauksen haavoittuvuuden kautta ja näin yksittäisten henkilöiden henkilötunnuksia päätyi ulkopuolisten käsiin. Tietojenkalastelu tuli ilmi Terveystalon saaman kiristysviestin myötä, mutta haavoittuvuus oli ollut tiedossa jo aikaisemmin. (Uusitalo 2020)

Tietyn terveydenhuollon toimijan lisäksi kalastelua on tehty muun muassa Omakannan nimissä. Kyberrikolliset ovat tehneet huijausviestejä Omakannan nimissä ja niiden tarkoituksena on ohjata uhri huijausviestin kautta rikollisten luomalle verkkosivustolle, joka

muistuttaa ulkonäöltään Omakantaa. Huijausviestejä ja virheellisille sivustoille ohjaavia linkkejä on esiintynyt sähköposteissa, sosiaalisissa medioissa sekä verkon hakukoneissa. Huijauksien tarkoituksena on saada uhri kirjautumaan omien pankkitunnusten kautta sivustolle, jonka kautta rikolliset saavat pääsyn verkkopankkiin ja uhrin tileihin. (Pennanen 2022) Samankaltaista tietojenkalastelua on tapahtunut myös Oulun yliopistollisen sairaalan nimissä. Näissä tapauksissa henkilöille on soitettu puhelimitse ja pyydetty todentamaan henkilöllisyys verkkopankkitunnuksilla potilastietojen päivittämiseksi. (OYS:n nimissä tietojen kalastelua - sairaala ei koskaan kysy potilaiden verkkopankkitunnuksia 2020)

3. LÄÄKINNÄLLISTEN JA LÄÄKETIETEELLISTEN LAITTEIDEN KYBERTURVALLISUUS

Kyberturvallisuudella voidaan vaikuttaa negatiivisesti tai positiivisesti potilashoittoon. Huonolla ja vajavaisella kyberturvallisuudella voidaan vaarantaa potilastietoja ja vaikuttaa potilaan terveyteen heikentävästi (Norri-Sederholm et al. 2019). Yhtenä merkittävänä osa-alueena kyberturvallisuudessa ovat erilaiset lääketieteelliset ja lääkinnälliset laitteet, jotka kuuluvat terveydenhuollon organisaatioiden toimintaan vahvasti yhä enenevässä määrin (Sosiaali- ja terveysministeriö 2019). Lääkinnälliset laitteet ovat kehittyneet viime vuosien aikana tukemaan myönteistä vaikutusta potilaan hoitoon ja potilasturvallisuuden muun muassa tietojen liikuttavuudella ja digitaalisella saavutettavuudella. Tämä on kehittänyt terveydenhuollon laitteista tietoverkkoon liitettäviä ja ne sisältävät integraatiopintoja potilastietojärjestelmiin. (Norri-Sederholm et al. 2019). Kuvassa 1 lääkinnälliset laitteet kuvataan osana terveydenhuollon toimintaympäristöä, johon kuuluu tietosuoja, sähköiset potilastiedot, kyberfyysiset järjestelmät ja IoT eli Internet of Things (Piggin 2017).



Kuva 1. Piggin (2017) mukainen kuvaus terveydenhuollon toimintaympäristöstä.

Terveydenhuollon organisaatioissa on paljon internetiin liitettyjä järjestelmiä ja lääketieteellisiä laitteita (Trapx Labs 2015). Tällaisessa ympäristössä lääkinnällisiä laitteita on suuri määrä käytössä ja yhä suuremmissa määrin laitteet ovat kytkettyinä internetiin, tietoverkkoihin sairaalassa sekä muihin laitteisiin (Sosiaali- ja terveysministeriö 2019). Näille laitteille on myös tyypillistä olla kytkettyinä sähköisiin potilastietojärjestelmiin (Trapx Labs 2015). Lääkinnällisten laitteiden määrää on edistänyt teknologian kehittyminen.

nen sekä ihmisten käyttötottumuksen myötä tapahtunut arkipäiväistyminen. Lääkinnällisten laitteiden määrän ja käytön yleistymisen tuovat haasteen kyberturvallisuudesta ja sen turvaamisesta, jota ei välttämättä osata ottaa huomioon hyväksyntäkriteereissä esimerkiksi muuttuvien uhkien ja riskien suhteen. (Sosiaali- ja terveysministeriö 2019) Lisäksi terveydenhuollossa kyberturvallisuuden huomiointi keskittyy edelleenkin suurimmalta osin potilastietojen suojaamiseen, jolloin kyberturvallisuuteen liittyvät muut uhkat jäävät huomioimatta (Pöyhönen et al. 2019).

Lääketieteelliset laitteet yhdessä muiden laitteiden ja potilastietojärjestelmien kanssa muodostavat toisiinsa vahvasti liitetyn yhteisön, jossa käsitellään arvokasta dataa ja tietoa ja käytetään haavoittuvimpia laitteita (Trapx Labs 2015). Lääkinnällisten laitteiden kehityskulku on jatkunut osaksi esineiden internetiä ja sen jatkuvaa laajentumista. Tulevaisuudessa voidaan nähdä, että lääkitieteelliset laitteet tulevat olemaan osana IoT-laitteiden käytön lisääntymistä, mikä tarkoittaa monien digitaalisen tiedon välittämistä, kokoamista ja hyödyntämistä monien miljardien älykkäiden laitteiden ja sensorien avulla. (Lehto et al. 2019, s.9) Lääkinnällisten laitteiden jatkuva kehitys on mahdollistanut laitteiden kytkemisen toisiin laitteisiin ja internetiin, joiden avulla laitteiden avulla on voitu kehittää tehokkaampia ja jopa uusia hoitomenetelmiä sairaalaympäristöihin, terveydenhuollon toimijoille sekä kotihoitoon. Tällöin lääkitieteellisten laitteiden käyttöä on saatu laajenemaan sairaaloiden ulkopuolelle ja näin myös huolehdittua yhä kokonaisvaltaisemmin potilaiden hoidosta. Kokonaisvaltaisemman hoitopolun tarjoaminen tarkoittaa lääkitieteellisten laitteiden ja koko terveydenhuollon järjestelmien suhteen myös tarvetta huomioida kokonaisvaltaisesti erilaisista terveydenhuollon toimintaympäristöistä ja sen laitteista, sovelluksista ja muista siihen liittyvistä asioista. (Sosiaali- ja terveysministeriö 2019) Kyberhyökkäyksien kohdistuessa yhä enemmän terveydenhuollon toimijoihin ja hyökkäysten määrän kasvaessa myös lääkitieteellisten laitteiden yritykset yhdessä terveydenhuollon organisaatioiden kanssa joutuvat kohteiksi erilaisille kyberhyökkäyksille, jotka ovat yhä kehittyneempiä ja kohdistettuja tai kohdistamattomia (Piggin 2017).

3.1 Lääkitieteelliset laitteet terveydenhuollossa

Lääkitieteellisiin laitteisiin liittyy monien digitaalisten laitteiden kautta kyberturvallisuusriskejä, jotka tulevat todennäköisesti määrällisesti kasvamaan teknologian kehittyessä (Euroopan Parlamentin ja Neuvoston asetukset 2017). Lääkitieteellisten laitteiden määrä tulee kasvamaan ja toimiala kehittymään, sillä lääkitieteellisten laitteiden kehityksellä pyritään vastaamaan terveydenhuollon alan digitalisaatioon liittyviin uusiin haasteisiin ja tarpeisiin (Aram et al. 2016). Lääkitieteelliseksi laitteeksi luokitellaan esimerkiksi instrumentit, laitteistot ja ohjelmistot, jotka valmistaja on tarkoittanut ihmisille käytettäväksi lääkitieteellisiin

tarkoituksiin muun muassa sairauden tai vamman diagnosointiin, tarkkailuun ja hoitoon (Euroopan Parlamentin ja Neuvoston asetus 2017). Lääkintälaitteita valvotaan lääkintälaitedirektiivillä, joka koskee kaikkia lääkinnällisiä laitteita sekä kaikkia laitteisiin liitettäviä tarvikkeita ja käyttöön tarvittavia ohjelmistoja. Direktiivi ottaa kantaa näihin laitteisiin ja tarvikkeisiin, joita käytetään ihmisten sairauksien diagnosointeihin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen, vammojen tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin, anatomian tai fysiologisen toiminnon tukemiseen, korvaamiseen tai muunteluun tai hedelmöityksen säätelyyn. (Lääkintälaitedirektiivi 93/42/ETY) EU-tason asetus 2017/745 lääketieteellisten laitteiden yhdenmukaisista säännöistä EU:n jäsenmaissa (Euroopan Parlamentin ja Neuvoston asetus 2017).

Lääkintälaitedirektiivin 93/42/ETY tarkoituksena on määritellä vaatimuksia laitteiden suunnitteluun, valmistukseen ja käyttöön, jotta laitetta käytettäisiin turvallisesti vaarantamatta potilaan, käyttäjän tai muiden henkilöiden terveyttä ja turvallisuutta (Lääkintälaitedirektiivi 93/42/ETY). EU-tason direktiivien lisäksi lääketieteellisten laitteiden käyttöä ohjaa Suomen lainsäädäntö, joka määrittää laissa terveydenhuollon laitteista ja tarvikkeista 629/2010 (Laki terveydenhuollon laitteista ja tarvikkeista 629/2010). Terveydenhuollon laitteiden ja tarvikkeiden käyttämistä ja valmistusta ohjaa Suomen lainsäädäntö, jossa on laitteiden käyttöön liittyviä määräyksiä turvallisuudesta käytössä ja suunnittelu- ja valmistusprosesseissa. Toiminnanharjoittajalla on laissa määritetty velvollisuus noudattaa valmistajan ohjeita kuljetuksesta, säilytyksestä, asennuksesta, huollosta ja muusta käsittelystä eli laitteen elinkaaresta toiminnanharjoittajan käytön aikana. Lainsäädännön tarkoituksena on edistää lääketieteellisten laitteiden ylläpitoa. Suomessa valvontavirasto Valvira valvoo toiminnanharjoittajien lääketieteellisten laitteiden käyttöä ja voi tehdä ilman ennakoilmoituksia käyntejä toiminnanharjoittajille valvomaan säädösten noudattamista. (L 24.6.2010/629).

Lääkinnällisten laitteiden ollessa tarkasti valvottuja ja määritelmien säädelyjä EU-tason direktiivien mukaisesti, käytetään diplomityössä käsitettä lääketieteellinen laite. Diplomityön tarkoituksena on tarkastella fyysisiä verkkoon liitettäviä lääketieteellisiä laitteita, jonka rajauksen takia ei voida käyttää tarkasti säädelyä lääkinnällisen laitteen nimikettä ja määritelmää. Fyysiset verkkoon liitettävät lääketieteelliset laitteet ovat kuitenkin lääkinnällisiä laitteita, mutta lääkinnälliset laitteet eivät kaikki ole fyysisiä verkkoon liitettäviä lääketieteellisiä laitteita. Tämän vuoksi käytetään diplomityössä tutkittavista laitteista nimikettä fyysinen verkkoon liitettävä lääketieteellinen laite, jolla tarkoitetaan lääkinnällistä laitetta, joka on fyysinen laite ja jolla on ominaisuus tulla liitettäväksi verkkoon. Rajaus fyysisiin laitteisiin on tehty, jotta tutkimuksessa jätettäisiin ulkopuolelle erilaiset lääkinnällisiksi laitteiksi luettavat ohjelmistot.

3.2 Lääketieteellisten laitteiden elinkaari ja kunnossapito

Lääketieteellisten laitteiden elinkaareissa tulisi huomioida kyberturvallisuuden riskit ja niiden arvioinnit ja vähentämistoimet osana riskienhallintaa. Kyberturvallisuusriskien huomiointia tulee tehdä laitteen käytön koko elinkaaren ajan lisäksi myös valmistuksen elinkaaren kaikissa vaiheissa suunnittelusta valmistukseen, testaukseen ja markkinoille pääsemisen jälkeiseen monitorointiin. (IMDRF 2020) Kyberturvallisuuden näkökulmasta lääketieteellisten laitteiden suunnittelussa haasteena on potilasturvallisuuden priorisointi välittömän turvallisuuden turvaamiseksi, jolloin kyberturvallisuuden huomiointi on jäänyt vähäisemmäksi (Pöyhönen et al. 2019). Kokonaisvaltainen suunnittelu kyberturvallisuuden parantamiseksi on merkityksellistä, sillä lääkinnällisten laitteiden kanssa operoivat yritykset ja organisaatiot joutuvat hallitsemaan ja suojautumaan jatkuvasti kehittyviltä kyberhyökkäyksiltä (Piggin 2017).

Terveydenhuollon organisaatioilla, jotka toimivat laitteiden käyttäjinä, on parhaimmat mahdollisuudet vaikuttaa lääketieteellisten laitteisiin ja niiden käyttöön laitteiden elinkaaren käytön aikana. Lääketieteellisten laitteiden pitkän käyttöiän vuoksi laitteiden kunnossapito on erityisen tärkeää ja hyvällä kunnossapidolla voidaan edistää tehokasta käyttöä ja parantaa laitteen käyttövarmuutta. (Dhillon 2009) Laitteiden käyttövaiheen kunnossapitoa voidaan edistää myös palveluntarjoajien kanssa yhteistyöllä erilaisten palveluiden kautta, joiden avulla lääketieteellisten laitteiden elinkaarta voidaan hallita kokonaisvaltaisemmin (Deloitte Centre for Health Solutions 2018). Hyvän kunnossapidon avulla voidaan laitteen käyttöikä pidentää ja vaikka huoltokustannukset voivat olla merkittävä osuus laitteen elinkaarikustannuksista, voivat vikaatilanteet olla loppujen lopuksi huoltokustannuksiakin korkeampia kalliimpia kustannuksia. (Dhillon 2009) Kunnossapitoa voidaan tarkastella viiden eri teeman kautta: huollon, ehkäisevän kunnossapidon, korjaavan kunnossapidon, parantavan kunnossapidon sekä vikojen ja vikaantumisen selvittämisen kautta (Järviö 2012, s.49).

Huollolla tarkoitetaan laitteen käyttöominaisuuksien ylläpitoa, toimintakyvyn palauttamista heikentyneestä tilasta tai vaurion syntymisen estämistä. Huoltoon sisältyy muun muassa laitteen tarkastus, säädöt, puhdistamiset ja muut mahdolliset toimenpiteet. Huoltoa tulisi tehdä säännöllisesti ja jaksotetusti riippumatta laitteen kunnosta. Ehkäisevässä kunnossapidossa tarkoituksena on tehdä säännöllistä ja tarpeen mukaista huoltoa sekä seurata laitteen suorituskykyä. Laitteen seuraamisella ja säännöllisillä huolloilla voidaan ehkäistä vikaantumisia ennen niiden ilmestymistä. Korjaavassa kunnossapidossa korjaukset tehdään laitteen vikaantumisen jälkeen osana suunnittelematonta häiriötä tai suunniteltua kunnostusta. Tavoitteena korjaavassa kunnossapidossa on saada viat kor-

jattua ja saada laite mahdollisimman nopeasti takaisin käyttöön. Parantavassa kunnossapidossa puolestaan halutaan parantaa laitteen käytettävyyttä ja luotettavuutta. Parantavassa kunnossapidossa voidaan päivittää osia tai komponentteja sekä tehdä uudelleensuunnittelua, jotta laitteesta voitaisiin saada nykyaikaisempi tai se voisi vastata uudistuneita vaatimuksia. Vikojen ja vikaantumisten selvittämisessä laitteesta pyritään selvittämään vikaantumista aiheuttava tekijä. Aiheuttavan tekijän löytyessä ja syyn selvittäessä voidaan suunnitella toimenpiteitä, joilla voitaisiin tulevaisuudessa estää vikaantuminen. (Järviö 2012)

Laitteen vikaantumisella tarkoitetaan tilannetta, jossa laite ei pysty suorittamaan laitteelta vaadittua toimintaa vaaditulla tavalla. Vikaantuneessa laitteessa sen suorituskyky ja käyttövarmuus ovat heikentyneet tai laitetta ei pysty välttämättä käyttämään ollenkaan sen toimimattomuuden tai vaarallisuuden takia. Vikaantumisia aiheuttavat yleensä monet tekijät, kuten esimerkiksi asennuksessa ja käytössä tapahtuvat virheet, laitteiden kuluminen käytössä sekä ulkoiset tekijät kuten onnettomuudet. Vikaantumiset voidaan nähdä johtuvan laitteiden ohjeiden vastaisesta käytöstä, käyttäjien ja kunnossapitäjien vähäinen osaaminen, ikääntyvien laitteiden toimintakykyjen korjaamattomuus, käyttöolosuhteiden riittämättömyys ja laitteiden suunnittelussa ei ole otettu huomioon käyttöön liittyviä todellisia tarpeita. (Järviö 2012)

Kokonaisuudessaan kyberturvallisuustoimenpiteitä tulisi toteuttaa ja huomioida lääketieteellisten laitteiden koko elinkaaren ajan ja jokaisessa vaiheessa (Aram et al. 2017). Vikaantumisten estämiseen on mahdollista vaikuttaa parhaiten laitteen säännöllisillä kunnottotarkastuksilla sekä käyttäjien kouluttamisella laitteen turvallisesta käytöstä. Vikaantumisten välttämiseksi on syytä kiinnittää huomiota laitteen toiminnan ylläpitoon, oikeisiin käyttöolosuhteisiin, toimintojen palauttamisiin uutta vastaavaan tilaan, suunnitteluvaiheen heikkouksien korjaamiseen sekä käyttö- ja kunnossapitotaitojen kehittämiseen. (Järviö 2012) Vikaantumisista voi seurata piileviä ja näkyviä toimintoja. Piilevät toiminnot eivät välttämättä vaikuta normaalikäytössä, mutta voivat aiheuttaa haittaa tavallisesta käytöstä poikkeavassa tilanteessa. Näkyvät toiminnot aiheuttavat haittaa normaalikäytössä, joka voi kokonaan estyä tai aiheuttaa jonkintasoista haittaa. (Mikkonen 2009)

3.3 Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet terveydenhuollossa

Nykyaikainen teknologia ja sen kehitys on luonut terveydenhuoltoalalle tarjoaman erilaisista lääketieteellisistä palveluista ja laitteista potilaille (Aram et al. 2017). Lääkinnälliset laitteet kattavat laajan valikoiman erilaisia laitteita ja siksi diplomityössä tutkittaviksi lääkinällisiksi laitteiksi rajataan tietoverkkoon kytkettävät fyysiset lääketieteelliset laitteet.

Fyysisillä lääkinällisillä laitteilla viitataan instrumentteihin, välineisiin, laitteisiin ja implanteihin, jotka ovat fyysisiä laitteita ja puolestaan erilaiset järjestelmät ja ohjelmistot rajautuvat ulos. Tietoverkkoon kytkettävien laitteiden määrä on kasvanut ja sitä kautta myös Euroopan unioni on pyrkinyt reagoimaan muun muassa uudella lääkintälaitteasetuksella lääkinällisten laitteiden turvallisuusvaatimuksiin. Näillä säädöksillä pyritään varmistamaan, että EU:n markkinoilla olevien laitteiden kyberturvallisuuden taso on tarpeeksi hyvä vastaamaan uusia teknologisia haasteita. Tietoverkkoon liitettävillä laitteilla on yhtenäisiä ominaisuuksia, jotka mahdollistavat laitteen yhdistämisen tietoverkkoon ja tämä luo erilaisia uhkia ja riskejä näihin laitteisiin. Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet ovat erityisen alttiita kyberturvallisuusriskeille, kuten esimerkiksi kyberhyökkäyksille, sillä laitteiden suojausmekanismit laitteissa itsessään eivät ole vahvoja (Aram et al. 2017).

Fyysisillä tietoverkkoon liitettävillä lääketieteellisillä laitteilla voidaan tarkoittaa esimerkiksi mobiililaitteita, puettavia ulkoisia laitteita, implantoitavia laitteita, kiinteitä laitteita ja tukilaitteita. Näitä laitteita käytetään nykyaikaisissa ja moderneissa terveydenhuollon toimijaorganisaatioissa ja näin potilashoitoa voidaan toteuttaa myös etäkäytössä mahdollistaen kuitenkin potilasvalvonnan. Mobiililaitteilla tarkoitetaan esimerkiksi glukosin mitauslaitetta. Puettavasta ulkoisesta laitteesta esimerkkinä toimivat kannettavat insuliinipumput ja langattomat lämpömittarit. Implantoitavilla laitteilla tarkoitetaan ihmiskehon sisälle laitettavia laitteita, kuten esimerkiksi sydämentahdistimia. Tietoverkkoon liitettävien sydämentahdistimien avulla voidaan sydämentahdistimiin suorittaa päivityksiä vähentäen laitteiden vaihtoväliä. Kiinteillä laitteilla tarkoitetaan isoja terveydenhuollon laitteita, joita voivat olla esimerkiksi tietokonetomografiat (CT), skannerit, elämää ylläpitävät laitteet ja kemoterapian jakeluasemat. Kiinteät laitteet yhdessä mobiililaitteiden kanssa ovat olleet jo pidemmän aikaa osana lähes kaikkien sairaaloiden kalustoa, mutta nykyaikaisemmalla toimijalla näitä laitteita voidaan käyttää osana päätöksentekoa yhdessä kliinisten tietojärjestelmien ja tunnistuskomponenttien kanssa. Tukilaitteet voivat olla erilaisia avustavia robotteja esimerkiksi kirurgisissa toimenpiteissä. (Enisa 2016)

Tehokkaasta ja toimivasta kyberturvallisuudesta on tullut merkittävä osa lääkinällisten laitteiden toimivuutta (IMDRF 2019). Laitteiden ja terveydenhuollon toimijoiden välisten parannettujen yhteyksien kehityksessä voidaan nähdä kuitenkin hyötyjen lisäksi haittoja. Potilashoidon ja -kulun toteuttamisen helpottamisen lisäksi varjopuolena on erilaiset kyberturvallisuushaasteet, kuten esimerkiksi terveystietojen häviäminen tai kaappaaminen. (Aram et al. 2017) Kyberturvallisuuden avulla voidaan terveydenhuollossa varmistaa toimivat ja turvalliset tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet, joiden turvallisuudesta on huolehdittava erityisellä tavalla niiden langattomien ja internettiä tai

tietoverkkoa hyödyntävien ominaisuuksien myötä (IMDRF 2019). Lääkinnällisten laitteiden valmistajien etäyhteydet valmistettuihin laitteisiin voivat aiheuttaa erilaisia haavoittuvuuksia. Valmistajien etäyhteydet mahdollistavat paremman valvomisen ja laitteiden vikojen ennakoitua sekä niiden korjaamista. Toisaalta etäyhteyksien ylläpitäminen tarkoittaa myös terveydenhuollon toimijoiden yhteyksien avaamista sisäverkkojen ja internetin välillä. Tämän toteuttaminen turvallisesti vaatii tarkkoja yksityiskohtia etäyhteyksistä ja huolellista toteutusta sekä valvontaa. (Sosiaali- ja terveysministeriö 2019, s.19) Turvallisen verkottamisen tueksi suositellaan standardinmukaisten IT-prosessien hyödyntämistä lääkitieteellisten laitteiden osalta (esimerkiksi ITIL). (Jauhiainen & Varri 2017, s.12)

IT-verkkojen ja lääkitieteellisten laitteiden yhdistämiseen liittyy kyberturvallisuusriskejä, jotka tulee ottaa huomioon ennen laitteen kytkemistä. Tyypillisesti nämä riskit liittyvät ohjelmistoihin, laitteisiin tai jonkin toimijan puutteeseen. Standardin SFS-IEC 80001-1 mukaisesti riskit liittyvät IT-riskien arviointipuutteisiin, valmistajan tuen tai turvallisuustarkastusten puutteeseen, laitteiden tai ohjelmistojen yhteensopimattomuuteen ja päivitysnopeuksien ristiriitaan. (Jauhiainen & Varri 2017, s.12)

Viime vuosien aikana terveydenhuollon alalla on nähty erilaisten kyberriskien realisoitumisia muun muassa kiristävirusohjelmia, palvelunestohyökkäyksiä ja kyberhyökkäyksiä. Nämä osoittavat minkälaisiin uhkiin verkottuvassa lääkitieteellisympäristössä tulee tulevaisuudessa pystyä vastaamaan. (Jauhiainen & Varri 2017) Kyberturvallisuushyökkäykset ja -häiriöt voivat tehdä tietoverkkoon liitettävistä lääketieteellisistä laitteista ja sairaalan verkoista toimintakyvyttömiä ja häiritä näin merkittävästi potilashoitoa terveydenhuollon organisaatioissa (IMDRF 2019). Kyberriskien ja -uhkien erilaistuessa ja määrrien kasvaessa tulee terveydenhuollon toimijoiden huolehdittava lääkitieteellisten laitteiden turvallisuudesta muun muassa sisäverkoissa liikkuvilta verkkoviruksilta ja -madoilta (Jauhiainen & Varri 2017, s.12). Tällaisten kyberhyökkäysten tapahtumat voivat pahimmillaan johtaa potilasvahinkoihin, virheellisiin diagnooseihin ja hoitoihin sekä hoidon viivästymisiin (IMDRF 2019). Kasvavat kyberturvallisuuden uhat asettavat haasteita lääkitieteellisten laitteiden käyttämiseen ja mahdollisen kyberhaitan tunnistamiseen sekä siitä toipumiseen. Lääkitieteellisten laitteiden käyttäjillä ja lääkitieteellisen henkilöstöllä tulee olla riittävä koulutus, jota tulee päivittää ajankohtaisesti, ja käytännön kokemusta tilannekuuvan luomiseen sekä toimenpiteiden johtamiseen ja toteuttamiseen toipumiseksi. Koulutuksen lisäksi yhteistyötä tulee ylläpitää tietoturva-asiantuntijoiden ja laite-edustajien kanssa. (Jauhiainen & Varri 2017, s.12)

3.4 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kyberturvallisuusuhat ja -haavoittuvuudet

Kyberrikolliset tavoittelevat terveydenhuoltoon liittyviä tietoja arvokkuuden ja taloudellisten hyötyjen vuoksi joko itsenäisinä toimijoina tai osana suurempaa ryhmittymää. Terveystiedot sisältäen vakuutustiedot voivat olla jopa 20 kertaa arvokkaampia kuin luottokorttitiedot mustilla markkinoilla. Terveystietojen arvokkaana pitäminen on jo yksi merkittävä syy kyberrikollisille, mutta terveydenhuollon haavoittuvuudet tekevät hyökkäyksistä entistä helpompia ja kiinnostavimpia. (Tapx Labs 2015). Lääketieteellisten laitteiden kanssa tekemisissä oleviin organisaatioihin on kohdistunut kyberhyökkäyksiä, jotka voivat olla kohdistamattomia tai kohdistettuja (Piggin 2017).

Terveydenhuollossa erityisesti verkotettuihin lääkinnällisiin laitteisiin kohdistuu kyberturvallisuushaavoittuvuuksia liittyen niiden kykyyn muodostaa yhteyksiä tietoverkkoihin ja siten olla yhteydessä muiden laitteiden ja järjestelmien kanssa. Lääketieteellisissä laitteissa haavoittuvuuksia on raportoitu olevan monenlaisissa laitteissa kuten esimerkiksi diagnoosilaitteissa, terapeuttisissa ja elämää ylläpitävissä laitteissa. Diagnoosilaitteisiin voivat kuulua esimerkiksi CT-skannerit, terapeuttisiin laitteisiin erilaiset pumput ja kirurgiset laitteet ja elämää ylläpitäviin laitteisiin dialyysilaitteet. (Enisa 2016) Lehto & Lehto (2017) ovat raportoineet terveydenhuollon laitteiden kyberturvallisuuden nykytilasta ja julkaisun mukaan laitteiden kyberturvallisuustasot vaihtelivat laitteiden välillä paljon. Vuoden 2015 TrapX Labsin tekemän tutkimusraportin mukaan suurimmassa osassa lääketieteellisiä laitteita ympäri maailmaa on haavoittuvuuksia ja alttiuksia kyberhyökkäyksiin.

Lääkinnällisten laitteiden nopean kehityksen myötä terveydenhuollon toimijoiden ja valmistajien on pystyttävä ottamaan kyberturvallisuus huomioon laitteiden koko elinkaaren ajan aina valmistuksesta käytön kautta hävittämiseen saakka. Yhdysvalloissa terveydenhuollon toimijoille KPMG:n teettämän kyselyn mukaisesti tietoturvaluolista kysyttäessä noin 30% vastaajista piti suurimpana huolena terveydenhuollon laitteiden turvallisuutta tai ikääntyvää tietotekniikkaa (KPMG 2015). Lääketieteellisten laitteiden haavoittuvuuksien, uhkien ja riskien näkökulmasta valmistajien, käyttäjäorganisaatioiden ja muiden kolmansien osapuolien tulee tehdä yhteistyötä, jotta uhkilta voitaisiin suojautua eri tasoilla ja tavoilla mahdollisimman kokonaisvaltaisesti (Norri-Sederholm et al. 2019).

Syntaktisen kerroksen haavoittuvuudet vaikuttavat lääkinnällisiin laitteisiin erityisesti tietoverkkojen, valvontajärjestelmien ja järjestelmien suojaustasojen kautta (Lehto 2017). Samaan tietoverkkoon voidaan liittää lääkinnällisten laitteiden lisäksi työasemia ja pal-

velimä, jotka voivat altistaa lääkinälliset laitteet työasemien haavoittuvuuksille (Vartiainen 2017). Verkon segmentointi on vähentänyt samoihin verkkoihin liittämistä, joka voidaan nähdä turvallisempänä tapana toimia. Toisaalta taas lääkinälliset laitteet luovat kyberturvallisuushaasteen, sillä niihin voidaan muodostaa etäyhteyksiä esimerkiksi huolto- ja vikatilaselvityksiä varten (Kyberturvallisuuskeskus 2016). Etäyhteyksimahdollisuudet luovat periaatteellisen mahdollisuuden kyberrikollisille hyökätä laitteiden kautta sairaalan muihin laitteisiin, mikäli yhteyksiä ei ole suojattu ja turvattu tarvittavilla teknisillä toimenpiteillä.

Terveydenhuollon laitteiden uhat muodostuvat pääasiallisesti ihmisten käyttäytymisestä, laitteiden käytöstä sekä teknisten haavoittuvuuksien ja riskien hallinnasta. Käyttäjänhallintaan liittyen lääketieteellisten laitteiden kyberturvallisuuteen vaikuttavat puutteelliset salasana ja niiden käytännöt (Williams & Woodward 2015). Ihmisen toimintaan liittyvistä uhista lääketieteellisiin laitteisiin liittyvät esimerkiksi USB-tikkujen ja muistikorttien käyttö (Lehto & Lehto 2017). Lääketieteellinen laite voi saada saastuneen USB-tikun kautta haittaohjelmataartunnan esimerkiksi laitevalmistajan huollon yhteydessä (Vartiainen 2017).

Lisäksi mobiililaitteiden käytöstä ja käyttäjien toiminnasta liittyen salasanoihin ja järjestelmiin muodostuu omat uhkansa terveydenhuollossa, mitkä voivat vaikuttaa lääkinällisten laitteiden ukiin välillisesti (Kyberturvallisuuskeskus 2016). Ihmisen toiminta liittyy moniin kyberturvallisuuden ukiin ja riskeihin, ja sitä kautta myös lääkinällisten laitteiden käyttöön. Williams & Woodwardin (2015) mukaan lääkinällisten ja muiden terveydenhuollon laitteiden ohjekirjoissa löytyy hyödyllisiä tietoja muun muassa haavoittuvuuksista. Jokaisesta terveydenhuollon laitteesta toimitetaan ohjekirja terveydenhuollon organisaatiolle lainsäädännön ja turvallisuusvaatimusten mukaisesti ja nämä ohjekirjat ovat valmistajan laatimia kattavia ohjekirjoja sisältäen kyberturvallisuuteen liittyviä huomioita (Williams & Woodwardin (2015).

Lääkinällisten laitteiden suojaukseen on vaikutettava inhimillisten virheiden ehkäisemisen lisäksi teknisin keinoin, sillä Lehdon & Lehdon (2017) mukaan monissa laitteissa on puutteellisia WLAN-yhteyksiä eikä niiden salauksista ole saatavilla olevaa tietoa kattavasti tai se on puutteellista. Heikosti tai puutteellisesti salatut laitteet ovat vaaraksi terveydenhuollossa, sillä ne voivat toimia portteina kyberrikollisille tunkeutua organisaatioiden tietoverkkoihin (Norri-Sederholm et al. 2019). Osa laitteista käytti myös salaamattomia liikenteitä ja helposti murrettavissa olevia WEP-salauksia. (Lehto & Lehto 2017)

Norri-Sederholm et al. (2019) mukaan terveydenhuollon uhkista lääkinällisiin laitteisiin erityisesti liittyvät terveydenhuollon laitteiden ohjelmistoista ja etähallittavista laitteista

muodostuvat uhkat. Haavoittuvuuksia voivat aiheuttaa lääkinnällisiin laitteisiin muodostettavat etäyhteydet, joita määrittävät ja hallinnoivat eri laitteiden valmistajat. (Sosiaali- ja terveysministeriö 2019) Lääkinnällisten laitteiden valmistajat vaikuttavat vahvasti laitteiden päivityksiin ja haittaohjelmilta suojautumisiin. Vaikka lääkinnälliset laitteet tai niiden ohjaustietokoneet olisivat terveydenhuollon toimijan tietoverkossa, terveydenhuollon organisaatioilla itsessään on rajallinen kyky suojata lääkinnällisiä laitteita esimerkiksi työasemien lailla ja saada laitteita esimerkiksi valvontaohjelmien piiriin. Terveydenhuollon laitteiden kuin työasemienkin päivittämättömyydet luovat haavoittuvuuksia toimijoiden ympäristöihin. Tämä tekee lääkinnällisistä laitteista helpon hyökkäyksen kohteen esimerkiksi haittaohjelmien levittämiseksi ja luo terveydenhuollon organisaatioille kyberturvallisuusuhkan. (Norri-Sederholm et al. 2019).

Lehdon (2019) mukaisesti kyberuhkina voidaan pitää kybervandalismia, -rikollisuutta, -vakoilua, -terrorismia, -sabotaasia ja -sodankäyntiä. Haavoittuvuudet puolestaan voidaan jakaa ihmisiin, prosesseihin ja teknologioihin. Lehto (2019) esittää kyberuhkien ja riskien hallinnan kokonaisuudessa kattavasti kyberuhkien, -haavoittuvuuksien ja -riskien sekä vastatoimenpiteiden kautta. Riskien arvot voidaan määrittää liiketoimintaan ja IPR:ään, maineeseen, oikeudelliseen tai EU:n yleiseen tietosuojasetukseen eli GDPR:ään sekä palautukseen ja korjaukseen. Vastatoimenpiteisiin kuuluvat kuvion mukaisesti kyberturvallisuuden johtaminen, kyberkulttuuri ja kybersuojaus. Kyberturvallisuuden johtaminen sisältää toimintaohjeet ja politiikat, implementaation ja osaamisen hallinta. Kyberkulttuurissa puolestaan vaikuttavat yhteisön arvot ja normit, sääntely ja yhteisöllisyys. Kybersuojauksessa puolestaan kiinnitetään huomiota riskienhallintaan, suojausteknologioihin ja resilienssiin. (Lehto 2019)

Vaikka haavoittuvuuksia ja uhkia on raportoitu terveydenhuollon laitteissa, on toimijoiden ja laitteiden väliltä löytynyt suuriakin eroja kyberturvallisuuden käytäntöjen ja ominaisuuksien suhteen. Terveydenhuollon laitteiden ison haavoittuvuuksien määrän lisäksi Lehto & Lehto (2017) raportoivat osan laitteista toimineen kyberturvallisuuden näkökulmasta riittävällä ja hyvällä tasolla. Teknisten ominaisuuksien ja yhteyksien näkökulmasta osasta laitteista löytyi WPA- ja WPA2-salauksien tukemista ja mahdollisuudet autentikointeihin. (Lehto & Lehto 2017). Tämä osoittaa, että laitteiden kyberturvallisuuden nykytila ja kyvykkyydet vaihtelevat riippuen laitteiden toimittajista sekä käyttäjäorganisaatioista.

3.5 Toteutuneita hyökkäyksiä fyysisiin tietoverkkoon liitettyihin lääketieteellisiin laitteisiin

Tietoverkkoon liitettäviin fyysisiin lääketieteellisiin laitteisiin kohdistuu kyberturvallisuus-hyökkäyksiä samalla tavalla kuin muihin verkkoon liitettäviin sairaalan laitteisiin ja työasemiin (Vartiainen 2017). Kyberrikolliset hyödyntävät lääketieteellisten laitteiden ominaisuutta olla yhteydessä terveydenhuollon toimijan tietoverkkoon. Hyökkäykset ovat mahdollisia tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kautta, sillä niiden kautta voidaan päästä internetiin tai niihin on päästy terveydenhuollon toimijan verkon ulkopuolelta. Lääketieteellisten laitteiden kautta tapahtuvat kyberhyökkäykset ovat yksiä keskeisimpiä tapoja kyberrikollisille tunkeutua terveydenhuollon organisaatioihin, sillä lääketieteelliset laitteet ovat näkyvimpiä haavoittuvuuksia terveydenhuollon toimijoiden ympäristöissä. Lääketieteellisten haavoittuvuuksien hyödyntämisen etuna hyökkäjille on myös se, että haavoittuvuuksia voi olla vaikeaa paikata ja hyökkäystä haastavaa tunnistaa ja estää. (Trapx Labs 2015)

3.5.1 Haittaohjelmat

Lääketieteellisiin laitteisiin on kohdistunut monia haittaohjelmia joko suoraan kohdistetuna tai työasemien kautta levinneenä. Työasemien kautta saastuttavien haittaohjelmien lisäksi lääkinnällisiin laitteisiin on kohdistettu omia haittaohjelmia. Symantecin (2018) mukaan terveydenhuoltoon kohdistunut Orangeworm-matohaittaohjelma oli erityisesti tarkoitettu terveystekniikan teollisuuteen ja laitteisiin. Orangewormin haittaohjelmaa on havaittu esimerkiksi röntgen- ja magneettikuvauslaitteiden ohjaustietokoneista. Haittaohjelmaa ei Symantecin mukaan ole Suomesta löytynyt, mutta puolestaan Ruotsissa ja Norjassa haittaohjelmaan kohdistuneista uhreista oli kokonaisuudessaan 2% molemmissa maissa. (Norri-Sederholm et al. 2019)

Lääketieteellisissä laitteissa yksi tunnetuimmista ja laajimmista haittavaikutuksista aiheuttanut haittaohjelma on WannaCry. WannaCry-haittaohjelma aiheutti kansainvälisesti suurta haittaa yli 200 000 työasemaan ja lääketieteelliseen laitteeseen esimerkiksi Yhdysvalloissa ja Isossa-Britanniassa. Varsinais-Suomen sairaanhoitopiirissä haittaohjelmaa löytyi kuvantamisen laitteista ja vaikutti noin kymmenen laitteen toimintaan. (Keränen 2017). Yhdysvalloissa haittaohjelmaa raportoitiin löytyneen fyysisissä verkkoon liitettävissä lääkinnällisissä laitteissa kuten esimerkiksi radiologian laitteita. Laitteita ja työasemia yhdisti Windows-järjestelmä, jossa hyödynnettiin vanhan käyttöjärjestelmän haavoittuvuutta. Monet isot lääketieteelliset laitteet, kuten röntgen-, magneetti- ja CT-kuvauslaitteet, käyttävät Windows-käyttöjärjestelmää. Haittaohjelmahyökkäyksen

vuoksi lääketieteellisten laitteiden käyttöön tuli katkoja, resurssien lisätarpeita, hoidon viivästymisiä ja mahdollisesti jopa klinisiä virheitä. (Brewster 2017)

Haittaohjelmien torjumisessa tärkeässä roolissa on tarkka valmistajien valinta lääketieteellisten laitteiden hankintavaiheessa. Suurimmassa osassa lääketieteellisiä laitteita vain valmistajat pystyvät tekemään tietoturvapäivityksiä ja hallitsemaan kyberturvallisuutta suojaavia ominaisuuksia laitteissa. Mikäli tarvittavia haittaohjelmien torjuntaohjelmia ei voida asentaa laitteisiin, haittaohjelmahyökkäykset uusiutuvat monesti aikaisemman haittaohjelman poistamisen jälkeen. Haittaohjelmien uusimista edistää työkalujen käyttö, jolla voidaan aiemmin käytetyistä haittaohjelmista muokata ja naamioda uusia haittaohjelmia helposti. Tällä tavalla hyökkääjät voivat tehdä uusia haittaohjelmia helposti ja nopeasti uudelleen ilman, että niitä tunnustetaan vanhoiksi haittaohjelmiksi. Tämän vuoksi terveydenhuollon kyberhyökkäyksiin voidaan käyttää vanhojakin haittaohjelmia kuten esimerkiksi Conflicker -haittaohjelmaa. Muuttuvia haittaohjelmia kutsutaan polymorfisiksi haittaohjelmiksi, jotka muuttuvat ajan myötä niin, etteivät haittaohjelmien torjuntaohjelmat niitä tunnista. Niiden perustoiminnot tai tavoitteet eivät muutu, mutta niiden haitallinen koodi, salaus, tunnisteet tai pakkaustapa voi muuttua. (Tapx Labs 2015).

3.5.2 Verkkoysteitä käyttävät kyberhyökkäykset

Lääkintälaitteisiin voi kohdistua verkon kautta tehtäviä hyökkäyksiä, joiden tavoitteena on päästä potilastietojärjestelmiin ja niiden sisältämiin potilastietoihin. Hakkerointi on erityisen merkityksellistä terveydenhuollon toimijaympäristössä, jossa kyberhyökkäyksen onnistuessa tietoverkkoon liitettäviä fyysisiä lääketieteellisiä laitteita voidaan käyttää osana hyökkäystä ja vahingoittaa. (Enisa 2016) Vaikka kyberturvallisuus olisikin huomioitu sisäverkon suojaamisessa ja työasemissa sekä palvelimissa, on lääkinnällisissä laitteissa tyypillisesti haavoittuvuuksia. Tietoverkkoon liitettävissä fyysisissä lääketieteellisissä laitteissa voi olla suora internet-yhteys ja tällöin haavoittuvuuksia on mahdollista käyttää hyödyksi haittaohjelmien avulla. Haittaohjelman avulla kyberhyökkääjän on mahdollista luoda niin kutsuttu takaovi, jonka kautta on mahdollista päästä sisäverkkoon. Sisäverkon kautta puolestaan hyökkääjät voivat päästä käsiksi ja saastuttaa isoon määrään lääketieteellisiä laitteita terveydenhuollon toimijan ympäristössä. (Enisa 2016)

Verkkoa voidaan hyödyntää myös palvelunestohyökkäyksissä. Hajautetuissa palvelunestohyökkäyksessä keskitytään estämään jotakin toimintaa kuten esimerkiksi tietojärjestelmän tai muun verkkoressurssin käyttämistä monien hyökkäyslähdeiden avulla. Hajautetuissa palvelunestohyökkäyksissä lääketieteelliset laitteet voivat olla osana niin sanottua bottiverkkoa. (Enisa 2016) Bottiverkolla tarkoitetaan kyberhyökkääjän tietoverkon

kautta haltuun ottamia tietokoneita ja laitteita (Turvallisuuskomitea 2018). Hajautettu palvelunestohyökkäys voidaan tehdä sairaan verkosta ulko- tai sisäpuoliseen kohteeseen. Terveystietojen toimijan sisäpuolelle kohdistuva palvelunestohyökkäys voi johtaa potilasjärjestelmien ja -tietojen käytettävyyden vaarantumiseen sekä lääketieteellisten laitteiden toimimattomuuteen tai tietojen vääristymiseen. Terveystietojen toimijoista esimerkiksi Boston Children's Hospital (BCH) joutui vuonna 2015 palvelunestohyökkäyksen kohteeksi, jossa hakkerioimalla asiaansa ajavat aktivistit hyökkäsivät sairaalan (Enisa 2016). Palvelunestohyökkäyksellä oli vaikutusta muun muassa sähköisten terveystietojen käytön suhteen, joka vaikuttaa myös tietoverkkoon liitettyjen fyysisten laitteiden käyttöön.

Tietoverkkoon liitetyt lääketieteelliset laitteet ja terveydenhuollon toimijat ovat palvelunestohyökkäyksille hyviä kohteita, sillä hajautetussa palvelunestohyökkäyksessä voidaan hyödyntää huonosti turvatoimenpiteitä noudattavia laitteita. Suurin hajautettu palvelunestohyökkäys vuoteen 2016 mennessä on tehty käyttämällä älylaitteita, joista on puuttuneet tiukat turvavaatimukset (Khandelwal 2016). Tämä luo kyberhyökkääjille mahdollisuuden luoda kyberhyökkäys terveydenhuollon toimijaa kohtaan, mutta myös kaapata ja käyttää tietoverkkoon liitettäviä lääketieteellisiä laitteita osana kyberhyökkäystä bottiverkossa.

3.5.3 Laitevarkaudet

Terveystietojen laitevarkaudet kuuluvat kybermaailman fyysisen kerroksen hyökkäykseen ja kyberrikollisia kiinnostavat niin perinteiset työasemat kuin lääketieteelliset laitteetkin (Norri-Sederholm et al. 2019). Perinteisten työasemien lisäksi lääketieteellisten laitteiden varkaudet ovat yleistyneet ja alkaneet kiinnostaa yhä enemmän kyberrikollisia laitteiden sisältämien henkilö- ja potilastietojen takia. Erityisesti puettavat laitteet ja mobiililaitteet ovat kasvattaneet laitevarkauksien määrää. Esimerkiksi Isossa-Britanniassa varastettiin yhden vuoden aikana vuosina 2010 ja 2011 yli 220 000 punnan edestä lääketieteellisiä laitteita North West London Hospitals NHS Trust -sairaalassa. (Enisa 2016) Työasemien varkauksia on tapahtunut terveydenhuollon organisaatioissa yhtä lailla kuin muidenkin toimialojen organisaatioissa. Työaseman varkaus terveydenhuollon toimijalta voi johtaa kuitenkin potilastietojen vuotamiseen. Erään työaseman varastaminen varastosta Iso-Britannian NHS North Central London -sairaalassa johti kahdeksan miljoonan potilaan potilastietojen päättymiseen väärin käsiin (Enisa 2016).

Lääketieteellisistä ja muista terveydenhuollon laitteista on kiinnostuttu vasta viimeisten vuosien aikana. Lääketieteellisten laitteiden teknisiä ominaisuuksia ja yhteyksiä on kehitetty niin, että laitteet sisältävät potilasdataa ja niihin voi päästä käsiksi muodostamalla

yhteyden laitteen kanssa. Siksi hakkerointien lisäksi laitteiden fyysinen varastaminen on tullut yhä kiinnostavammaksi kyberrikollisille. Esimerkiksi Yhdysvalloissa on raportoitu jopa ultraäänilaitteen varkaudesta, jonka mukana hävitettiin henkilötietoja ja kuvantamiseen liittyviä materiaaleja itse laitteen menettämisen lisäksi (Lehto & Lehto 2017). Laittevarkauksien jälkeen kyberrikolliset voivat tehdä kyberhyökkäyksiä entistä helpommin. Hyökkäysten lisäksi laitteita voidaan palauttaa takaisin terveydenhuolto-organisaatioon niihin tehtyjen käsittelyiden jälkeen, jossa laitteeseen on voitu lisätä esimerkiksi haittaohjelmatartunta tai tietoja voitu muokata. (Enisa 2016)

3.6 Lääketieteellisten laitteiden riskit, riskienhallinta ja uhkilta suojautuminen

Kaikkiin lääketieteellisiin laitteisiin liittyy jonkinlaisia ja tiettyjä kyberturvallisuusriskejä (Csulak et al. 2017). Tietoverkkoon liitettävillä fyysisillä lääketieteellisillä laitteilla on monenlaisia riskejä ja uhkia, jotka tulee ottaa huomioon osana terveydenhuollon organisaatioiden riskienhallintaa. Lääketieteellisten laitteiden riskienhallintaan ja uhkilta suojautumiseen vaikuttaa vahvasti terveydenhuollon toimiala, joka on kriittinen yhteiskunnalle (Tapx Labs 2015). Riskien olemassaolon takia kyberturvallisuuden kehittämiseksi tunnistetut riskit tulee huomioida laitteiden suunnittelussa mahdollisimman turvallisen käytön mahdollistamiseksi. Riskit ja uhat lisääntyvät tietoverkkoon liitettävien laitteiden yhdistyessä ja käyttäessä terveydenhuollon organisaatioiden tietoverkkoihin ja muihin laitteisiin. Liitettävyyden on tärkeää potilashoidon parantamisen kannalta, mutta luo tarpeen jatkuvaan riskien hallinnoimiseen. Kyberturvallisuusuhkia ja -riskejä ei pysty eliminomaan kokonaan, jolloin käyttäjäorganisaatioiden tehtävänä on huolehtia ja suojella potilasturvallisuutta. (Csulak et al. 2017)

Taulukkoon 3 on kerätty mukaillen Deloitte Center for Health Solutions (2013), Piggini (2017) ja Csulak et al. (2017) tietoverkkoon liitettävien lääketieteellisten laitteiden merkittävimpiä kyberturvallisuusriskejä. Riskit koostuvat pääasiassa laitteiden toiminnallisuuteen ja käyttämiseen liittyvistä riskeistä sekä laitteiden tietoverkkoon liitettävyyteen, ihmisten käyttäytymiseen ja kyberrikollisuuteen sekä väärinkäyttämiseen. Taulukosta nähdään riskejä muodostuvan muun muassa sähkömagneettisesta häirinnästä, testamattomista tai viallisista ohjelmista ja laiteohjelmistoista, fyysisestä turvallisuudesta ja yksityisyyteen liittyvistä riskeistä, luvattomista käytöistä sekä kyberhyökkäyksistä. Turvallisuuteen ja yksityisyyden haavoittuvuuksiin liittyy monia riskejä esimerkiksi huonoista salasanaikäytännöistä ja turvallisuuskäytännöistä, varkauksista, manipulaatiosta, potilastietojen hävittämisestä ja laitepäivitysten laiminlyönnöistä. (Deloitte Center for Health Solutions 2013)

Lääketieteellisten laitteiden merkittävimpiä kyberturvallisuusriskejä terveydenhuollon digitaalisessa toimintaympäristössä	
Riskit ja uhat	Esimerkki riskien ja uhkien realisoitumisesta
Sähkömagneettinen häirintä	Sähkömagneettisen säteilyn aiheuttama häiriötoiminta
Laitteiden menettäminen	Laitevarkaudet ja -häviämiset
Viestintä	Verkko- ja laiteviestinnän häiriöt Avoimet ja käyttämättömät viestintäportit laitteessa, jotka mahdollistavat luvattomat laiteohjelmiston etälätauokset
Yksityisyys	Yksityisten tietojen menettäminen Potilastietojen suodattaminen verkosta Potilastietojen virheellinen hävittäminen
Tietokantainjektiot	Tietoihin ja järjestelmiin pääseminen sekä tietojen varastaminen
Toistaminen	Tietojen toistaminen järjestelmiin pääsemiseksi ja tietojen varastamiseksi
Väärentäminen ja jäljittely	Laitteiston tai ohjelmiston kommunikaatio tulee muualta kuin alkuperäisestä lähteestä
Sosiaalinen manipulointi	Tiedon saaminen henkilöä harhauttamalla ja tiedon käyttäminen laitteisiin, verkkoihin tai tietokoneisiin hyökätessä
Tietojenkalastelu	Sosiaalista manipulointia, jossa käytetään esim. huijaus-sähköpostia tai väärennettyä verkkosivustoa tietojen saamiseksi Tietojen kerääminen ja verkossa liikkuvan tiedon sieppaaminen työkalujen avulla
Väärennetyt koodit	Väärennetyillä koodeilla voidaan kerätä ja tuhota tietoja, päästä järjestelmiin, väärentää järjestelmien tietoja ja raportteja tai aiheuttaa haittaa käyttäjille ja ylläpitäjille

Palvelunestohyökkäykset	Verkkojen ja tietojenkäsittelyresurssien saatavuuden heikentäminen vaikuttaen käyttöjärjestelmiin, kiintolevyihin ja sovelluksiin sekä laitteiden tekeminen käyttökelvottomiksi
Kyberhyökkäykset	Langattomia teknologioita hyödyntävät kyberhyökkäykset, joiden tarkoituksena on saada pääsy potilastietoihin, sekä niiden valvontajärjestelmiin ja istutettuihin lääkinällisiin laitteisiin Tartunnat haittaohjelmilla
Käyttöoikeudet	Käyttöoikeuksien eskalointia käytetään hyökkäyksen tehokkuuden lisäämiseksi, jotta voidaan saavuttaa pääsy etuoikeutettujen toimien toteuttamisiin Salasanojen hallitsematon jakelu ja hallinnointi
Tietoverkot	Luvaton pääsy terveydenhuollon tietoverkkoihin, joka mahdollistaa pääsyn muihin laitteisiin Väärin määritetyt tietoverkot tai huonot verkon suojauskäytännöt
Fyysinen tuhoaminen	Hyökkäykset, joiden tarkoituksena on tuhota tai heikentää fyysisesti laitteita tai niiden osia.
Laiteohjelmistot ja -ohjelmat	Testaamattomat ja vialliset laiteohjelmistot tai ohjelmat Asetusten uudelleenohjelmointi Tietoturvaohjelmien päivityksiä ja korjauksia ei ole tehty tai toimitettu ajoissa Tietoturva-aukot ohjelmistoissa puutteellisen suunnittelun ja vajavaisten suojausominaisuuksien vuoksi
Laiteturvallisuus	Laitteiden käyttäjä- ja potilasturvallisuutta vaarantava laitteen käyttäminen Asetusten luvaton muuttaminen

Taulukko 3. Kyberturvallisuuden merkittävimmät riskit lääketieteellisille laitteille mu-
kailien Deloitte Center for Health Solutions (2013), Piggin (2017) ja Csulak et al. (2017).

Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden toimintojen monimuotoisuuden vuoksi mahdolliset ja potentiaaliset riskit ovat moninaisia – kuten myös toimintahäiriöt ja niiden seuraukset. Nämä laitteet ovat alttiita manipuloinnille ja luvattomiin pääsyihin ja siksi tiedon suojaaminen tulee olla vahvasti toteutettua tietosuojan takaamiseksi. (eHealth Suisse 2020, s.40) Lääkinnällisten laitteiden turvallisuusriskeinä voidaan nähdä kaksi isoa riskiä – laitteisiin liittyvän datan ja laitteen itsessään joutuminen ulkopuolisen käsiin. Nämä riskit luovat tarpeen tarkastella lääketieteellisiä laitteita potilas- ja tietoturvallisuuden näkökulmasta, sekä tehdä yhteistyötä näiden riskien vähentämiseksi eri sidosryhmien kanssa. (Pöyhönen et al. 2019).

Lääketieteellisten laitteiden yhtenä haasteena tietoturvallisuudelle on, että ne ovat useilla terveydenhuollon toimijoilla jatkuvassa käytössä ympäri vuorokauden. Laitteiden suuren käyttöasteen vuoksi laitteisiin voi kohdistua turvallisuuteen liittyviä haasteita, mikäli laitetta ei pystytä huoltamaan tai päivittämään vikojen tai päivitystarpeiden esiintyessä. Vika- ja huoltotilojen käsitteleminen sekä ratkaiseminen saattavat viivästyä pitkiäkin aikoja suuren käytön ja laitteiden tarpeen vuoksi. Viivästyksiin vaikuttavat myös valmistajien kyvykkyydet ja resurssit korjata häiriöitä, sillä terveydenhuollon toimijat eivät useimmiten saa itsenäisesti korjata laitteita. (Tapx Labs 2015) Pitkät korjausajat voivat johtaa laitteiden potilashoidon viivästyksiin. Toisaalta pitkien korjausaikojen pelossa vioittuneiden laitteiden käyttö voi johtaa potilastietojen vaarantumisiin sekä saastuneiden tai virheellisesti toimivien ja haavoittuneiden laitteiden käyttöön.

ISO 14971 käsittelee lääkitieteellisten laitteiden riskienhallintaa laitteiden kehitys-, valmistus- ja käyttövaiheessa. Lääketieteellisten laitteiden valmistajilla on velvollisuus todistaa, että laitteisiin liittyvät potilasriskit ovat otettu huomioon ja ovat hallittavissa. Riskien tulee olla mahdollisimman vähäisiä ja riskit tulee määritellä, jotta ne voidaan ottaa huomioon terveydenhuollon toiminnassa. (ISO 14971:2019) Kyberturvallisuusriski tulee huomioida lääkitieteellisen laitteen riskienhallintaprosessissa, mikäli se vaikuttaa laitteen turvallisuuteen, suorituskykyyn, negatiivisesti kliiniseen leikkaukseen tai tuloksiin virheellisesti. Laittevalmistajilla on velvollisuus sisällyttää riskienhallinnan prosessiin kyberturvallisuksien haavoittuvuuksien tunnistaminen ja niihin liittyvien riskien arvioiminen, riskien hallitseminen hyväksyttävällä tasolla ja riskienhallinnan tehokkuuden valvominen. (AAMI TIR57:2016). Pääasiallisesti vastuu laitteiden käyttämisestä on kuitenkin lääketieteellisten laitteiden kuluttajilla eli terveydenhuollon organisaatioilla, jolloin toimijoiden tulisi varmistaa laitteiden käyttöturvallisuus ja huolehtia laitteiden käytön aikaisista riskeistä. Laittevalmistajien tekemien riskien tunnistamisen lisäksi olisi merkityksellistä, että tervey-

denhuollon toimijat ja muut terveydenhuoltoalan sidosryhmät tekisivät yhteistyötä jakamalla tietoa ja parhaita käytäntöjä haavoittuvuuksiin ja uhkiin liittyvissä toimenpiteissä ja niiden suunnitteluissa. (IMDRF 2019)

Laitteiden riskienhallinnan suunnittelu ja sen toteuttaminen tulisi tapahtua mahdollisimman varhaisessa vaiheessa, kuten ohjelmiston suunnitteluvaiheessa, jotta laitteiden turvallisuus osattaisiin ottaa suoraviivaisimmin ja kestävimmin mukaan osaksi terveydenhuollon toimijan kokonaisvaltaiseen riskienhallintaan. Suunnitteluvaiheessa tulisi miettiä vahvasti riskienhallintaa liitettävyyden kannalta muiden laitteiden ja verkkojen kanssa, pääsyn suojausten ja käyttöoikeuksien, kirjautumisten, verkkoviestinnän ja palvelinsuojausten, varmuuskopioinnin suojausten, tietojen salauksen, tietojen arkistoinnin ja poistamisen, tietojen eheyden ja ohjelmistopäivitysten näkökulmasta. (eHealth Suisse 2020)

Koska terveydenhuollon toimijat eivät voi vaikuttaa laitteen käyttövaiheessa ohjelmistoihin, päivityksiin tai suojauksiin, on erityisen tärkeää huomioida nämä asiat jo ennen laitteen hankintaa organisaatioon. Laitteen hankinnan jälkeen laite tulee ottaa osaksi terveydenhuollon toimijan omaa riskienhallintaa ja osaksi prosesseja ja suunnitelmia riskien ja uhkien realisoitumisen varalta. Terveydenhuollon toimijoiden on kannatettavaa ottaa käyttöön riskienhallintaprosessi turvallisuuden, tehokkuuden ja kyberturvallisuuden huomioimiseksi verkkoon kytkettävissä lääkinnällisissä laitteissa. Kyberturvallisuusuhkat ja -haavoittuvuuksia ja niihin liittyviä riskejä tulee arvioida ja huomioida laitteen kaikkien käyttövaiheiden ajan aina suunnittelusta tuen päättymiseen saakka. Tehokkaan ja toimivan riskienhallinnan kehittämiseksi kyberturvallisuusriskejä tulisi ottaa huomioon lääkinnällisen laitteen koko elinkaaren ajalta. Tällöin kyberturvallisuusriskejä voitaisiin arvioida ja mahdollisesti vähentää suunnittelusta alkaen ja jatkaen valmistukseen, testaukseen sekä markkinoille saattamisen jälkeiseen aikaan. (IMDRF 2019)

Osana riskienhallintaprosessia terveydenhuollon toimijoiden tulisi huolehtia ja soveltaa kyberturvallisuuden parhaita käytäntöjä osana organisaation kokonaisvaltaista turvallisuutta ja sen suunnitelmaa (IMDRF 2019). Riskienhallinnan prosessissa fyysiset tietoverkkoon kytkettävät lääketieteelliset laitteet tulee ottaa huomioon yhtäläisesti muiden tietoteknisten laitteiden tavoin. Laitteisiin liittyviin hyviin kyberturvallisuuskäytäntöihin kuuluu esimerkiksi riittävän hyvätasoinen fyysinen suojaus, käyttövaltuus- ja kulunvalvontatoimenpiteet, verkkoliikenteen pääsynvalvonta, haavoittuvuuksien ja korjauspäivitysten hallinta, haittaohjelmasuojauksen ja istuntojen aikakatkaisut luvattomien pääsyjen estämiseksi (IMDRF 2019). Fyysisten tietoverkkoon liitettävien lääkinnällisten laitteiden hyviä käytäntöjä voidaan tarkastella eri riskienhallinnan osa-alueiden näkökulmasta kuten esimerkiksi kyberturvallisuuden tilannekuvien, prosessien ja politiikkojen, valmistajien, yhteyksien, tietoturvaohjelmien, ihmisten toiminnan ja fyysisen turvallisuuden.

3.6.1 Kyberturvallisuuden tilannekuvat, prosessit ja politiikat

Terveystieteiden ja lääketieteellisten laitteiden kyberturvallisuuden uhkien- ja riskienhallinnassa merkityksellistä on muodostaa kattava kokonais- ja tilannekuva kyberturvallisuudesta organisaatiossa (Norri-Sederholm et al. 2019). Tilannekuvan luominen tapahtuu IT-resurssien ja kybertoimintaympäristön valvomisesta ja se on osana kyberriskienhallintaprosessia (Lehto 2019 s. 109). Epätarkka kybertilannekuva voi johtaa muun muassa syntaktisen kerroksen haavoittuvuuksiin (Lehto 2017). Hyvää tilannekuvaa on tärkeää ylläpitää kybersuojauksen toteuttamiseksi. Systeemitason tilannekuvan myötä kehittyvä havaintokyky ja tilannetietoisuus muodostuvat eri päätöstentekojen tasoilla tapahtuvista yhteisvaikutuksista (Pöyhönen et al. 2019).

Tilannetietoisuus koostuu havaitsemisesta, tiedon jakamisesta, tilannekuvasta ja analyysistä, jotka auttavat luotettavan tilannekuvan muodostamisessa. Tilannekuvan ylläpitäminen on organisaatioille erityisen tärkeää myös siksi, että tilannekuvalla voidaan viestiä johtamisprosesseihin oikeanlaista ja ajantasaista tietoa. (Lehto 2019). Tilannekuvaa ja sen luomaa havaintokykyä ja tilannetietoisuutta tulee käsitellä laajana kokonaisuutena, johon voidaan vaikuttaa esimerkiksi organisaatioiden välisen yhteistyön kautta. Systeemitasolla tilannetietoisuutta voidaan kehittää SOC:n (Security Operations Center) avulla eri tasoilta saatavan tilannekuvaan perustuen. Operatiivisesta näkökulmasta tilannetietoisuuden ylläpitämistä voidaan nähdä toiminnan jatkuvuuden varmistamisena. Taktisesta ja teknillisestä näkökulmasta katsottuna tilannetietoisuutta voidaan edistää hyödyntämissuunnitelmilla ja henkilöstön koulutuksella kyberturvallisuusriskien aiheuttamien tapahtumien vastaamiseksi. (Pöyhönen et al. 2019)

Prosessien riittämättömyydet voivat johtaa inhimillisiin virheisiin lääketieteellisten laitteiden käytössä. Käyttäjien inhimillisten virheiden ehkäisemiseksi olisi tärkeää luoda käyttöön liittyviä ohjeita ja prosesseja, jotka olisivat hyvin dokumentoituja ja päivitettyjä. (IMDRF 2019) Lääketieteellisten laitteiden näkökulmasta prosesseja ja politiikkoja tulisi päivittää ja luoda kattamaan ja käsittämään lääketieteelliset laitteet erillisenä laiteryhmänä. Terveystieteiden organisaatioille on tyypillistä olla tekemättä eroa lääketieteellisten ja ei-lääketieteellisten laitteiden välillä, joka tuo haasteen esimerkiksi lääketieteellisten laitteiden riskiarviointien menetelmiin. (The Deloitte Center for Health Solutions 2013) Kyberturvallisuuden tilannekuvan luomiseen ja jakamiseen sekä prosesseihin ja politiikkoihin liittyy vahvasti myös tiedon jakaminen, joka on tärkeää ja merkityksellistä kyberturvallisuusuhkien, -haavoittuvuuksien ja riskienhallinnassa. (IMDRF 2019)

Tiedon jakaminen voidaan nähdä työkaluna, jonka avulla terveydenhuollon toimialalla parhaita käytäntöjä ja esimerkkitaapauksia voidaan jakaa ja niistä oppia ja kehittää toimintatavoista kyberturvallisempia. Rakitinin (2009) mukaan terveydenhuollon organisaatioiden tulisi jakaa kokonaisvaltaisesti tietoa ja tilannekuvaa sidosryhmille. Tietoverkkoon liitettäviin fyysisiin lääketieteellisiin laitteisiin liittyviä eri sidosryhmiä tulee kannustaa ottamaan parhaita käytäntöjä käyttöön eri toimialoilta ja sektoreilta, joilla tunnustettu hyväksi havaittuja työkaluja ja -toimia lääketieteellisten laitteiden ekosysteemin turvallisuuden vahvistamiseksi (IMDRF 2019). Kaikilla sidosryhmillä on oma vastuu ja rooli tietojen jakamisessa. Laittevalmistajien vastuuna voidaan nähdä tietojen jakaminen suunnittelun validoinnista ja riskeistä, poikkeavuuksien havainnoista sekä niiden vaikutuksesta turvallisuuteen. IT:n ja palveluntarjoajien tulee puolestaan huolehtia omasta näkökulmastaan tietojen jakamisesta lääketieteellisiin laitteisiin liittyen. Sääntelyviranomaisten rooliin kuuluu jakaa ohjeita riskien vähentämiseksi ja turvallisuuden valvomiseksi. (Rakitin 2009) Tietoa voidaan jakaa erilaisin tavoin ja menetelmin sidosryhmille, mutta tärkeintä on kehittää parhaita käytäntöjä jatkuvasti kyberturvallisuuden kehittyessä lääketieteellisten laitteiden osalta eri valmistajien, laitetyyppien, yhdistetyn infrastruktuurin, organisaation koon, kypsyyssasteen ja uhkatason myötä. (IMDRF 2019)

3.6.2 Laittevalmistajien ja muiden sidosryhmien välinen yhteistyö

Lääketieteellisten laitteiden turvallisuuden ja tehokkuuden parantamiseksi tulisi terveydenhuoltoalan sidosryhmien luoda yhteistä kieltä ja yhteistyömuotoja sekä jakaa tietoa laajasti ja systemaattisesti (Rakitin 2009). Terveydenhuollon kyberturvallisuusuhkien vähentämiseksi ja niiltä suojautumiseksi on suositeltavaa toimia yhteistyössä kaikkien laitteisiin liittyvien sidosryhmien kanssa (Pöyhönen et al. 2019). Deloitte Centre for Health Solutions (2018) mukaan yhteistyö toimittajien, valmistajien ja käyttäjien kanssa on välttämätöntä lääketieteellisten laitteiden ja IoT:n (Internet of Things) kehittämiseksi. Yhteistyön edistämiseksi ja laitteiden kehityksen kannalta kaikkien laitteisiin liittyvien osapuolien kanssa tulisi tunnustaa ja arvioida erilaisia kyberuhkia sekä hallinnoida niihin liittyviä riskejä (Pöyhönen et al. 2019). Tiiviiseen sidosryhmäyhteistyöhön olisi kannattavaa osallistuttaa sääntelyviranomaisia, laittevalmistajia, terveydenhuollon organisaatioita, IT-toimittajia ja potilaita (Grimes 2016, s.18) Laaja sidosryhmien hyödyntäminen yhteistyössä edistää lääketieteellisten laitteiden kehittämistä ja laitteiden käyttöönottoa vakiintuneisiin hoitopolkuihin. Tämä vaatii jatkuvaa ja merkittävää sidosryhmien yhteistyötä. (Deloitte Centre for Health Solutions 2018)

Yhteistyön avulla voidaan terveydenhuollon toimialalla luoda kattavia ja kokonaisvaltaisia suunnitelmia, prosesseja ja ohjeistuksia, jotka liittyvät yleisesti terveydenhuollon toimialaan sekä kohdistuen lääketieteellisiin laitteisiin. Sidosryhmien välisestä yhteistyöstä voidaan tuottaa toiminta- ja varautumissuunnitelmia, joita voidaan tuottaa yhdessä sidosryhmien kanssa. Nämä suunnitelmat takaavat myös liiketoiminnan jatkuvuutta ja terveydenhuollon toimivuutta ja niitä tarvitaan kyberturvallisuuden varmistamiseksi sekä riskeiltä suojautumiseen. (Pöyhönen et al. 2019)

Lääketieteellisten laitteiden uhkia ja riskejä voidaan hallita tilannekuvan luomisen lisäksi hyvillä ja kattavilla ohjekirjoilla laitevalmistajilta terveydenhuollon toimijaorganisaatioille. Valmistajan on tuotettava terveydenhuollon laitteiden toiminnanharjoittajalle ohjeet laitteen koko elinkaarelle ja toiminnanharjoittajan tulee noudattaa näitä ohjeita lakiin määriteltynä. Ohjeiden luonnilla ja niiden käyttämisellä pyritään edistämään lääkinnällisiin laitteisiin kohdistuvaa ylläpitoa ja käyttöä. (L 24.6.2010/629) Ohjekirjojen avulla voidaan laitteita käyttää oikealla tavalla ja laitevalmistajan määrittelevillä kyberturvallisuutta tukevilla tavoilla. Vaikka kattavat ohjekirjat ylläpitävät turvallista laitteiden käyttöä, voidaan ohjekirjoja käyttää myös kyberhaavoittuvuuksien löytämiseksi (Williams & Woodward 2017). Ohjekirjojen väärinkäyttöä on kuitenkin mahdollista ehkäistä vahvoilla, teknisillä ominaisuuksilla ja tietoverkkojen suojaamisella ja valvonnalla.

Valmistajien ohjekirjojen seuraaminen ja niiden mukaan toimimisen lisäksi olisi merkityksellistä tehdä jatkuvaa yhteistyötä laitevalmistajan kanssa. Laitevalmistajia kannustetaan olemaan yhteydessä ja tekemään yhteistyötä terveydenhuollon toimijoiden kanssa mahdollisuuksien mukaisesti, jotta laitteiden käyttöönotto ja konfigurointi onnistuisi mahdollisimman hyvin (IMDRF 2019). Organisaatioiden yhteisellä ja monitahoisella yhteistyöllä ja kehittämisellä lääketieteellisten laitteiden kyberturvallisuuden edistämiseksi on merkitystä, sillä yhteistyössä myös tiedonvaihto ja jakaminen eri toimijoiden välillä korostuu. Tiedon jakaminen on merkityksellistä, sillä verkkorikollisuudelta suojaudutaan monin eri keinoin ja monien eri tahojen avulla, jolloin on luonnollista tarvita sujuvaa tiedon ja osaamisen jakamista. (Pöyhönen et al. 2019) Laitevalmistajien taholta tulevan yhteistyön ja yhteydenpidon lisäksi terveydenhuollon toimijoiden kannattaisi kuitenkin toimia proaktiivisesti laitevalmistajien suuntaan sekä tulevien hankintojen, että käytössä olevien laitteiden osalta.

Parhaimmassa tapauksessa lääketieteellisten laitteiden kyberturvallisuuden kehittämisessä laitevalmistajat, terveydenhuollon organisaatiot ja muut sidosryhmät voivat kaikki hyötyä yhteistyöstä. Yhteistyön avulla voidaan luoda lääketieteellisiin laitteisiin liittyviä ratkaisuja, joilla on kliinistä, toiminnallista ja taloudellista arvoa (Deloitte Centre for Health

Solutions 2018). Terveysturvaolosssa ja palveluntarjoajilla yhteistyön haasteeksi ja rajoitukseksi saattaa joskus kuitenkin muodostua korkeat kustannukset, kun kyberturvallisuuden tietty korkeus on saavutettu erityisesti teknisin ratkaisuiden osilta. Teknisten ratkaisuiden ja suojausten jäljelle jääviä riskejä on siksi otettava osaksi päivitettäviä ja ylläpidettäviä, yhtenäisiä suunnitelmia, toimintatapoja, prosesseja ja järjestelmiä. (Pöyhönen et al. 2019)

3.6.3 Tekniset turvatoimenpiteet ja yhteydet

Merkittävänä osuutena kyberturvallisuuden kehittämistä ovat tekniset ratkaisut ja yhteydet tietoverkkoon liitettävien lääketieteellisten laitteiden osalta. Teknis-taktisella tasolla on tietoverkkoon liitettävät lääketieteelliset laitteet tunnistettava ja määritettävä kuinka ne ovat yhteydessä toisiin laitteisiin ja internettiin (Pöyhönen et al. 2019). Enisan (2016) mukaan merkittäviin turvatoimenpiteisiin kuuluvat muun muassa verkon segmentointi sisältäen älykkäät palomuurit, verkon valvonta ja tunkeutumisen havaitseminen, vankka salaus, kulunvalvonta, käytön autentikointi ja valtuutus. Teknisten kyberturvallisuusriskien hallitsemiseksi ja suojaamiseksi terveydenhuollon organisaatioiden tulisi tietää minkä teknologioiden kanssa tietoverkkoon liitettävät lääketieteelliset laitteet kommunikoivat. Lisäksi laitteisiin tulee määritellä käytettäväksi vain tekniikalla, jolla on tarvittavat tunnisteet. (Csulak et al. 2017) Langatonta verkkoa tulee valvoa jatkuvasti turvallisuusuhkien ehkäisemiseksi ja varustaa uusilla puolustustekniikoilla. Tärkeimpiä langattomiin verkkoihin vaikuttavia uhkia ja hyökkäyksiä ovat esimerkiksi tietojen kaappaaminen, muuttaminen tai vuotaminen. (Aram et al. 2017)

Yhteyksien suhteen Lehdon & Lehdon (2017) mukaan kyberturvallisuusriskien vähentämiseksi lääketieteellisten laitteiden tulisi välttää puutteellisia WLAN- ja salaamattomia yhteyksiä sekä helposti murrettavissa olevia WEP-salauksia. Lääkinnällisten laitteiden käytössä tulisi hyödyntää esimerkiksi WPA- ja WPA2-salauksia ja varmistaa etäyhteyksien olevan hyvin suojattuja muun muassa huolto- ja vikatilanneselvityksiä varten. (Lehto & Lehto 2017) Aram et al. (2017) mukaisesti tietoturvastandardeja tulisi noudattaa täsmällisesti langattomien yhteyksien osalta, sillä niiden käyttämättömyys voi johtaa langattomien teknologioiden toimintahäiriöihin ja haittaohjelmatartuntoihin. Vikaselvitysten yhteydessä on myös huomioitava potilasturvallisuuden toteutuminen ja salassa pidettävien tietojen käsittelyn suhteen. Turvallisten ja suojattujen yhteyksien luonnin lisäksi lääketieteellisten laitteiden tulisi jakaa eri verkko-osioihin muista talotekniikan laitteista ja työasemista kyberturvallisuuden ylläpitämiseksi. Tällöin myös lääketieteelliset laitteet, joita ei

pystytä suojaamaan virustentorjuntaohjelmilla, saadaan paremmin suojattua kyberhyökkäyksiltä. (Norri-Sederholm et al. 2019)

Käytön autentikointi ja valtuutus ovat tärkeitä turvatoimenpiteitä, joilla voidaan suojata ja valvoa laitteiden käyttöä. Lääkinnällisissä laitteissa tulisi lähtökohtaisesti suosia laitteita, jotka tukevat monivaiheista ja kattavaa autentikointia. (Lehto & Lehto 2017) Puutteellinen käyttäjän tunnistaminen ja tunnistautuminen on kyberturvallisuusriski, sillä se luo kyberrikollisille mahdollisuuden tunkeutua laitteeseen helpommin (Kyberturvallisuuskeskus 2016). Mikäli lääketieteellisissä laitteissa ei pystytä noudattamaan ohjeistuksia esimerkiksi kaksivaiheisesta tunnistautumisesta ja henkilökohtaisten tunnusten käyttämisestä, on tällaisten laitteiden varalta syytä luoda omat ohjeistukset. Henkilökunnan osaamista voidaan kehittää säännöllisillä koulutuksilla ja kursseilla sekä luomalla erillisiä ohjeistuksia viestittäväksi erityisesti sellaisiin työtilanteisiin tai kohderyhmälle, jossa epätoivottua käytöstä on huomattu eniten olevan. Henkilökunnan käyttäjätunnusten ja -oikeuksien lisäksi toinen puoli lääketieteellisten laitteiden käyttövaltuuksien kyberturvallisuutta on laitteiden käyttäjäorganisaatioiden todennus ja valtuutus käyttää laitteita hoitotyössä.

3.6.4 Tietoturva- ja virustentorjuntaohjelmat sekä laitepäivitykset

Terveystieteiden laitteiden suojauksesta on huolehdittava laitekohtaisesti virustorjunta- ja tietoturvaohjelmilla. Virustorjunta- ja tietoturvaohjelmien olemassaolon lisäksi kyberturvallisuuden ylläpitämiseksi laitteiden päivityksiä on tehtävä haavoittuvuuksien korjaamiseksi ja muiden teknisten ominaisuuksien parantamiseksi. Virustorjuntaohjelmien asentaminen lääketieteellisiin laitteisiin voi kuitenkin olla haastavaa, sillä osassa laitteissa voidaan käyttää vain valmistajien määrittämiä ohjelmia (Lehto & Lehto 2017). Tapx Labsin (2015) raportin mukaisesti haittaohjelmahyökkäyskorjausten jälkeen monissa lääketieteellisissä laitteissa havaittiin nopeasti uudelleen haittaohjelmatartunta, sillä laitteen haavoittuvuutta ei ollut korjattu. Joissakin laitteissa puolestaan tietoturva- ja virustentorjuntaohjelmia ei voida käyttää ollenkaan (Williams & Woodward 2015).

Laitevalmistajien omien haasteiden lisäksi tietoverkkoon liitettyjen lääketieteellisten laitteiden kyberturvallisuus voi heikentyä testaamattoman tai viallisen laiteohjelmiston tai ohjelman vuoksi. Testaamattomuuden tai viallisuuden rinnalla tapahtuu myös laitevalmistajien ohjeiden noudattamattomuutta. Laitteiden riskienhallinnassa korostuu laitevalmistajien tietoturvapäivitysten ja korjaustiedostojen ajankohtainen päivittäminen ja ohjeiden noudattaminen. Laitepäivitysten tekeminen ajankohtaisina niiden tullessa laiteval-

mistajilta voivat myös ehkäistä mahdollisten toimintahäiriöiden riskiä johtuen haavoittuvuuksien tai vanhojen ohjelmien väärinkäytöstä. (The Deloitte Center for Health Solutions 2013) Laitteissa käytössä olevia valvontaohjelmia tulisi pystyä päivittämään, vaikka laitteet olisivatkin vain lyhytaikaisesti verkossa. Lääketieteellisten laitteiden virustorjuntaohjelmien lisäksi työasemien suojaaminen viruksilta on isossa osassa lääketieteellisten laitteiden kyberturvallisuutta – virustorjuntaohjelmien tulisi olla pakollisia muiden tarvittavien tietoturvaohjelmien kanssa kaikkiin työasemiin ja laitteisiin, joihin niitä voidaan asentaa turvallisesti (Vartiainen 2017).

Yhtenä merkittävämpänä kyberturvallisuuteen vaikuttavista riskeistä lääketieteellisissä laitteissa ja järjestelmissä ovat laitepäivitykset ja erityisesti niiden puutteelliset testaukset. Laitepäivitysten puutetta voi hyödyntää ulkopuoliset ja sisäpiiriläiset toimijat, jotka voivat aiheuttaa passiivista tai aktiivista uhkaa terveydenhuollon organisaatioille. Taulukossa 3 on listattuna (The Deloitte Center for Health Solutions (2013), Piggini (2017) ja Csulak et al. (2017) mukaisesti uhista, joita lääketieteellisissä laitteissa voi realisoitua digitaalisessa toimintaympäristössä esimerkiksi puutteellisten laitepäivitysten vuoksi. Taulukon monimuotoisista uhkista voidaan nähdä, että laitepäivitysten puutteet voivat mahdollistaa monenlaisia riskejä, jotka liittyvät muihin hallittaviin riskeihin kuten ihmisten käyttäytymiseen, fyysiseen turvallisuuteen ja pääsynhallintaan.

3.6.5 Ihmisten käyttäytyminen ja koulutus

Hyvien ja suojattujen yhteyksien sekä teknisten ominaisuuksien lisäksi lääkinnällisten laitteiden kyberturvallisuudessa on huomioitava laitteiden käyttäjien käyttäytyminen ja toimintatavat. Tietoverkkoon liitettävien fyysisten laitteiden loppukäyttäjiä ovat esimerkiksi potilaat, lääkärit, sairaanhoitajat, omaishoitajat ja kuluttajat (IMDRF 2019). Riskienhallinnan näkökulmasta tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden käytöstä ja toiminnasta tulisi tarjota koulusta ja harjoituksia kaikille laitteita käyttäville ta hoille ja henkilöille. Ihmisten kouluttaminen on tärkeää ja merkityksellinen osa lääketieteellisten laitteiden kyberturvallisuutta, sillä ihminen voidaan nähdä kyberturvallisuudessa isona tekijänä turvalliselle toiminnalle (Norri-Sederholm et al. 2019, s.89). Lääketieteellisten laitteiden osalta laitteiden käyttäjät, eli muun muassa terveydenhuollon ammattilaiset ja potilaat, ovat usein itse niitä, jotka tekevät päätöksiä laitteiden korjaustarpeista ja raportoivat mahdollisista vioista ja epätavallisista tapahtumista (IMDRF 2019). Tämän vuoksi koulutusta tarvitaan yleisesti kyberturvallisuudesta, mutta myös kohdistettuna tietoverkkoon liitettäviin fyysisiin laitteisiin ja niiden käyttöön eri sidosryhmille erilaisina koulutustyyppinä.

Lääketieteellisten laitteiden käyttäjiin liittyvässä riskienhallinnassa on otettava huomioon muun muassa laitteiden käyttö, yleinen kyberturvallisuustietoisuus kyberhyökkäyksistä ja hyvistä käytännöistä sekä käyttäjätunnukset ja salasana. Terveystieteiden organisaatioissa ihmisiin liittyviin riskeihin kuuluvat esimerkiksi salasanoiden ja käyttäjätunnusten jakaminen, salasanoiden näkyvillä oleminen, salasanoiden ja kirjautumisten pois ottaminen käytöstä tai laitevalmistajan oletussalasanoiden käyttö. (The Deloitte Center for Health Solutions 2013) Näitä riskejä voidaan hallita parhaiten kouluttamalla ihmisiä suoraan organisaation salasa- ja käyttäjätunnuskäytännöistä ja huolehtia, että tietoverkkoon liitettävät lääketieteelliset laitteet noudattavat organisaation yleisiä ohjeistuksia.

Ihmisten kyberturvallista käyttäytymistä tukemalla ja käyttäjien koulutuksella lääketieteellisistä laitteista voidaan vaikuttaa kokonaisvaltaiseen kyberturvallisuuteen terveydenhuollon toimijaorganisaatioissa. Terveystieteiden toimijoiden tulisi tarjota kyberturvallisuudesta peruskoulutusta kyberturvallisuustietoisuuden lisäämiseksi. (IMDRF 2019) Esimerkiksi yleistä kyberturvallisuutta voidaan lisätä erilaisten aktiviteettien ja viestinnän avulla laajalle kohderyhmälle. Kyberturvallisuuden kautta kyberturvan kehittämisen tavoitteena on kehittää kohderyhmän yksilöiden kykyä tunnistaa epätavalliset kyberturvallisuuteen liittyviä tapahtumia ja ilmoittaa niistä eteenpäin. (Enisa 2016) Lisäksi olisi merkityksellistä esitellä kyberturvallisuuteen liittyviä perustietoja ja parhaita käytäntöjä laajasti eri terveydenhuollon toimijan työntekijöille kuten esimerkiksi lääkäreille, sairaanhoitajille, biolääketieteen insinööreille ja tekniikoille. Työntekijöiden koulutuksen lisäksi myös potilaita tulisi kouluttaa ja perehdyttää erityisesti verkkoon liitettävien lääketieteellisten laitteiden käytön kyberturvallisuudesta, sillä potilaat toimivat lääketieteellisten laitteiden käyttäjinä kotikäyttöön tarkoitetuissa laitteissa tai jatkuvasti käytössä olevien laitteiden, kuten insuliinipumpun ja glukosimittarin kanssa. (IMDRF 2019) Suoraan laitteisiin liittyvien koulutusten lisäksi laitteiden käyttäjien tulisi ymmärtää toimijan keskusjärjestelmistä ja niiden vuorovaikutuksista muihin järjestelmiin ja komponentteihin (Enisa 2016).

Kyberturvallisuuskoulutuksen fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden osalta tulisi sisältää tietoa ainakin turvallisesta laitteen käytöstä, suojatuista tietoverkoista ja poikkeavista tapahtumista ja häiriöistä sekä niiden ilmoittamisesta terveydenhuollon organisaatioon tai hoitavalle taholle. (IMDRF 2019) Turvallinen käyttö ja suojattujen tietoverkkoyhteyksien käyttäminen ennaltaehkäisevät mahdollisia kyberhyökkäyksiä ja -tapahtumia, kun taas poikkeaman tai epätavallisen tapahtuman tunnistaminen ja siitä ilmoittaminen oikealle taholle kouluttaminen tukee nopeata toimintaa mahdollisen hyökkäyksen torjumisessa. Koulutuksella voidaan myös vaikuttaa henkilöstön ajatus-

maailmaan liittyen laitteiden turvatoimiin ja käytäntöihin, jotka voivat vaikuttaa työn tehokkuuteen hidastavasti ja hankaloittavasti. Kouluttamalla turvatoimien tärkeydestä ja tarpeellisuudesta, käyttäjien näkemyksiin turvatoimista voidaan vaikuttaa positiivisesti ja vähentää kyberturvallisuudesta joustamista ajallisesti paineistetussa työympäristössä. (Enisa 2016)

Ihmisten kyberturvallisuuskoulutuksella voidaan vaikuttaa verkossa tapahtuvien kyberturvallisuusriskien ja -tapahtumien tunnistamiseen, mutta myös terveydenhuollon työntekijöiden koulutuksella ja kyberturvallisuustietoisuuden lisäämisellä on mahdollista vähentää myös tietoverkkoon liitettävien fyysisten lääketieteellisten laitevarkauksien määrää. Toisaalta taas juuri työntekijöiden vuoksi laitevarkauksia on lähes mahdotonta välttää, sillä heillä on organisaation sisäistä tietoa esimerkiksi käyttäjäoikeuksista, järjestelmistä ja turvatoimenpiteistä. (Enisa 2016).

3.6.6 Fyysinen turvallisuus ja laitteiden suojaaminen

Hyvällä fyysisellä suojauksella voidaan estää luvattomat pääsyt lääketieteelliseen laitteeseen tai verkkotukipisteeseen (IMDRF 2019). Fyysisen turvallisuuden perusteena toimii hyvin suunniteltu ja toteutettu toimitilojen käyttö ja niiden suojaaminen. Toimitilaturvallisuuden näkökulmasta haasteen terveydenhuollon toimijoille tuottaa tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hajallaan olevat fyysiset sijainnit ympäri toimitilaa. Fyysistä turvallisuutta on vaikeaa toteuttaa käytännössä kaikille laitteille ja komponenteille, mutta siihen tulisi kiinnittää huomiota laitteiden väärinkäytösten ja laitevarkauksien takia. (Enisa 2016)

Lääketieteellisten laitteiden varkaudet ovat merkittävä riski yhdessä laitteiden häviämisten ja tuhoamisten kanssa (The Deloitte Center for Health Solutions 2013). Lääketieteellisten laitteiden varkaudet kohdistuvat erityisesti puettaviin laitteisiin ja mobiililaitteisiin, mutta myös tunnistuskomponentteja ja esimerkiksi kuvantamisen laitteita on varastettu. Varkaudet vaikuttavat verkotettujen lääketieteellisten laitteiden käyttöön ja siten potilashoittoon, tunnistuskomponentteihin, asiakaslaitteisiin ja potilastietoihin. Laitteiden fyysisen viemisen myötä tulevat taloudelliset ja potilashoidon viivästymisen vaikutukset, mutta johtavat usein myös arkaluonteisten potilas- ja terveystietojen menettämiseen. (Enisa 2016)

Vaikka lääketieteellisten laitteiden varkaudet ovat kasvussa, terveydenhuollon ammattilaisten työasemat ovat silti yleisin varkauden kohde. Työaseman varastaminen nykyisissä digitaalisesti kehittyneissä terveydenhuolto-organisaatioissa nähdään entistä vaa-

rallisempänä skenaariona, sillä mikäli kone on heikosti salattu, konetta voidaan hyödyntää käyttäen etäyhteyksiä. Varkauksia rajoittaa laitteiden suuri koko, jolloin laitevarkauksien todennäköisyyttä terveydenhuollon toimijoilta voidaan kuvata keskinertaisena. (Enisa 2016)

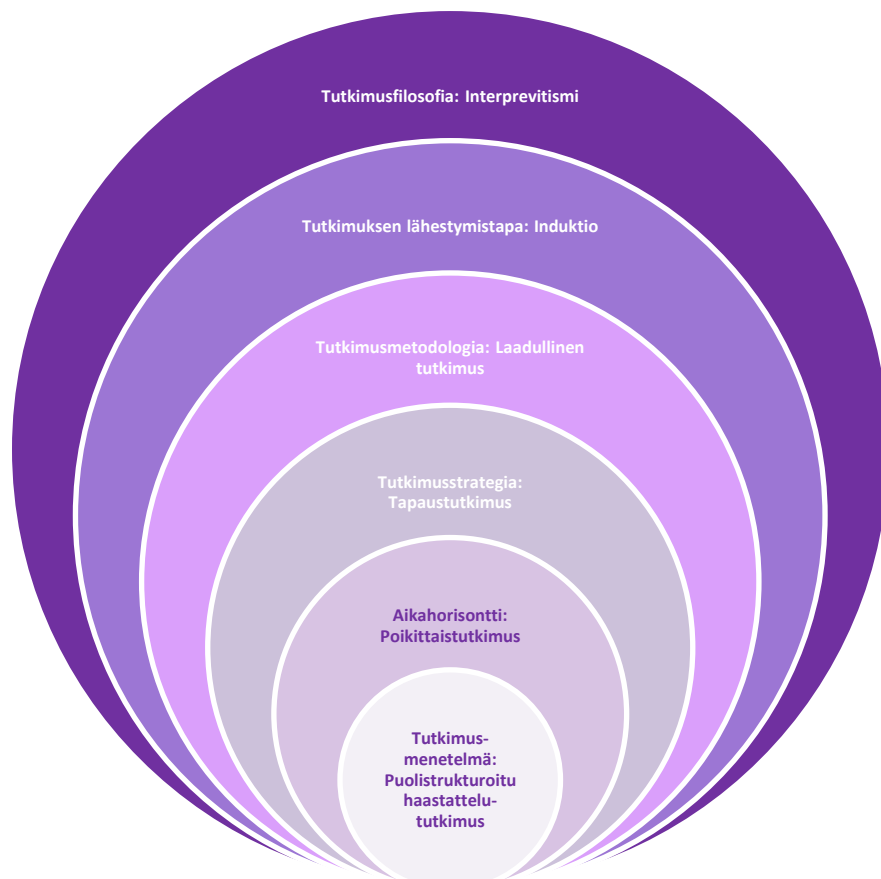
Lääketieteellisten laitteiden varkauksien yhteydessä olisi tärkeää suorittaa riskienhallintaan liittyviä toimenpiteitä ja tarkastella laitevarkauksia organisaatioprosessien, politiikkojen ja proseduurien, omaisuuden ja konfiguroinnin hallinnan, fyysisen turvallisuuden ja käyttäjien tietoisuuden kannalta. Laitevarkauksien vähentämiseksi IoT-ratkaisut voivat tulevaisuudessa auttaa ehkäisemään varkauksien tapahtumista ja havaitsemaan sekä tutkimaan laitevarkauksia tarkemmin. Laitteiden etähallinnan ratkaisuna voisi olla reaaliaikainen paikantamisjärjestelmä, jonka avulla voitaisiin seurata laitteita. Laitevarkauksien vähentämiseksi ja niiden välttämiseksi tulisi työasemat ja tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet olla vahvasti salattuja, käyttäjän tunnistusmenetelmät vahvoja ja lukittavissa etäältäkin. Fyysisen turvallisuuden suojaamiseen ja laitteiden varkauksien ehkäisemiseen voidaan vaikuttaa hyvällä fyysisellä kulunvalvonnalla toimiympäristössä sekä huolehtimalla hälytysjärjestelmien olemassaolosta. Laitteita voidaan myös lukita kaapeleilla niiden käsiksi pääsemisen ehkäisemiseksi. Näiden kaikkien toimenpiteiden ja ominaisuuksien lisäksi on tärkeää ottaa kaikki lääketieteellisten laitteiden kyberturvallisuusnäkökulmat osaksi politiikkoja, prosesseja ja käytännön toimenpiteitä. (Enisa 2016)

4. TUTKIMUSMENETELMÄ

Tässä luvussa käsitellään tutkimusmetodologiaa tutkimusasetelman ja tutkimuksen vaiheiden toteutusten lähtökohdista. Tutkimuksen viitekehystenä käytetään Saundersin et al. (2019) esittelemää sipulimallia (eng. research onion), jonka avulla kuvataan tutkimusprosessin vaiheet sisältäen tutkimusaihetta taustoittavan kirjallisuuskatsauksen sekä puolistrukturoidun haastattelututkimuksen tutkimuksen syventämiseksi. Tutkimusvaiheiden ja -menetelmän taustoitukseen tarkoituksena on kuvata läpinäkyvästi tutkimuksen kulkua sekä sitä, miten tulokset on saatu johdettua aineistosta.

4.1 Tutkimusasetelma

Tutkimusasetelma kuvaa tutkimuksen suunnitteluun käytettävää tieteellistä viitekehystä sekä tutkimuksen tekemistä ja tulkintaa ohjaavia valintoja. Tutkimusasetelma kattaa tutkimusmetodologian ja -menetelmät, joita käytetään tutkimuksessa. Saunders et al. (2019) sipulimallin avulla voidaan kuvata tutkimuksen lähtökohtia ja valintoja suunniteltaessa tutkimusta. Tässä tutkimuksessa käytetyt tutkimusmetodologiavalinnat esitetään sipulimallia hyödyntäen kuvassa 2.



Kuva 2. Saundersin et al. (2019) sipulimallia käyttäen esitetyt tutkimusmetodologiset valinnat.

4.1.1 Tutkimusfilosofia: Interpretivismi

Saundersin et al. (2019) sipulimallin ensimmäisenä kuorena sijaitsevalla tutkimusfilosofialla viitataan tutkimuksen taustalla vaikuttaviin uskomuksiin ja oletuksiin tietämyksen kehittymisestä sekä siitä, miten tietoa luodaan ja minkälainen nykyisen tiedon ja tutkimuksessa saatavan tiedon välinen suhde on (Saunders et al. 2019, s.130) Tutkimusfilosofian avulla määritellään, millaista tietoa tutkimuksesta voidaan etsiä ja minkälaisia oletuksia on mahdollista tehdä. Tutkimusfilosofioista tässä tutkimuksessa hyödynnetään interpretivismistä tutkimusfilosofiaa, joka on subjektiivinen filosofia ja jossa korostetaan ihmisten erilaisuutta fyysisistä ilmiöistä, sillä ne luovat merkityksiä. Interpretivismisissä tutkimuksissa pyritään luomaan yleensä uutta ja syvällisempää ymmärrystä organisaatioiden realiteeteista. Empiirisesti interpretivismi korostaa yksilöiden kokemuksia ja pyrkii sisällyttämään osallistujien tulkinnat osaksi tutkimusta. (Saunders et al. 2019, ss.159)

4.1.2 Lähestymistapa: Induktio

Saundersin et al. (2019) mukaisesti tutkimuksen lähestymistavat voidaan jakaa kolmeen päätapaan: deduktioon, induktioon ja abduktioon. Deduktiolla tarkoitetaan lähestymistapaa, jossa jo olemassa olevia ja kehitettyjä teorioita ja tutkimuksessa on tarkoitus testata hypoteeseja. Induktiossa puolestaan kerätään ensin tietoa ja tästä analysoidusta tiedosta muodostetaan teoria. Abduktiossa on kyse induktion ja deduktion yhdistelmästä, jossa tyypillisesti aineistoa kerätään eri ilmiöiden, teemojen ja mallien ymmärtämiseen ja tarkoituksena on lopulta luoda uusia teorioita tai muokata olemassa olevia. (Saunders et al. 2019)

Päälähestymistavoista tässä tutkimuksessa käytetään induktiota, jossa lähestytään tutkimusta ensin keräämällä tietoa ja aineistoa, sekä ilmiön ymmärtämisellä. Empiirisen tutkimustiedon keräämisen jälkeen induktiivisessa lähestymistavassa luodaan teoria perustuen tutkimusaineiston analysointiin (Saunders et al. 2019, s. 160). Induktiivista lähestymistapaa käytetään Saundersin et al. (2019) mukaan tyypillisesti tutkimuksissa, joiden tutkimusfilosofiana käytetään interpretivismiä. Tässä tutkimuksessa induktiivista lähestymistapaa käytetään empiiriseen tutkimukseen, jossa pyritään selvittämään kyber turvallisuuden nykytilasta lääketieteellisten laitteiden osalta terveydenhuollon organisaatioissa, ja näin saadaan ymmärrystä ja käsitys tutkittavana olevasta ilmiöstä, josta muodostuu empiirisen aineiston tutkimustulos.

4.1.3 Tutkimusmetodologia: Laadullinen tutkimus

Tutkimusmetodologian valitseminen on osana tutkimuksen suunnittelua. Tutkimusmetodologiat jaetaan kvantitatiivisiin ja kvalitatiivisiin tutkimuksiin, sekä niiden molempien tutkimuksien yhteismenetelmään. Kvantitatiivisessa tutkimuksessa kerätty tieto on numeerista ja laskennallista. Kvalitatiivisessa tutkimuksessa aineistoksi kerätään laadullista tietoa, jota voidaan saada esimerkiksi haastatteluista ja avoimien kysymysten kyselyissä. (Saunders et al. 2019, ss. 174-180)

Laadulliselle tutkimukselle tyypillisiä piirteitä ovat esimerkiksi tutkimuskohteiden toiminnan tai tilanteiden suhteiden, uskomusten ja olettamusten tutkiminen, tutkimuksen perustuminen sanalliseen tai kuvalliseen merkitysten kuvaamiseen, sekä kokoelmaan vastauksista, jotka eivät ole standardeja ja vaativat kategorisointia (Saunders et al. 2019, ss. 174-180). Tässä tutkimuksessa hyödynnetään laadullista tutkimusta ja tutkimussuunnitelmaa, jossa tarkoituksena on ymmärtää ja kuvailla tiettyä ilmiötä, tilannetta tai toimintaa sekä tunnistaa mahdollisesti niiden välillä olevia suhteita ja yhteyksiä. Tutkimuksessa pyritään saamaan vastauksia tutkimuskysymyksiin, jotka pyrkivät selvittämään kyberturvallisuuden nykytilaan liittyvää toimintaa. Näin ollen tutkimuskysymykset ohjaavat käyttämään laadullista tutkimusta, jossa voidaan saada vastauksia määrittämättömässä muodossa ja avoimilla kysymyksillä. Laadullisista tutkimussuunnitelmista käytetään laadullista monimenetelmää, sillä tutkimus koostuu kirjallisuuskatsauksesta sekä haastattelututkimuksesta, jotka molemmat ovat laadullisia tutkimusosia ja tyypillisiä aineistonkeruumenetelmiä laadulliselle tutkimukselle (Patton 2005).

4.1.4 Tutkimusstrategia: Tapaustutkimus

Tutkimusstrategialla tarkoitetaan tutkimuksen suunnitelmaa sille, miten tutkimuksen tavoite on tarkoituksena saavuttaa ja miten tutkimuskysymyksiin pystytään vastaamaan tutkimuksesta saatavalla tiedolla. Tutkimusstrategiaan ja sen valintaan vaikuttavat tutkimuksen lähestymistapa, metodologiset ja muut valinnat liittyen tutkimukseen, jotka yhdessä vaikuttavat käytettävien tutkimusstrategioiden rajaukseen. Aiempien tutkimusvalintojen valossa tässä tutkimuksessa tutkimusstrategiana käytetään tapaustutkimusta, joka on yksi laadullisten tutkimusten päätutkimusstrategioista. (Saunders et al. 2019) Tapaustutkimusta käytetään monissa eri tieteenaloissa ja erilaisista lähtökohdista, jolloin yleistä selitystä tai määrittystä tapaustutkimukselle voi olla haastavaa antaa. Kaikissa tapaustutkimuksissa tyypillistä kuitenkin on tietyn tai tiettyjen tapausten tarkastelu ja siitä

jatkuva määrittely, analysointi ja ratkaisu, jotka kuuluvat tapaustutkimuksen tavoitteeseen. (Eriksson & Koistinen 2005)

Tapaustutkimusta käytetään tutkimusstrategiana usein tutkimuksissa, joissa tarkoituksena on tutkia tarkemmin jotakin yksittäistä tapahtumaa, ilmiötä tai tiettyä kokonaisuutta eri tietolähteitä hyödyntäen (Saunders et al. 2019). Tapaustutkimus voidaan nähdä myös kokoavana tutkimusotteena jonkin tietyn ilmiön tai asian tarkempaan tutkimiseen (Korhonen 2009). Tapaustutkimus on empiiristä tutkimusta, jossa tutkitaan tiettyä ilmiötä nykyisessä kontekstissa (Yin 2014 s. 237). Tyypillisesti tapaustutkimukset voivat käsittää useita tutkimustapoja ja -aineistoja ja yhdistellä niitä tutkimuksessa (Korhonen 2009).

Tapaustutkimus sopii hyvin tutkimusstrategiaksi tähän tutkimukseen, sillä tutkimuksen kohteena ovat eri terveydenhuollon organisaatiot samasta tutkittavasta ilmiöstä, kyberturvallisuuden nykytilasta tietoverkkoon liitettävistä fyysistä lääketieteellisistä laitteista, ja niihin liittyvistä prosesseista ja tapahtumista ja toiminnasta. Tapaustutkimuksen tavoitteena nähdään olevan ymmärryksen luominen ja yleistettävyyys, joka tässä tutkimuksessa toteutuu haastattelemalla terveydenhuollon eri organisaatioita ja luomalla näiden aineistojen avulla ymmärrystä kyberturvallisuudesta lääkinnällisissä laitteissa terveydenhuollossa kansallisella tasolla. Rajaamalla tutkimuksen ilmiön tapauskontekstiksi, voidaan tutkimuksen avulla luoda syvällistä ymmärrystä ja laajempaa tietämystä tietystä tutkimuksen kohteena olevasta ilmiöstä.

4.1.5 Aikahorisontti: Poikittaistutkimus

Saundersin et al. (2019) sipulimallin seuraava kerros tutkimusmetodologisesta valinnasta on aikahorisontin määrittelemine. Tutkimuksen aikahorisontiksi voidaan valita pitkittäis- tai poikittaistutkimus, jotka määrittävät ilmiön tutkimisen aikaväliä. Pitkittäistutkimuksessa tutkittavaa ilmiötä on tarkoitus seurata pitkällä aikavälillä ja tutkia erityisesti tuolla aikavälillä tapahtuvaa mahdollista kehitystä ja muutosta. Poikittaistutkimuksessa puolestaan tarkoituksena on tutkia tietyssä ajanhetkessä esimerkiksi jonkin asian nykytilaa ja muodostaa senhetkisestä tilanteesta tilannekuva. (Saunders et al. 2019) Tässä tutkimuksessa hyödynnetään poikittaistutkimusta, sillä tavoitteena on selvittää ja saada ymmärrystä lääketieteellisten laitteiden kyberturvallisuuteen liittyvästä nykytilasta terveydenhuollon organisaatioissa tällä hetkellä. Nykytilaa tutkitaan haastattelemalla eri organisaatioita tietyn aikavälin sisällä, jolloin voidaan vertailla haastattelutuloksista koostettavia eri organisaatioiden nykytiloja toisiinsa samassa ajanhetkessä.

4.2 Tapaustutkimuksen menettelytavat – kirjallisuuskatsaus ja haastattelututkimus

Tutkimus koostuu teoriapohjaisesta kirjallisuuskatsauksesta ja empiirisestä tutkimuksesta, jotka toimivat tutkimuksen menettelytapoina. Tutkimus toteutetaan laadullisena monimenetelmänä, jossa ensin esitellään kirjallisuuskatsaus, joka luo teoreettisen ymmärryksen ja syventävän tiedon kyberturvallisuudesta terveydenhuollossa ja lääketieteellisten tietoverkkoon kytkettävien fyysisten laitteiden osalta. Kirjallisuuskatsauksen jälkeen tarkastellaan aihetta empiirisen tutkimuksen, haastatteluaineistojen, valossa ja pyritään luomaan haastattelujen pohjalta kyberturvallisuudesta kattavaa nykytilakuvausta lääketieteellisten laitteiden osalta terveydenhuollon organisaatioihin yleistäen.

4.2.1 Kirjallisuuskatsaus

Tässä tapaustutkimuksessa käytetyistä menetelmistä tutkimuksessa ensimmäisenä käytetään kriittisesti toteutettavaa kirjallisuuskatsausta. Kirjallisuuskatsauksen avulla alustetaan empiiristä tutkimusta taustoittamalla tutkittavaa ilmiötä sekä lisäämällä siihen liittyvää tietoa ja ymmärrystä. Erikssonin & Koistisen (2005) mukaan teoriasta lähtevässä tapaustutkimuksessa on hyödyllistä tutustua aiheeseen liittyvää teoreettiseen viitekehykseen sekä luoda kirjallisuuskatsaus mahdollisuuksien mukaan ennen haastatteluaineiston keruuta. Kirjallisuuskatsauksella voidaan luoda aiheesta riittävä ymmärrys liittyen aiheeseen, taustaan ja mahdollisiin ristiriitaisuuksiin (Saunders et al. 2019) Tällaisen kirjallisuuskatsauksen tarkoituksena on saada tuotettua kokonaisvaltaista ymmärrystä ja teoreettista tietoa kyberturvallisuudesta terveydenhuollossa ja erityisesti lääketieteellisten laitteiden osalta.

Kirjallisuuskatsaukseen käytetään iteratiivista prosessia suoraviivaisen sijasta ja prosessi kestää koko tutkimusprosessin ajan ja kulminoituu tutkimuksen havaintoihin ja tuloksiin. Kirjallisuuskatsauksessa käytyä teoriaa hyödynnetään siis läpi tutkimuksen, empiiristä osuutta myöden, ja käsitellään uuden, luodun tiedon kanssa. Kirjallisuuskatsauksen iteratiiviseen prosessiin kuuluu teorian jatkuvan hyödyntämisen lisäksi myös sen korostettu kriittisyys. Kriittisyys muodostuu mukaan otettavan kirjallisuuden harkinnanmukaisella ja tarkalla valinnalla, tärkeimpien aineistojen kokonaisvaltaisella kuvaamisella sekä aineistojen valitsemisella. Kriittisyyden lisäksi kirjallisuuskatsauksessa tulee aineistojen käytön olla perusteltua, mikä tapahtuu läpinäkyvyytenä aineistojen kuvaamisessa ja hyödyntämisessä. (Saunders et al. 2019)

Kirjallisuuskatsauksen tutkimusaineistoa hakemiseen on käytetty Tampereen yliopiston tietokantoja, kuten Andorista, ScienceDirectistä ja Scopus:sta. Taulukossa 5 on kootusti

nähtävillä hakutulokset muutamilla esimerkkinä toimivilla hakulausekkeilla aiemmin mainituista kolmesta hakutietokannasta. Taulukon hakulausekkeiden lisäksi käytettiin muitakin hakulausekkeitä korkealaatuisten ja aiheeseen liittyvien teosten löytämiseksi. Hauissa on käytetty pääosin englannin kieltä, mutta myös joitakin suomalaisia hakulausekkeitä ja sitä kautta löytyviä aineistoja on tutkimuksessa hyödynnetty. Hakulausekkeiden tarkan kohdentamisen tarkoituksena on edistää ajankohtaisten ja aiheeseen vastaavien korkealaatuisten tieteellisten julkaisujen löytämistä.

Hakulauseke	Andor	Science-Direct	Scopus
"cyber security" AND "medical device"	15 243	285	822
"cybersecurity" AND "medical device"	32 797	496	1 338
"cybersecurity" AND "medical device" AND "current state"	597	68	68
"cybersecurity" AND "medical device network"	283	3	10
"cybersecurity" AND "networked medical device"	457	23	115

Taulukko 4. Hakulausekkeiden osumien määrä tutkimuskäsitteistä valikoiduissa tietokannoissa.

Tutkimuksessa käytetyt julkaisut ovat pääosin tieteellisiä ja vertaisarvioituja lähdemateriaaleja. Tieteellisten artikkeleiden ja julkaisujen lisäksi tutkimuksessa on hyödynnetty muita julkaisuja esimerkiksi käsitteiden määrittelyssä ja terveydenhuollon alaa koskissa säädöksissä. Käsitteiden määrittelyssä on käytetty muun muassa Turvallisuuskomitean (2018) "Kyberturvallisuuden sanasto" -julkaisua, josta on hyödynnetty käsitteitä kyberturvallisuuden kontekstista. Kirjallisuuskatsauksessa tarkastellaan ensin kyberturvallisuutta terveydenhuollossa ja sen organisaatioissa sekä lääketieteellisiä laitteita erityisesti tietoverkkoon liitettävien fyysisten laitteiden osalta. Tämän jälkeen tarkastellaan teorian pohjalta näiden tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kyberturvallisuutta terveydenhuollon organisaatioissa ja pyritään kokoamaan tämän teorian kautta ymmärrystä. Williams & Woodward (2015) artikkeli, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, kertoo tietoverkkoon liitettyjen lääkinnällisten laitteiden uhkista ja haasteista sekä sisältää yleisesti kyberturvallisuuteen liittyviä uhkia ja haavoittuvuuksia näissä laitteissa. Samaan aihe-

seen liittyen Yaqoob, Abbas & Atiquzzaman (2019) artikkeli *Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices* perehdyttää tarkemmin erilaisten lääkinällisten laitteiden tyypeihin, hyökkäysmetodologeihin ja haavoittuvuuksiin.

4.2.2 Puolistrukturoitu haastattelu

Tutkimuksen kohteena on kyberturvallisuuden nykytilan ymmärtäminen ja kartoittaminen lääketieteellisissä laitteissa ja tätä kokonaisuutta pyritään tutkimaan laadun, ominaisuuksien ja merkitysten avulla. Tutkimuksessa kerätään primääristä dataa tutkimushaastatteluiden avulla. Tutkimus on luonteeltaan subjektiivinen ja moninainen, missä tutkimuksen kohde ja tutkija ovat vuorovaikutuksessa toistensa kanssa. Tutkimus on tällöin arvosidonnainen ja tutkittavien äänet tulevat kuuluviin. (Hirsjärvi & Hurme 2001) Tutkimushaastatteluiden tarkoituksena on keskustelulla ja vuorovaikutuksella, jolla on ennalta päätetty tarkoitus eli tutkimustehtävä sekä osallistujaroolit, kerätä tietoa halutusta kohteesta. (Ruusuvoori & Tiittula 2017).

Tutkimushaastattelun menetelmäksi on valittu puolistrukturoitu haastattelu. Puolistrukturoitu haastattelut eivät ole standardimuotoisia, sillä niitä voi toteuttaa monella tavalla eri teemojen avulla (Saunders et al. 2019). Sen takia puolistrukturoitu haastattelu sijoittuu strukturoidun ja teemahaastattelun välille (Hirsjärvi & Hurme 2001). Lisäksi puolistrukturoidun haastattelun avulla voidaan saada selville ja ymmärtää tutkimuksen aiheiden ja tutkittavien asioiden välisiä suhteita, sekä tarjoamaan tutkimukselle tärkeää taustaa. (Saunders et al. 2019)

Puolistrukturoitu haastattelussa esitetään samat kysymykset kaikille haastateltaville. On kuitenkin mahdollista, että joitakin kysymyksiä jätetään välistä, mutta yleensä kysymysten järjestystä ei muuteta. (Hirsjärvi & Hurme 2001) Tässä tutkimuksessa haastatteluihin on hahmoteltu viisi eri aihealueittain rajattua teemaa, joita käsitellään haastateltavien kanssa. Haastattelujen kulkua voidaan muokata haastateltavan tietämyksen ja asiantuntijuuden mukaan, jolloin aihealueiden kysymyksiä voidaan tarkentaa, muokata tai jättää välistä. Kaikille haastateltaville esitetään kuitenkin kaikki kysymykset ja kysymykset ovat samassa esitysmuodossa, jotta haastattelussa pysyy sama runko ja haastattelu etenee samankaltaisesti kaikkien haastateltavien osalta. Puolistrukturoidun haastattelun avulla tutkittavat saavat oman äänen kuuluviin ja haastatteluista voidaan saada monitahoisia vastauksia eri organisaatioilta. Haastateltavien valinnassa on käytetty hyödyksi tarkoituksenmukaista valintaa, jossa hyödynnettiin lääketieteellisten laitteiden kanssa työskenteleviä asiantuntijoita tietystä organisaatiosta (Saunders et al. 2016).

Haastattelukysymykset on aiemmin määritelty ja kysymysrunko luotu. Kysymysrunko on kaikille haastateltaville sama, mutta kysymysten järjestys saattaa vaihdella ja niitä voidaan täydentää mahdollisilla tarkentavilla kysymyksillä haastattelun kulusta ja haastateltavan asiantuntijuudesta riippuen. Haastattelut toteutettiin etähaastatteluilla internetin välityksellä. Saundersin et al. (2019) mukaisesti tietokoneella tehtäviä haastatteluja kuvataan sähköisiksi haastatteluiksi, jotka jaotellaan vielä ei-synkronisiin ja synkronisiin sähköisiin haastatteluihin. Tässä tutkimuksessa hyödynnettiin synkronista sähköistä haastattelua, sillä haastattelu tehtiin reaaliajassa, yhdessä sovittuna ajanhetkenä. Internetin välityksellä toteutettavissa haastatteluissa on tärkeä hyödyntää mahdollisuuksien mukaan videokuvaa, jotta mahdolliset vastaukseen liittyvät havainnot ja elkeet tulisivat esille haastattelussa. Lisäksi haastatteluissa olisi Saundersin et al. (2019) mukaisesti tärkeää luoda rentoa ilmapiiriä, sillä tietokoneen ja puhelimen välityksillä tehtävissä haastatteluissa voi muuten muodostua hyvinkin suoraviivainen ja pelkästään asiapitoinen haastattelutilanne, jossa kaikkea ei välttämättä saada kuvattua tai haastateltava ei ole halukas kaikkea tietämystään jakamaan. Tällöin myös haastattelutilanteesta tulee enemmän vuorovaikutteisempi. Videokuvaa hyödynnettiin osassa haastatteluja, mutta muutamassa videokuvaa ei pidetty päällä teknisistä syistä.

4.2.3 Tutkimuksen luotettavuus ja tiedon laadukkuus

Tutkimuksen eri vaiheissa on syytä arvioida tutkimuksen laadukkuuteen vaikuttavia tekijöitä ja pyrkiä toteuttamaan tutkimusta näiden kriteerien kautta. Tässä tutkimuksessa hyödynnetään tapaustutkimusta, jossa Yinin (2014) mukaisesti voidaan arvioida tutkimusvaiheita rakenteellisen, ulkoisen ja sisäisen validiteetin sekä reliabiliteetin näkökulmasta. Rakenteellisella validiteetilla pyritään valitsemaan tutkimusmenetelmät ja -kohteet mahdollisimman sopiviksi tutkimuskohteen mukaisiksi (Yin 2014). Rakenteellista validiteettia on luotu tähän tutkimukseen valitsemalla tutkimusmenetelmäksi haastattelut, joista on saatu aineistoon monesta eri organisaatiosta ja rooleista näkemyksiä. Haastatteluiden rakenteellista validiteettia korostaa tässä tutkimuksessa erityisesti haastateltavien onnistunut valinta liittyen aiheen tietämykseen, joka korostuu vähäisemmässä haastatteluiden määrässä.

Ulkoista validiteettia voidaan hyödyntää teorian muodostuksessa sekä kirjallisuuden ja empiirisen osuuden vertailussa. Ulkoisessa validiteetissa tutkitaan, miten tutkimuksen tuloksia voitaisiin yleistää kattamaan tutkittavia ilmiöitä, tapahtumia tai organisaatioita. (Yin 2014, s. 234) Koska tutkimuksessa kuvataan ja tutkitaan lääketieteellisten laitteiden

kyberturvallisuutta ja nykytilaa kolmessa eri organisaatiossa, voidaan tutkimustuloksia yleistää suurimmalta osin terveydenhuollon organisaatioihin kansallisella tasolla.

Sisäisellä validiteetilla tarkoitetaan sitä, miten tutkimuksesta voidaan luoda syy-seuraussuhteita ja se voidaan nähdä yhdeksi tärkeimmistä laadullisista kriteereistä tutkimuksissa. Sisäisellä validiteetilla pyritään selittämään minkä takia tutkittavaan ilmiöön liittyvät asiat tapahtuvat ja löytämään samankaltaisia vastauksia ja kaavoja haastatteluaineistoista eri organisaatioista. (Yin 2014) Näistä aineistojen kohdista pyritään selittämään syitä ja seurauksia tapahtumille kokonaisvaltaisesti ja monipuolisesti. Tässä tutkimuksessa voidaan sisäistä validiteettia nähdä käytettävän erityisesti sen suhteen, miten ja miltä osin nykyistä kyberturvallisuuden tilaa voitaisiin kehittää lääketieteellisten laitteiden suhteen.

Reliabiliteetti kuvaa tutkimuksessa käytettyjen menetelmien kykyä tulla toistettavaksi ja toimia johdonmukaisesti. (Yin 2014) Reliabiliteettia voidaan edistää tutkimuksessa varmistamalla mahdollisimman neutraali ja objektiivinen aineiston kerääminen, tieteellisten käytäntöjen noudattaminen sekä yleisesti tutkimuksen suorittaminen mahdollisimman läpinäkyvästi esimerkiksi tutkimusmenetelmistä kertomalla ja niiden kanssa oikein toimimalla. Tutkimuksessa on pyritty tähtäämään korkeaan reliabiliteettiin kuvaamalla tutkimusmetodologian osuudet tarkasti ja luomalla haastatteluihin hyvien tieteellisten käytäntöjen sekä tutkimushaastatteluiden mukaisen ympäristön.

Tutkimuksen puolistrukturoiduissa haastatteluissa voidaan kohdata haasteita tiedon luotettavuuteen ja oikeellisuuteen liittyen, jotka voivat johtua esimerkiksi haastateltavasta, haastattelijasta tai haastattelun toteuttamisesta etäyhteyksillä. Haastattelijalla on vastuu luoda haastattelusta tilanne, jossa ei haastateltavaa johdateta vastaamaan tietyllä tavalla. Haastattelutilanteessa kysymysrungolla ja haastattelijan sanavalinnoilla tulee luoda neutraali tilanne haastateltavalle vastata kysymyksiin ilman, että muiden näkemykset ja uskomukset vaikuttavat vastauksiin. Toisena haasteena voidaan nähdä haastatteluissa tilanne, jossa haastateltava ei ole halukas kertomaan sensitiivistä tietoa haastatteluissa, jottei haastateltava joutuisi vastaamaan kysymyksiin, jotka voisivat asettaa hänet roolissaan tai organisaation epäsuotuisaan tilanteeseen. (Saunders et al. 2019) Tällöin haastateltavan vastaukset voivat jäädä vajaiksi ja haastatteluilla ei saada aiheeseen tai ilmiöön liittyviä todellisia haasteita tai epäkohtia esiin. Haastattelun luotettavuutta ja tiedon oikeellisuutta on edistetty tässä tutkimuksessa läpinäkyvällä tutkimussuunnitelmalla, joka on jaettu organisaatioiden nähtäväksi ennen tutkimuslupien saamista ja haastateltavat ovat päässeet tutustumaan tiedotteeseen tutkimuksesta. Osana tutkimussuunnitelmaa ja -tiedotetta on esitelty tutkimuksen toteutusmenetelmät sisältäen haas-

tattelujen toteutustapa ja aineiston analysointiin liittyvän datan käsittelyn elinkaari. Lisäksi haastateltavat ovat saaneet kalenterikutsun yhteydessä haastattelussa katettavien aiheiden ja teemojen listauksen.

Puolistrukturoidun haastattelututkimuksen luotettavuutta voidaan edistää tutkijan omalla, hyvällä tietämystasolla, kehittämällä haastatteluteemoja ja kommunikoimalla haastattelutilanteesta ennakkotietoa haastateltavalle sekä valitsemalla haastatteluympäristöksi siihen soveltuva tila (Saunders et al. 2019, s. 451). Tutkimuksen luotettavuutta ja laadukkuutta tässä tutkimuksessa on pyritty edistämään tutkijan oman tietämyksen varmistamisella lukemalla ja ottamalla selvää aiheeseen liittyvistä artikkeleista ja julkaisuista. Tutkijalla on myös aiheesta aikaisempaa tietämystä oman kyberturvallisuuteen liittyvän työnkuvan kautta.

4.3 Haastattelujen tiedonkeruu, kysymykset ja haastateltavat

Tapaustutkimukselle tyypilliseen tutkimustapaan tutkimusdata kerättiin haastatteluilla. Tutkimuksen puolistrukturoidut haastattelut toteutettiin asiantuntijahaastatteluina, joihin haastateltaviksi valikoitui kohdeorganisaatioista lääkinnällisten laitteiden ja tietohallinnon asiantuntijoita, jotka tunnistettiin tutkimusluvan hakemisen yhteydessä tietävän kyberturvallisuudesta sekä lääketieteellisistä laitteista terveydenhuollon toimintaympäristössä. Tutkimushaastatteluja järjestettiin kokonaisuudessaan viiden eri asiantuntijan kanssa ja kolmesta eri organisaatiosta. Haastateltavien tarkat roolikuvaukset ja -vastuut saattoivat erota toisistaan, mutta haastateltavien toimintaympäristöt ja vastuualueiden sisällöt olivat vertailtavissa. Taulukossa 6 on kuvattu haastateltujen henkilöiden vastuualueet ja viittaukset aineiston analyysissä.

Tutkimuksessa käytetty viittaus	Vastuualue ja kohdeorganisaation
Haastateltava 1	Lääkintäteknikka, organisaatio 1
Haastateltava 2	Tietoturva, organisaatio 1
Haastateltava 3	Lääkintäteknikka, organisaatio 2
Haastateltava 4	Lääkintäteknikka, organisaatio 2
Haastateltava 5	Lääkintäteknikka, organisaatio 3

Taulukko 5. Tutkimukseen osallistuneet haastateltavat henkilöt ja viittaustapa heihin tutkimuksessa.

Haastattelut järjestettiin etäyhteyksillä, haastateltavien kanssa kahdestaan toteutettuna, jossa haastateltavan ja haastattelijan välillä käytiin vuorovaikutuksellista keskustelua.

Haastatteluiden järjestämisessä on huomioitava sopivan ympäristön valinta, jossa haastateltava ja haastattelija voivat keskustella luottamuksellisesti ja totuudenmukaisesti (Rabionet 2011). Haastateltavan ja haastattelijan kaksistaan toteutetut haastattelut toimivat näissä asiantuntijahaastatteluissa, sillä niiden kautta saatiin yhden organisaation ja sen asiantuntijan näkökulmia kokonaisvaltaisesti esille sekä kuultiin luottamuksellista tietoa, mitä ei välttämättä voitaisi ryhmähaastatteluissa tuoda muuten esiin tai näkemykset jäisivät vajaiksi muiden henkilöiden kertoessa toista henkilöä enemmän.

Haastattelukysymyksien luonnostelussa ja lopullisen haastattelurungon valinnassa käytettiin apuna tietoturvallisuuden asiantuntijoita. Rabionetin (2011) asiantuntijoiden käyttäminen haastattelukysymyksien määrittämiseen on hyödyllistä erityisesti laadun näkökulmasta. Asiantuntijoiden avulla haastattelukysymyksiä saatiin tarkennettua ja määritettyä tarkemmin selkeyttämällä kysymysten muotoilua. Lisäksi kysymykset saatiin järjestettyä loogiseen järjestykseen ja muodostettua kysymyksistä selkeät aihealueet, jotka muodostivat tutkimushaastattelun punaisen langan.

Tutkimushaastattelu koostui kokonaisuudessaan viidestä eri osa-alueesta – haastateltavan taustatiedoista, fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden ja kyberturvallisuuden nykytilasta, laitteisiin liittyvästä kyberturvallisuuden hallinnasta ja valvonnasta, laitteiden hankinnasta ja siihen liittyvästä kyberturvallisuudesta sekä vastuiden jakamisesta laitteisiin liittyen. Tutkimushaastattelun haastattelukysymysrunko on liitteenä 2. Haastattelussa käsiteltiin aluksi lyhyesti haastateltavien henkilöiden taustatietoja nimeen ja työhistoriaan liittyvien kahden kysymyksen kautta. Tämän jälkeen siirrytään käsittelemään organisaation lääketieteellisiä laitteita ja niiden kyberturvallisuutta sekä kyberriskien vastuiden jakautumiseen, hallintaan ja seurantaan liittyviä asioita. Henkilötietojen jälkeen käsitellään toisessa osiossa lääkinnällisiä laitteita ja niiden kyberturvallisuuden nykytilaa. Kolmannessa osiossa kysymykset liittyvät kyberturvallisuuden hallintaan ja valvontaan lääketieteellisissä laitteissa. Neljäs osio kattaa aiheita liittyen kyberturvallisuuden huomiointiin lääketieteellisten laitteiden hankinnassa. Viidennessä ja samalla viimeisessä osiossa kysymykset liittyvät kyberturvallisuuteen liittyviin vastuisiin lääketieteellisistä laitteista organisaatiossa. Haastateltavat saivat haastattelun pääteemat ja jokaisen osion esimerkkikysymykset nähtäville ennen haastattelua, jotta he pystyivät tutustumaan teemoihin ja niiden tulokulmiin haastattelua varten.

Haastattelut järjestettiin noin 60 minuutin etähaastatteluina Microsoft Teamsin avulla. Etähaastattelut valikoituivat haastattelutavaksi mahdollisimman helpon saavutettavuuden ja tehokkuuden takia. Brymanin (2012) mukaan verkkotyökalujen käyttö on suositeltavaa, kun haastateltavat sijaitsevat eri kaupungeissa. Etähaastatteluihin liittyvät mahdolliset haasteet, kuten mahdolliset väärät tulkinnot ja visuaalisten apukeinojen rajallinen

käyttö, on otettava huomioon haastattelutilanteissa ja pyrittävä välttämään niitä (Gubrium et al. 2021). Haastatteluiden tallentamiseen käytettiin muistiinpanojen kirjoittamista.

Tutkimuksen kohderyhmänä on terveydenhuollon julkiset organisaatiot. Tutkimuksessa lähestyttiin viittä eri kansallista terveydenhuollon toimijaorganisaatiota, joista kolmesta saatiin tutkimuslupa. Yksi kontaktoiduista organisaatiosta ei vastannut tutkimuslupakyselyihin ja yksi organisaatio kieltäytyi tutkimusluvan etenemisprosessista. Haastateltavat valittiin kyberturvallisuuden ja lääkinnällisten laitteiden tietämyksen näkökulmasta. Kokonaisuudessaan haastatteluja saatiin kolmesta eri organisaatiosta viideltä eri henkilöltä, jotka työskentelivät kyberturvallisuuden ja lääketieteellisten laitteiden parissa tietohallinnon tai lääkinnällisten laitteiden työnkuvissa.

Kokonaisuudessaan haastatteluja pidettiin viisi kappaletta. Haastatteluihin pyrittiin löytämään alun perin organisaatiosta yhdestä kolmeen henkilöä, joita haastateltaisiin joko yksilö- tai ryhmähaastattelulla. Kaikista kolmesta organisaatiosta tunnistettiin kaksi henkilöä osallistumaan haastatteluihin, joihin lopulta osallistui kahdesta organisaatiosta kaksi henkilöä ja yhdestä organisaatiosta yksi henkilö. Haastatteluja pidettiin yksi haastattelu haastateltavaa kohden, mutta kaikille haasteltaville kommunikointiin mahdollisten lisäkysymysten ilmaantuessa, että olisi mahdollista kysyä niitä esimerkiksi sähköpostitse.

Haastateltavien tietämyksen ja kolmen eri organisaation haastatteluiden näkökulmien ja toimintatapojen avulla tutkimusta sekä sen aineistoa voidaan pitää varteenotettavana ja luotettavana tulosten yhteenvetojen ja johtopäätösten osalta, vaikka haastatteluotanta onkin suhteellisen pieni. Merkityksellisenä asiana kuitenkin nähdään haastateltavien onnistunut tunnistaminen organisaatioissa, jolla onnistuttiin haastattelemaan ihmisiä työrooleista, jotka osasivat kertoa aiheesta sekä tunnistaa siihen liittyviä haasteita, onnistumisia ja kehityskohteita. Tarvittaessa kysymyksiä voitiin tarkentaa tai antaa esimerkkejä, mikäli haastateltava ei ymmärtänyt minkälaista vastausta kysymykseen haettiin tai kaipasi esimerkkejä. Tällaisessa tilanteessa haastateltavan piti kuitenkin olla tarkkana, ettei haastatteluissa tapahtuisi johdattelua vastauksiin.

4.4 Haastatteluaineiston analysointi

Tutkimusaineisto koostui haastatteluiden muistiinpanoista. Haastattelut kestivät noin 45 minuutista 70 minuuttiin ja keskimäärin noin 60 minuuttia. Pitkien ja laadukkaiden yksilöhaastatteluiden avulla asiantuntijoilta saatiin kysymyksiin kokonaisvaltaisia ja laajoja

vastauksia eri näkökulmista. Muistiinpanot ja kaikki tiedot saatiin kerättyä tutkimushaastatteluiden vastauksista. Kaikilta haastateltavilta pyydettiin erikseen lupa lähestyä sähköpostilla tai uudella lyhythaastattelulla, mikäli haastattelun vastauksiin tarvittaisiin myöhemmin tarkennusta tai jatkokysymyksiä.

Tutkimuksessa kerättiin ja tallennettiin vain tutkimuksen tarkoituksen kannalta välttämättömiä henkilötietoja, jotka tässä tutkimuksessa olivat haastateltavan nimi ja työhistoria. Haastattelun tutkimustuloksia käsiteltiin luottamuksellisesti henkilötietojen käsittelyä koskevan lainsäädännön edellyttämällä tavalla ja organisaatioiden tutkimuslupien mukaisesti. Haastatteluihin osallistuvat henkilöt ja heidän edustamat organisaatiot jäivät vain tutkimuksen toteuttamiseen osallistuvien henkilöiden tietoon. Yksittäisen tutkittavan tunnistaminen ei ole mahdollista tutkimustulosten julkaisuista tai selvityksistä. Lopulliset tutkimustulokset raportoitiin opinnäytetyön yhteydessä siten, että vastaajan henkilöllisyyttä tai hänen edustamaa organisaatiota ei voida tunnistaa, ja tutkimuksen julkistamisen jälkeen aineisto anonymisoitiin henkilötiedoista.

Tutkimushaastatteluista saadut aineistot anonymisoitiin ja kaikkien haastateltavien vastaukset taulukoitiin haastattelukysymysten mukaan. Haastateltavien vastauksista pyrittiin löytämään yhtenäisyyksiä teemoissa ja aiheissa, joiden mukaan havaintoja vastauksista voitiin ryhmitellä ja jaotella keskenään kokonaisvaltaisen käsityksen muodostamiseksi tietyistä aiheista. Haastateltavista organisaatioista saatiin omaan toimintaan liittyviä vastauksia, joita voidaan verrata muiden organisaatioiden haastateltavien vastauksiin. Saman organisaation haastateltavien vastauksista saatiin vastauksia, jotka täydentävät ja tarkentavat toistensa vastauksia riippuen haastateltavan roolista ja työnkuvasta liittyen haastatteluaiheeseen.

Haastattelujen analysointiin on käytetty temaattista analyysiä aineistojen käsittelyssä. Temaattisessa analyysissä tutustutaan aineistoon tarkalla tasolla, koodataan aineistoa, jalostetaan teemoja ja testataan ehdotuksia (Saunders et al. 2019). Aineistoon tutustuminen tapahtuu haastatteluaineistoa tarkastellessa sekä koodatessa pääteemoja ja -sisältöjä (Gubrium et al. 2012) Värikoodausta on tehty teemojen mukaan aineistossa. Teemojen koodaamisen ja tunnistamisen jälkeen voidaan aineistosta havaita ja tarkastella tarkemmin teemoja suhteessa toisiin teemoihin (Saunders et al. 2019). Haastattelutulokset ja haastattelusta lainattuja suoria viittauksia esitellään kirjallisesti empiirisessä osuudessa. Haastatteluaineistoista pyrittiin löytämään eri organisaatioiden välisiä samankaltaisuuksia sekä eroavaisuuksia, jotka tulivat esille samoista aiheista ja teemoista. Myös samasta organisaatiosta haastateltavat henkilöt saattoivat tuoda eri asioita esille kysyttäessä samaa kysymystä. Erot vastauksissa liittyivät usein työrooliin ja siihen, että toinen

henkilö ei osannut vastata kysymykseen niin tarkasti kuin toinen, joka käsittelee kysymykseen liittyviä asioita toista enemmän. Tällaisissa asioissa on voitu aineiston analysoinnissa korostaa vastauksia henkilöltä, jolla on enemmän kosketuspintaa asian suhteen. Haastatteluaineistosta nostettiin esille myös saman organisaation haastatteluista molempien nostamia ja korostamia asioita, joilla voidaan vahvistaa nykytilanteen määrittämistä.

Temaattisen analyysin tavoitteena on tutkimuksessa saada nostettua nykytilaan liittyviä teemoja, sisältöjä ja osa-alueita terveydenhuollon organisaatioiden kyberturvallisuuden näkökulmasta fyysisistä tietoverkkoon liitettävistä lääketieteellisistä laitteista. Tarkoituksena on selvittää tarkemmalla tasolla, miten organisaatiot tekevät laitteisiin liittyvää riskienhallintaa, miten kyberturvallisuushilta suojaudutaan ja minkälaisia haavoittuvuuksia sekä uhkia on, kuinka hankinnassa otetaan kyberturvallisuus huomioon sekä miten vastuut jakautuvat laitteiden kyberturvallisuudessa. Haastatteluaineiston tehdyistä havainnoista muodostettiin sanallisesti kuvailua nykytilan analyysistä. Nykytilan analyysin lisäksi kuvataan kehityskohteita ja mahdollisuuksia liittyen lääketieteellisten laitteiden kyberturvallisuuteen liittyen terveydenhuollon organisaatioihin kansallisesti. Haastatteluaineiston laadullista dataa esitellään luvussa viisi, jossa dataa on analysoitu ja yhdistetty syyseuraussuhteiden luomiseksi. Analysointi on tehty haastattelurungon teemojen mukaisesti samassa järjestyksessä.

Haastattelutulosten analysoinnin jälkeen esitetään analysointia yhdistettynä kirjallisuuteen ja teoriaan sekä johtopäätöksiin. Haastattelutuloksia voidaan verrata aikaisempaan kirjallisuuteen ja tehtyihin tutkimuksiin fyysisistä tietoverkkoon liitettävistä laitteista. Tutkimuksen luvussa kuusi tehdään analysoinnin huomioista johtopäätöksiä yhdistettynä kirjallisuuden huomioihin terveydenhuollon kyberturvallisuuden hallinnoimisesta, vastuiden jakamisesta, riskienhallinnasta ja suojautumisesta fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden osalta.

5. KYBERTURVALLISUUDEN NYKYTILA TIETOVERKKOON LIITETTÄVISSÄ FYYSISISSÄ LÄÄKINNÄLLISISSÄ LAITTEISSA

Viidennessä luvussa esitetään tutkimuksen tulokset. Alaluvuissa käsitellään tutkimustuloksia tutkimuksen haastattelurungon mukaisten teemojen mukaisesti ja samassa järjestyksessä. Ensimmäisessä alaluvussa käsitellään tietoverkkoon liitettävien lääketieteellisten laitteiden riskejä ja riskienhallintaa sekä minkälaisia vaikutuksia kyberturvallisuusriskeillä on terveydenhuollon organisaatioihin. Toisessa alaluvussa käydään läpi tietoverkkoon liitettävien lääketieteellisten laitteiden hallintaa ja valvomista. Hallinnan ja valvomisen lisäksi toisessa alaluvussa käsitellään, miten haavoittuvuuksien ja poikkeamien hallintaa toteutetaan ja minkälaisia suojaustapoja on käytössä organisaatioissa. Kolmannessa alaluvussa tarkastellaan laitteiden hankintaa ja laitevalmistajien kanssa tehtävää yhteistyötä kyberturvallisuuden näkökulmasta. Neljännessä alaluvussa käsitellään kyberturvallisuuteen ja lääketieteellisten laitteisiin liittyvien vastuiden jakautumista ja seurannan tapoja. Näiden alalukujen käsittelyn jälkeen pystytään vastaamaan kyberturvallisuuden riskienhallinnasta tietoverkkoon liitettävien lääketieteellisten laitteiden osalta, joka toimii pääkysymyksenä ja jonka selvittämiseen käytetään alatutkimuskysymyksiä.

5.1 Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet ja niihin liittyvät riskit ja riskienhallinta

Tutkimuksen ensimmäisessä teemassa käsitellään tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden nykytilaa ja minkälaisia riskejä kyberturvallisuuden näkökulmasta laitteisiin kohdistuu ja miten riskienhallintaa toteutetaan. Teemaan liittyen esitettiin kysymyksiä haastatteleamalla haastateltavia sekä vertailemalla eri asiantuntijoiden vastauksia riskeistä ja uhkista sekä niiden tunnistuksesta, hallinnoimisesta ja mahdollisista vaikutuksista terveydenhuollon organisaatioon.

Lääketieteelliset laitteet terveydenhuollon organisaatioissa – Haastateltavat 4 ja 5 kertoivat erilaisista terveydenhuollon lääketieteellisistä laitteista, mitä heidän edustamillaan organisaatioilla oli ja mistä lääkintäteknikka on vastuussa. Organisaatioissa lääketekniikan asiantuntijoille oli määritely vastuut tiettyjen laitekategorioiden ja niihin kuuluvien laitemäärien mukaan. Haastateltavan 4 organisaatioissa rajaus lääketieteellisten laitteiden vastuista rajattiin pienten ja suurten lääketieteellisten laitteiden suhteen. Haastateltavan 4 vastuulla oli organisaation isoimmat laitteet, joihin kuului muun muassa kuvantamisen laitteita. Haastateltavan 4 vastuulaitteita organisaatioissa oli noin muutama

sata laitetta. Lääkintäteknisten vastuuhenkilöiden lisäksi organisaatioissa lääkintäteknii-
kan yksikössä työskenteli huoltomestareita, joiden vastuulla oli laitteiden huoltaminen.

Kuvantamisen laitteet muodostivat yhden ison fyysisten tietoverkkoon liitettävien lääke-
tieteellisten laitteiden ryhmän. Haastateltava 4 listasi lääketieteellisiä laitteita kuuluvan
esimerkiksi kuvantamisen laitteisiin sekä pienlääkintä-, anestesia-, laboratorio- ja muihin
sairaalalaitteisiin. Kuvantamisen laitteisiin haastateltava 4 listasi muun muassa säde-
hoito-, magneetti- ja ultraäänilaitteita. Haastateltava 5 lisäsi listaan myös angiografia-,
CT-kuvaus-, SPECT/CT-kuvantamisen, PET-CT-, hammaskuvaus- ja tietokonetomogra-
fialaitteen.

Haastateltava 4 listasi pienempiä lääketieteellisiä laitteita, joita hänen edustamassaan
organisaatiossa oli noin kymmeniä tuhansia laitteita. Pienempiä lääketieteellisiä laitteita
ovat esimerkiksi hengitysapulaitteet, ruiskupumput ja potilasvalvontamonitorit. Haasta-
teltava 5 kertoi lääketieteellisiä laitteita luokiteltavan myös anestesia-, laboratorio ja sai-
raaalalaitteisiin. Anestesia-laitteisiin kuuluu esimerkiksi anestesiatyöasemat, laboratorio-
laitteisiin tutkimuslaitteet ja sairaalalaitteisiin erilaiset valaisimet ja leikkaustasot. Iso osa
organisaation lääketieteellisistä laitteista kuuluu pieniin laitteisiin, jotka eivät ole liitettä-
vissä tietoverkkoon. Puolestaan isommat lääketieteelliset laitteet, kuten kuvantamisen
laitteet, ovat käytännössä kaikki tietoverkkoon liitettäviä fyysisiä lääketieteellisiä laitteita.

Kyberturvallisuusriskit ja -uhat – Eri organisaatioiden asiantuntijat olivat suhteellisen
samaa mieltä tietoverkkoon liitettävien fyysisten laitteiden kyberturvallisuusriskeistä ja
kaikki asiantuntijat mainitsivat samoja tai samankaltaisia riskejä haastattelussa. Haasta-
teltavat tunnistivat kyberturvallisuusriskejä ja -uhkia, jotka on määritelty ja tunnistettu
haastateltavissa organisaatioissa riskeiksi ja alan yleisesti määrittelemiä tyypillisiä ris-
kejä näille laitteille. Asiantuntijoiden haastatteluissa esille tuomat riskit lääketieteellisille
laitteille on listattuna taulukkoon 7. Kaikki haastateltavat mainitsivat haastatteluissa yh-
deksi isoksi riskiksi kyberhyökkäykset, jotka nostettiin esille esimerkkien kautta muissa
terveydenhuollon organisaatioissa niin Suomessa kuin muissakin pohjoismaissa ja ym-
päri maailmaa. Kyberhyökkäyksistä erityisesti palvelunestohyökkäykset ja haittaohjel-
mat nähtiin isoimpina riskeinä, jotka ovat myös realisoituneet kansallisen terveydenhuol-
lon organisaatioissa Suomessa. Haastateltavan 4 mukaan tulevaisuudessa riskinä voi-
daan nähdä kaikenlaiset verkkoon päässeet madot ja muut verkon kautta tapahtuvat
kyberhyökkäykset ja -tapahtumat.

Haastateltavien havain- tojen teemat	Haastateltavien päähavainnot	Maininnat
Ihmisten toiminta	Laitevarkaudet ja laitteiden häviämiset	H2

	Käyttäjien tahalliset ja tahattomat virheet	H3
Tietoverkkoliikenne	Verkon kaatuminen	H1, H2, H3, H5
	Huonot turvallisuuskäytännöt ja suojaus	H1, H2, H3
Työasemat	Työasemien heikko suojaaminen	H1
Fyysinen turvallisuus	Toimitilat	H3
	Sähkönjakelujärjestelmät	H3
Kyberhyökkäykset	Haittaohjelmat: kiristyshaittaohjelmat, troijalaiset, madot, jne.	H1, H2
	Palvelunestohyökkäykset	H1, H2
Organisaatioiden prosessit, hallinta ja suunnitelmat	Prosessien ja suunnitelmien puuttuminen tai vajavaisuus	H3
Kolmannet osapuolet	Kolmansien osapuolien toiminta	H3, H4

Taulukko 6. Haastateltavien vastauksista kootut merkittävimmät tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kyberturvallisuusriskit.

Haastatteluissa nostettiin myös laitteisiin epäsuorasti kohdistuvia riskejä. Tällaiset riskit kohdistuvat yleisesti tietotekniikan laitteisiin eli esimerkiksi työasemiin tai niiden komponentteihin, joihin monet fyysiset tietoverkkoon liitettävät laitteet ovat kytkettyjä. Esimerkiksi kuvantamisen laitteissa on työasemat, joihin kohdistuvat erilaiset riskit kuin itsessään kuvantamisen laitteeseen. Työasemien kautta lääketieteelliset laitteet voivat saastua esimerkiksi ohjelmistojen haavoittuvuuksia hyödyntävistä haittaohjelmista tai muista kyberhyökkäyksistä.

Tietoverkosta nousevat riskit ovat yhtäläisesti tietoverkkoon liitettäviin lääketieteellisiin laitteisiin vaikuttavia riskejä, sillä nämä laitteet ovat yhteydessä tietoverkkoihin. Haastattelussa nostettiin esille erilaisia riskejä, jotka voivat realisoitua, mikäli verkon suojausta ei ole tehty tai suunniteltu huolellisesti. Haastateltava 5 mainitsi tietoverkon kautta kohdistuvien uhkien lisäksi yhdeksi riskiksi myös tietoverkon kaatumisen. Tietoverkon kaatuminen ei ole pelkästään lääketieteellisten laitteiden käyttöön liittyvä riski tai uhka, vaan vaikuttaa käytännössä kaikkiin terveydenhuollon toimintaan potilashoidosta hoidon tuki-toimintoihin. Tietoverkon riskit tiedostettiin haastateltavissa organisaatioissa yleisesti hyvällä tasolla, sillä verkon tasolla tapahtuvaa suojausta tehtiin yleisesti vahvassa yhteistyössä palveluntoimittajan kanssa.

Teknisten riskien lisäksi haastateltava 4 mainitsi myös toimitilojen turvallisuuden ja käyttäjien olevan tunnistettuja riskejä organisaatiossa. Käyttäjät ja toimitilaturvallisuus ovat

molemmat yhteydessä esimerkiksi laitteiden varastamisiin ja häviämisiin. Toisaalta tiloihin liittyy välillisesti myös sähköjakelujärjestelmät ja niiden toimivuuden takaaminen. Terveystieteiden digitalisoitumisen myötä sähköjakelujärjestelmät ovat kriittisinä tekijöinä potilashoidon toteutumisessa ja vaikuttavat myös lääketieteellisten laitteiden käyttämiseen.

Riskien vaikutukset ja toteutumiset – Haastatteluista selvisi, että monet potentiaaliset ja fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden riskit eivät olleet toteutuneet haastateltavien organisaatioissa. Yhtenä taustalla olevana syynä sille, etteivät riskit ole toteutuneet haastatelluissa organisaatioissa voi johtua myös siitä, ettei kaikkia tietoturvapoikkeamia ja siten riskien toteutumisia ole havaittu. Riskien vaikutuksista tunnistettiin suoraan potilashoittoon vaikuttavia haittoja sekä välillisesti toteutumisesta syntyviä haittoja. Yhteenveto haastateltavien päähavainnoista ja -nostoista kyberriskien vaikutuksista on koottu taulukkoon 8.

Haastateltavat kertoivat haastatteluissa, että toteutuneet riskit olivat olleet suhteellisen pieniä vaikutukseltaan. Haastateltavat kertoivat riskeistä kyberhyökkäyksien ja laitevarauksien toteutuneen joiltakin osin. Yhdessä organisaatiossa fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin oli kohdistunut kyberhyökkäys, jolla oli ollut vaikutusta laajasti laitteiden ja organisaation toimintaan. Kyberhyökkäyksen toteutumisen myötä laitteista osa ei toiminut ollenkaan ja osa toimi osittain. Laitteisiin kohdistuneeseen kyberhyökkäyksen myötä organisaatioon kohdistui taloudellista ja mainehaittaa, sillä laitteet tuli korvata uusiin tai kunnostaa, siltä osin miten oli mahdollista. Toisaalta laitteiden läpikäynti ja saastuneiden laitteiden selvitystyö mahdollisti organisaatiolle kaikkien tietoverkkoon liitettävien lääketieteellisten laitteiden listauksen tuottamisen. Läpikäynnin ja listauksen tuottamisen myötä organisaatio sai tietoonsa kaikki organisaationsa laitteet. Laitevarauksia tunnistettiin myös tapahtuneen eri organisaatioissa, mutta niiden varaudet ovat lähinnä vaikuttaneet taloudellisesti uusien laitteiden hankinnan kautta.

Riskien tapahtuessa tai potentiaalisissa tapahtumissa fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin primäärisenä vaikutuksena on laitteiden toimimattomuus. Laitteiden ollessa käyttökelvottomia myös potilashoito viivästyy ja voi aiheuttaa vakavia haittoja erityisesti kiireellisille traumapotilaille. Potilashoitosten viivästymiset tunnistettiin riskeiksi kaikissa haastateltavien organisaatioissa.

”Lääketieteellisten laitteiden osalta kyberturvallisuusriskin toteutumisen yksi merkittävimmistä seurauksista on laitteen käytön estyminen, jolloin muun muassa potilashoito viivästyy ja tiedon eheys sekä saatavuus voivat vaarantua.” – Haastateltava 1

Haastateltavan 1 mukaan esimerkiksi traumapotilaiden tai pään kuvaamista vaativissa potilastapauksissa potilashoidon viivästyminen on potilasturvallisuudelle vaarallista ja voi jopa aiheuttaa hengenvaaran. Haastateltavan 3 mukaan hoitojen viivästyminen vuoksi potilaita joudutaan siirtämään toisiin kohteisiin. Potilashoidon kiireellisten tapaus-ten lisäksi myös kiireettömien potilashoitojen jonot ja odotusajat pitenevät aiheuttavat ruuhkaa potilashoittoon.

Riskien toteutuminen voi aiheuttaa laitteiden totaalisen käyttökelvottomuuden lisäksi tietojen eheytyksen ja saatavuuden vaarantumisen sekä väärentymisen. Haastateltavan 1 mukaan kansainvälisesti lääketieteellisten laitteiden kuvien ja tulosten, esimerkiksi kuvantamisen laitteista, väärentämisistä on tullut esille. Yhtenä riskinä haastatteluissa tunnistettiin myös laitteista saatavien tietojen myyminen, leviäminen ja väärin henkilöiden hallussa pitäminen.

Primääristen vaikutusten lisäksi haastateltavat kertoivat riskien realisoitumisista voivan aiheutua brändihaittaa sekä taloudellisia menetyksiä ja kuluja. Lääketieteellisten laitteiden varastamiset aiheuttavat pääasiassa taloudellista haittaa, sillä potilasdata on pääasiassa anonymisoitua laitteissa eikä näin aiheuta välitöntä potilasturvallisuuden vaarantumista. Potilasnumero ja potilastiedot yhdistyvät vasta työasemassa, minkä ansiosta laitevarkaudet eivät pääsääntöisesti aiheuta potilastietojen vaarantumista, sillä laitteessa olevat tiedot ovat pseudonymisoituja tietoja. Taloudellisesti kyberriskien realisoituminen tarkoittaa laitteiden osalta kokonaan uuden laitteen hankkimista tai laitteen kunnostamista. Kunnostaminen ja huoltaminen voi tarkoittaa esimerkiksi ohjelmiston korjaamista. Korjaaminen voi kuitenkin olla haastavaa, jos ohjelmisto on esimerkiksi tuhoutunut tai saastunut pahasti. Brändi- ja mainehaitat luovat samaan tapaan taloudellista uhkaa laitevarkauksien rinnalla. Haastateltavan 1 mukaan brändihaittoja on käsiteltävä yhtenä merkityksellisempänä riskinä terveydenhuollon organisaatioissa, sillä potilailla on vapaus valita terveydenhuollon organisaatioista ja näin on tärkeää luoda onnistuneet potilaspolut asiakkaille.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Brändihaitat	Mainehaitta	H1
Potilasturvallisuuden vaarantuminen	Tietojen eheyden ja saatavuuden vaarantuminen	H1
	Potilashoidon viivästyminen	H1, H3
	Virheellinen potilashoito	H1
	Potilastietojen väärentäminen, myyminen ja hallussapito	H1

Taloudelliset vaikutukset	Uusien laitteiden hankkiminen ja saastu- neiden laitteiden korjaaminen	H1
	Potentiaalisten potilaiden menettäminen	H1, H3
Laitteisiin kohdistuneet vaikutukset	Laitteiden toimimattomuus	H1, H3, H4
	Laitteiden virheellinen toiminta	H1

Taulukko 7. Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden kohdistu-
vien riskien potentiaaliset vaikutukset riskien toteutuessa.

Riskienhallinta ja -prosessien käyttö organisaatiossa – Haastateltavat kertoivat ky-
berturvallisuusriskien hallinnasta omissa organisaatioissa liittyen tietoverkkoon liitettä-
viin lääketieteellisiin laitteisiin. Yhteenveto haastateltavien päähavainnoista ja -nostoista
laitteiden riskienhallinnasta ja -prosessien käytöstä on koottu taulukkoon 9. Haastatelta-
vien kertomusten perusteella riskienhallintaa toteutetaan jokaisessa organisaatiossa,
mutta toteuttamisen muodoissa ja tavoissa oli erinäisyyksiä. Haastateltavat 1 ja 2 kertoi-
vat oman organisaationsa riskienhallinnan toimivan järjestelmällisesti ja systemaattisesti
sekä lääketieteellisten laitteiden olevan osana riskienhallinnassa. Haastateltava 2 kertoi
riskienhallinnan politiikan, prosessin ja hallintamallin olemassaolosta sekä vuosikellon
mukaisesta riskienhallinnasta, jonka mukaan tehdään päivityksiä ja katselmoiteja.
Myös riskienhallintasuunnitelma oli käytössä ja vastuut ja omistajuudet määriteltäviä.
Haastateltavat 1 ja 2 kertoivat käytössä olevan riskienhallintaohjelmisto, jonka avulla voi-
daan hallita riskejä ja toteuttaa organisaation riskienhallintaa keräämällä tietoturvariskejä
esimerkiksi kyberhyökkäyksistä, laitevarkauksista, kovalevyistä.

Haastateltava 3 kertoi, ettei hänen organisaatiossaan ole käytössä formaalia riskienhal-
linnan prosesseja, mutta riskienhallintaa toteutetaan silti omien parhaiden käytäntöjen
mukaisesti ja kokemusperäisesti. Riskienhallinta näkyi haastateltavan 3 mukaan myös
riskienhallinnan ISO-standardin käytössä. Riskienhallinnasta vastuussa kerrottiin olevan
tekninen johtaja, jonka tehtävänä on ilmoittaa altistumisista ja realisoitumisista tarvitta-
essa. Lisäksi olemassa on tietoturvaryhmä, joka hallinnoi tilanteita ja tapahtumia. Haas-
tateltavan 5 organisaatiossa puolestaan tietohallinto hallinnoi riskienhallintaa ja sen to-
teutumista jollakin tavalla myös lääketieteellisten laitteiden osalta. Haastateltava 1 nosti
omassa haastattelussaan esille myös toimittajan riskienhallinnan, johon on kiinnitetty
huomiota organisaatiossa. Haastateltavan 1 mukaan toimittaja tekee sisäisesti riskien-
hallintaa, jonka malli on suunniteltu ja otettu käyttöön myös haastateltavien 1 ja 2 orga-
nisaatiossa. Haastateltavan 1 mukaan organisaatiosta voidaan pyytää nostoja erikseen
lääketieteellisistä laitteista ja niiden riskeistä.

Haastateltava 4 nosti esille, että laitetoimittajat tekevät omaa riskienhallintaa, johon sairaala ei voi vaikuttaa. Näkyvyys laitetoimittajien riskienhallintaan ja heidän laitteiden riskeihin on hyvin rajattu eivätkä haastatellut organisaatiot osanneet tarkemmin sanoa siitä. Laitetoimittajien riskienhallinta on kuitenkin merkityksellinen asia, joka liittyy organisaatioiden laitehankintoihin ja niiden riskienhallintaan sekä kolmansien osapuolien, kuten verkkotoimittajan, riskienhallinnan toimenpiteisiin. Myös haastateltava 5 näki riskienhallinnan kriittisenä ja tärkeänä asiana erityisesti hankinnoissa, joissa organisaatioiden on mahdollista vaikuttaa laitteiden turvalliseen toimintaan valitsemalla kyberturvallisuuden näkökulmasta parhain mahdollinen lääketieteellinen laite.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Organisaation riskienhallinta	Organisaatio toteuttaa riskienhallintaa.	H1, H2, H3, H5
	Organisaatiolla on olemassa riskienhallinnan politiikka.	H1, H2,
	Organisaatiossa riskienhallinnan vastuhenkilöt ja roolit on määritelty.	H1, H2
	Organisaatiolla on olemassa riskienhallinnan prosessi ja/tai toimintamalli.	H1, H2
	Organisaatiolla on olemassa riskienhallinnan suunnitelma.	H2
	Organisaatiolla on käytössä riskienhallinnan työkalu.	H1, H2
	Organisaatio tekee riskianalyyseja.	H2
	Organisaatio noudattaa parhaita käytäntöjä riskienhallinnassa.	H3

Taulukko 8. Haastateltavien organisaatioiden riskienhallintaan ja sen prosesseihin liittyvät havainnot.

Kyberriskeiltä ja -uhilta suojautuminen ja niiden huomioiminen terveydenhuollon ympäristössä. Haastatteluissa kävi ilmi, että haastateltavien organisaatioissa on huomioitu lääketieteellisten laitteiden potentiaalisten riskien mahdolliset realisoitumiset erilaisilla keinoilla. Riskeiltä on pyritty suojautumaan organisaatioissa erityisesti tietoverkon vahvistamisen keinoin, yhteistyöllä sidosryhmien kanssa ja vahvistamalla sisäisiä prosesseja. Kyberriskeiltä ja -uhilta suojautumista on tehty erityisesti yleisimpien lääketieteellisiin laitteisiin kohdistuvien uhkien toteutumisen ehkäisemiseksi. Yhteenveto haastateltavien päähavainnoista ja -nostoista kyberriskeiltä ja -uhilta suojautumiseen on koottu taulukkoon 10.

Tietoverkon puolella organisaatiot olivat kiinnittäneet huomiota kyberturvallisuusriskeihin erityisesti ja tehneet paljon suojaamista esimerkiksi eri kerroksilla ja ympäristöissä. Mo-

net haastateltavat kertoivat verkon tasolla tehtävän monipuolista suojausta ja, että tietotekniikkapuolelta on tunnistettu riskejä lääketieteellisille laitteille. Verkon kyberturvallisuustoimenpiteet koettiin haastatteluissa erityisen tärkeiksi, sillä lääketieteellisiin laitteiden suojaaminen muutoin esimerkiksi ohjelmistojen avulla on rajoitettua laitevalmistajien ja regulaation myötä. Verkon turvallisuudesta huolehtimista pidettiin haastatteluissa ensiarvoisen tärkeänä myös kyberhyökkäyksiltä suojautumiseksi esimerkiksi palvelunestohyökkäyksien suhteen.

”Verkon tasolla tehdään paljon erilaista suojausta, sillä vahva kuorikerros ja ympäristö ovat parhaimpia suojautumiskeinoja” – Haastateltava 1

Haastateltavat 1 ja 2 kertoivat haastatteluissaan, että heidän edustamassa organisaatiossa verkkotason suojaamista on tehty monitasoisesti ja tehty esimerkiksi eriyttämiä esimerkiksi aliverkoissa muun muassa työasemien, vierailijaverkon ja kuvantamisen laitteiden kesken. Kuvantamislaitteet pidettiin haastateltavien 1 ja 2 organisaatiossa eri fyysisessä tai virtuaalisessa verkossa. Haastateltavan 3 organisaatiossa toimittajilta puolestaan vaadittiin ISO-standardien mukaisia verkkojen toimitusta ja ylläpitoa. Yhteistyön merkitystä ja tarvetta korostettiin eri organisaatioiden asiantuntijahaastatteluista ja haastatteluissa koettiin, että vaikka jonkinlaista yhteistyötä tehdään, tulisi vuorovaikutusta ja kommunikointitapoja vahvistaa eri sidosryhmien kanssa myös tietotekniikkapuolen toimittajien ja palveluntuottajien kanssa.

Kaikki haastateltavat näkivät merkitykselliseksi edistää eri sidosryhmien välistä vuoropuhelua fyysisistä tietoverkkoon liitettävistä lääketieteellisistä laitteista. Haastateltavan 1 mukaan erityisesti tietohallinnon, lääkintätekniiikan ja toimittajien välistä keskustelua tulisi edistää ja vuorovaikutukseen kannustaa, jotta kaikki osapuolet tietäisivät toisistaan ja osaisivat ottaa huomioon erilaiset näkökulmat liittyen lääketieteellisten laitteiden turvalliseen käyttöön. Yhteistyön edistäminen lääkintätekniiikan, tietohallinnon ja muiden tiimien kanssa ei kuitenkaan kaikissa haastatteluissa organisaatioissa ollut itsestäänselvyys ja kehitettävää löytyi. Haastateltavan 1 mukaan kehittämistä vuorovaikutuksessa on vielä edessä, mutta hänen organisaatiossaan kommunikointi on toiminut suhteellisen hyvin lääkintätekniiikan sisältyessä tietohallintoon organisaatiokaaviossa.

”Yhteistyö tietohallinnon, lääkintätekniiikan ja toimittajien kanssa on tärkeää, jotta kaikki tietäisivät toisistaan ja meneillään olevista lääketieteellisten laitteiden hankinnoista ja muista tapahtumista.” – Haastateltava 4

Haastateltavien kesken yhteistyö eri tiimien kanssa koettiin parantavan organisaation henkilöstön osaamista ja tukee osajien verkostoitumista teeman ympärillä. Organisaation sisällä toimivien osajien lisäksi haastateltavilla organisaatioilla oli kaikilla jossakin

määrin palveluntoimittajia lääketieteellisten laitteiden toimintaympäristöön liittyen. Haastatteluista kävi ilmi, että organisaation sisäisen yhteistyön lisäksi organisaatioiden olisi tärkeää vahvistaa vuorovaikutusta ja yhteistyötä muiden sidosryhmien, kuten laitevalmistajien, palvelutoimittajien sekä tietoturvallisuusalan organisaatioiden kanssa. Haastateltava 5 kertoi organisaatiossa pyrittävän toimivaan yhteistyöhön esimerkiksi kyberturvallisuusriskien kriisiharjoitusten avulla – Haastateltavan 5 organisaatiossa oli järjestetty kokonaisvaltaisia harjoituksia, joihin osallistui organisaation eri tiimeistä asiantuntijoita ja johtoa. Harjoitusten tarkoituksena oli valmistaa organisaatiota toimimaan mahdollisen kyberturvallisuusriskin tapahtuessa. Harjoituksiin oli sisällytetty esimerkiksi roolien määrittämistä, sisäistä varautumista ja toimenpiteiden listaamista.

Haastateltujen organisaatioiden yhteistyö oli monipuolista ja toisistaan eroavia. Haastateltava 2 kertoi organisaation pyrkineen saamaan käyttöönsä parhaimpia osajia omassa ja toimittajaorganisaatiossa sekä luomalla keskustelua ja vuorovaikutusta seminaareissa, foorumeissa ja muissa yhteistyöympäristöissä myös laitteisiin liittyvistä riskeistä ja asioista, joita voisi kehittää ja parantaa. Lisäksi haastateltava 1 kertoi hänen edustamansa organisaation tehneen yhteistyötä projektin muodossa Huoltovarmuuskeskuksen kanssa lääketieteellisten laitteiden hankintaprosessin kehittämiseksi. Tämän projektin myötä organisaatiolle luotiin hankintavaatimusluettelo ja implementointisuunnitelma vaatimusluettelon prosessimaiseen käyttöön.

ICT-laitteiden toimittajille lääketieteelliset laitteet eivät ole tuttuja ja siksi vuoropuhelua yritetään ylläpitää, mutta välillä on haastavaa löytää samaa kieltä ja mitä tehdä, missä ja miten.” – Haastateltava 4

Myös hankintojen ja niiden elinkaaren hallinnan yhteydessä tapahtuva yhteistyö laitetoimittajien kanssa mainittiin yhtenä riskienhallinnallisena toimenä kyberturvallisuusriskien ja uhkien suojaamisessa. Haastateltavan 4 mukaan laitetoimittajalla on iso vastuu lääketieteellisten laitteiden kyberturvallisuuden riskien ja uhkien hallitsemiseksi, sillä toimittajat huolehtivat pääsääntöisesti laitteiden päivityksistä, palomuuureista ja muista teknisistä tietoturvatiedoista. Haastateltavan 4 mukaan turvallisuuden ylläpitäminen on siis näin laitetoimittajan vastuulla ja ohjelmistoihin ei pystytä vaikuttamaan terveydenhuollon organisaatioissa. Sopimuksellisesta näkökulmasta katsottuna kuitenkin terveydenhuollon organisaatiot hallinnoivat laitteita ja ovat niistä vastuussa. Haastateltavan 3 organisaatiossa hankinnan yhteydessä käydään keskustelua kyberturvallisuudesta toimittajien kanssa. Lisäksi organisaatiolla oli olemassa tietoturvaliite ja toimittajan tuli täyttää vaatimusliite.

Hankintojen osalta haastateltavan 1 organisaatiossa oli tehty yhteistyötä lääketieteellisten laitteiden hankintaprosessin kehittämiseksi yhdessä tietoverkko- ja tietoturvallisuuspalvelujen toimittajan ja Huoltovarmuuskeskuksen kanssa. Lisäksi hankinnoissa sekä tietohallinto, että lääkintäteknikka toimivat yhdessä hankintojen yhteydessä haastateltavan 1 mukaan. Haastateltavan 5 organisaatiossa hyödynnetään suunnitteluvaiheessa olemassa olevaa työryhmää, joka miettii laitehankintojen näkökulmasta, miten kyberturvallisuusuhkia tulisi huomioida kilpailutuksissa ja hankinnoissa. Kilpailutus tehdään asiantuntijaryhmän avustuksella, jossa on monialaista osaamista lääkintäteknikasta, käyttäjäistä, laista, tietoturvasta ja -suojasta sekä tietohallinnosta. Monipuolisten osaajien avulla kilpailutuksessa voidaan ottaa huomioon kokonaisvaltaisesti lääketieteellisiin laitteisiin liittyviä uhkia ja riskejä. Haastateltava 3 kertoi, että tulevaisuudessa tulisi ottaa huomioon koko lääketieteellisten laitteiden elinkaarissa tietoturvallisuuden näkökulma sekä toimittajien ja ylläpidon kyvykkyydet. Haastateltavan 3 mukaan tällä hetkellä huomiointia on tapahtunut pääasiassa vain pelkässä hankinnassa.

Haastateltava 1 kertoi myös yhteistöistä, joihin hänen työnantajaorganisaationsa oli osallistunut yhtenä terveydenhuollon organisaatioista. Yhteistyötä oli tehty siis muiden terveydenhuollon organisaatioiden kesken. Haastateltava 1 kertoi, että hänen organisaationsa oli myös vertaillut omaa toimintaansa alan toisten organisaatioiden toimiin ja parhaisiin vastaaviin käytäntöihin. Haastateltavan 1 mukaan hänen organisaationsa sai varmuutta vertailusta siihen, että he toimivat kohtuullisen hyvin ja tietoturvallisesti ja toisaalta, että muissa organisaatioissa toiminta ei välttämättä ole yhtä systemaattista ja parhaisiin käytäntöihin nojaavaa.

Organisaatioiden sisäiset prosessit ja suunnitelmat nähtiin yhtenä riskienhallinnallisena toimenpiteenä ja uhilta suojautumisen keinona. Haastateltavan 3 organisaatiossa riskien realisoitumiset olivat opettaneet organisaatiota mahdollisista lääketieteellisten laitteiden riskeistä, sekä mitä muuta niihin saattaa liittyä, miten riskejä tulisi kartoittaa ja mitä tulisi tehdä. Vaikka kehitystä haastateltavan 3 mukaan oli tapahtunut sisäisissä toimintatavoissa ja suunnitelmissa, olisi hänen mukaansa silti tarpeen kehittää erityisesti ohjeituksia tilanteisiin, joissa kyberturvallisuusriskit tai -uhat toteutuvat. Riskeiltä suojautumisessa merkityksellisessä roolissa nähtiin myös jatkuva kehittäminen ja kehittyminen sekä uusien työkalujen ja tekniikoiden hyödyntäminen. Haastateltava 2 kertoi haastattelussaan, että organisaatiossa on mietitty työkalujen kautta kyberuhkia ja -riskejä ja siten kehitetty työkaluja tietoturvallisemmaksi esimerkiksi tietoturva-arviointien avulla.

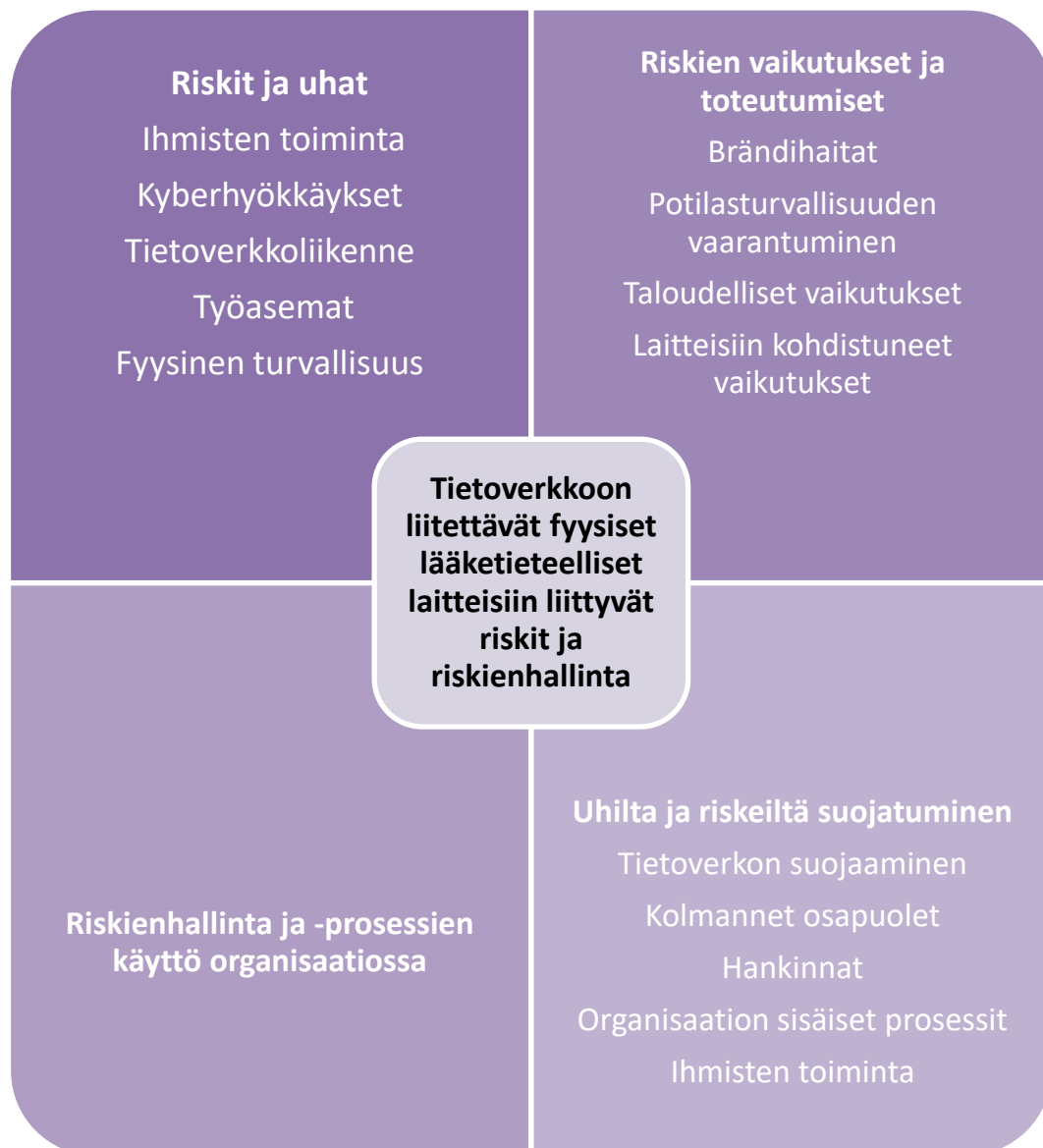
Lisäksi haastateltava 3 kertoi, että tunnistetuista kyberturvallisuusriskeistä on tunnistettu myös ihmisiin ja käyttäjiin liittyviä riskejä ja uhkia. Haastateltavan 3 mukaan yksi isoim-

mista uhista ovat käyttäjälähtöiset riskit yhdessä verkon kautta tuleviin riskeihin. Haasteena käyttäjälähtöisissä riskeissä on ihmisten vääränlainen toiminta, joka vaarantaa lääketieteellisten laitteiden kyberturvallisuutta. Haastateltavan 3 esimerkkinä käyttäjälähtöisistä riskeistä on USB-tikun käyttö, jota ei sallita organisaatiossa, mutta jota käyttäjät voivat potentiaalisesti käyttää laitteissa ja niiden työasemissa. Käyttäjälähtöisiin riskeihin haastateltava 3 näki parhaimpana riskienhallinnallisena toimenpiteenä käyttäjien koulutuksen, jolla vääränlaiseen toimintaan voitaisiin puuttua ja opettaa ihmisiä tietoturvallisista käytännöistä organisaatiossa.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Tietoverkon suojaaminen	Verkon turvakontrollit ja tekniset suojaukset sekä eriyttämiset	H1, H2
	Työkalujen ja ohjelmien käyttäminen, analytiikka	H2
	ISO-standardoitu verkon toimitus ja ylläpito	H3
	Organisaation sisäinen ja verkon toimittajien välinen yhteistyö ja vuorovaikutus	H1, H2
Kolmannet osapuolet	Palveluntarjoajien kanssa tehtävä yhteistyö ja vuorovaikutus	H1, H3
	Muiden kolmansien osapuolien kanssa tehtävä yhteistyö ja vuorovaikutus	H1
	Terveystieteiden organisaatioiden välinen yhteistyö ja vuorovaikutus	H1
Hankinnat	Hankintaprosessin ylläpitäminen ja kehittäminen	H1, H3, H5
	Vastuullisen ja tietoturvan vaatimukseen vastaavan toimittajan valinta	H1, H3, H4, H5
	Vaatimuslistan ylläpitäminen	H1
	Tietoturvaliitteen ja sen vaatimusten luominen	H1, H2, H3, H4, H5
	Hankinnan kanssa tehtävä yhteistyö ja vuorovaikutus	H1, H2, H3, H4, H5
	Organisaation sisäinen laitehankintojen työryhmä ja yhteistyö yksiköiden välillä	H1, H3, H4, H5
Organisaation prosessit	Organisaation sisäisten prosessien, mallien ja suunnitelmien käyttäminen	H1, H3
	Jatkuva kehitys ja suunnitelmien ylläpito ja päivitys	H3
	Harjoitukset	H5
Ihmisten toiminta	Tietoturvakoulutukset	H3

Taulukko 9. Haastateltavien päähavainnot ja -havainnot kyberriskeiltä ja -uhilta suojaamiseen.

Yhteenveto tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden riskeistä ja riskienhallinnan tavoista haastatelluissa organisaatioissa – Haastattelujen perusteella haastateltavat tunnistivat edustamissaan organisaatioissa samankaltaisia tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden riskejä ja uhkia. Haastattelujen päähavainnot eri alateemoista riskienhallintaan ja riskeihin on koottuna kuvaan 3. Mahdollisia laitteiden riskejä ja uhkia tunnistettiin liittyvän pääasiallisesti ihmisten toimintaan, kyberhyökkäyksiin, tietoverkkoihin ja työasemiin, sekä fyysiseen turvallisuuteen. Haastateltavat kuvasivat riskien ja uhkien vaikutusten koskettavan erityisesti potilashoitoa viivästymisillä ja tietojen eheyden ja saatavuuden vaarantumisella. Lisäksi haastateltavat kuvasivat potentiaalisten riskien toteutumisella olevan negatiivista vaikutusta organisaatioiden talouteen ja maineeseen.



Kuva 3. Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteisiin liittyvät riskit ja riskienhallinta.

Riskienhallinnan osalta haastateltavissa organisaatioissa prosessien ja suunnitelmien käyttö ja toimintatavat vaihtelivat organisaatioittain. Kaikissa organisaatioissa riskienhallintaa tehtiin jollakin tasolla, mutta systemaattisuus, kokonaisvaltaisuus ja tavat vaihtelivat riippuen organisaatiosta. Kyberriskeiltä suojautumista toteutettiin organisaatioissa pääasiallisesti teknisillä tavoilla ja tietoverkkoa vahvistamalla, mutta organisaatiot toivat esille myös yhteistyön toimittajien, hankinnan ja organisaation sisäisten yksiköiden kanssa, sekä prosessien ja sovitujen toimintatapojen merkityksellisyyden suojautumisen näkökulmasta.

5.2 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arviointi, valvonta ja hallinta

Laitteiden turvallisuuden arviointi ja validointi - Haastattelujen perusteella tietoverkkoon liitettävien lääketieteellisten laitteiden turvallisuuden arvioinnit ja validoinnit sekä tietoturvatestaamiset tapahtuvat pääasiallisesti lääketieteellisten laitteiden elinkaaren hankintavaiheessa. Hankintavaiheessa käyttäjäorganisaatiot suorittavat käyttöönotot ja laitteiden tarvittavat testaukset. Kaikki organisaatiot toteuttivat jonkinlaista tietoturva-arviointien tekemistä, mutta niiden välillä oli eroja erityisesti testausten määrässä, laadussa ja tyypeissä sekä siinä, missä kohtaa laitteiden elinkaarta arviointeja ja validointeja tehtiin. Yhteenvedo haastateltavien päähavainnoista ja -nostoista laitteiden turvallisuuden arvioinnista ja validoinnista on koottu taulukkoon 11.

Haastateltavan 1 ja 2 organisaatiossa kerrottiin hankintaprosessin sisältävän turvallisuuden arviointia. Haastateltava 1 kertoi haastattelussaan, että hankintaprosessi käynnistyy potilashoidosta tulevasta kliinisestä määrittelystä ja tarpeesta, jonka jälkeen lääkintätekniikan asiantuntijat tuottavat vaatimuksia teknisistä ja huoltoon liittyvistä tarpeista. Samalla tuotetaan vaatimuksia tietosuojaan ja -turvaan liittyen, joista on olemassa omat liitteet ja kokonaisuudet hankinnan määrittelyvaiheeseen. Haastateltava 1 kertoi hankintojen jatkuvan kilpailutuksesta tarjouksiin ja sen jälkeen vaatimusten täyttymisten katselmointiin, jonka jälkeen muutoshallintaprosessissa tulee hyväksyä verkkoon liitettävät laitteistot ja laitteet. Mikäli tarpeellista on, niin verkkoon liitettävien vaatimusten arvioimiseksi voidaan hankintaa käyttää teknisen tietoturvan erikoisasiantuntijoiden arviointitehtäviä. Arviointi suoritetaan pisteyttävällä riskiarvioinnilla ja mikäli pistemäärä on liian suuri riskiarvioinnissa, niin laitteelle on tehtävä erityistoimenpiteitä kuten esimerkiksi oma verkko. Haastateltava 1 kertoi, että hankinnan jälkeen tietoturvallisuuden näkökulmasta tehtävää tarkastelua tehdään vielä ennen käyttöönottoa.

Hankinnan yhteydessä organisaatioissa, tyypillisesti asennusvaiheessa, suoritettiin tietoturva-arviointeja, -testauksia ja verkon kovennuksia. Haastateltavan 3 organisaatiossa

tietoturva-arvioiteja tehtiin hankintojen yhteydessä ja asennusvaiheessa, jossa suoritetaan verkon kovennusta. Haastateltava 1 kertoi organisaatiossa tehtävän käyttöönoton aikana integraatioiden yhteydessä viimeisiä tietoturvakäytäntöjen arvioimista esimerkiksi salasanaikäytäntöjen kautta. Käyttöönoton jälkeiset tietoturvatestaustavat ja -tottumukset puolestaan vaihtelivat organisaatioittain.

Haastateltavan 2 haastattelussa tuli esille, että hänen edustamassaan organisaatiossa tietoturvatestausta tehtiin kokonaisvaltaisesti käyttäen palveluntarjoajia ja muita sidosryhmiä oman organisaation resurssien lisäksi. Haastateltavan 2 organisaatiossa oli tunnistettu ulkoverkon olevan riski suuren rajapintansa vuoksi ja siksi palveluntarjoajaa oli hyödynnetty ulkoverkon skannauksien osalta sekä penetraatiotestauksissa. Sisäverkon skannauksia oli organisaatiossa tehty harvemmin kokonaisvaltaisesti kaikkien yhteyksien läpikäymiseksi tietoliikenneverkossa. Verkon skannauksien ja penetraatiotestauksien lisäksi verkon turvallisuuteen liittyviä muita testauksia sekä potilastietojärjestelmien testauksia oli tehty. Lisäksi haastateltavan 2 organisaatiossa oli erikseen olemassa testiverkko ja ympäristö tietoverkkoon liitettävälle lääketieteellisille laitteille. Muissa organisaatioissa testaukset suoritettiin käytännössä vain laitteiden käyttöönottojen yhteydessä. Haastateltavan 3 ja 4 organisaatiossa puolestaan laitteiden testauksia ei ollut tehty käyttövaiheen yhteydessä.

Laitetoimittajalla on iso vastuu huolehtia lääketieteellisen laitteen turvallisuudesta vaatimuksiin vastaamisella, sekä laitteiden huollon ja päivittämisten osalta. Haastateltava 5 kertoi, että laitevalmistajien tietoihin on luotettava turvallisuustiedoista. Haastateltava 4 kertoi puolestaan, että laitetoimittajan tulee huolehtia ja huolehtii laitteiden turvallisuudesta. Hänen mukaansa huoltoja ja muita päivityksiä laitteisiin tehdään vain, jos laitetoimittaja näin käskää tai vaatii. Haastateltavan 5 mukaan laitevalmistajilta vaaditaan sertifikaatteja ja mahdollisia lausuntoja hankinnassa, mikäli laitevalmistajilla ei ole haluttuja sertifikaatteja. Näillä valmistajan sertifikaateilla voidaan hankintojen yhteydessä validoida laitevalmistajaa ja sen lääketieteellisten laitteiden turvallisuutta. Haastateltava 1 oli samoilla linjoilla haastateltavan 5 kanssa sertifikaateista ja siitä, että organisaation tulee pystyä luottamaan laitevalmistajien antamiin sertifikaattitietoihin ja että ne täyttävät vaatimukset. Haastateltavan 5 haastattelun mukaan sertifikaattien puuttuminen ei välttämättä estä laitteiden ostoa, sillä laitevalmistajilla on paljon vaatimuksia ennen markkinoille pääsyä, joilla voidaan turvata lääketieteellisten laitteiden turvallisuutta.

”Laitevalmistajien antamiin tietoihin ja sertifikaatteihin on luotettava.” – Haastateltava 5

Haastateltavan 5 mukaan laitevalmistajien sertifikaatteihin ja muihin antamiin tietoihin on pystyttävä luottamaan, sillä terveydenhuollon organisaatioilla ei ole käytännössä muuta vaihtoehtoa. Laitevalmistajien tietojen erilliset todentamiset toisivat prosessiin hidasteita, eikä organisaatioilla ole aikaresursseja haastaa valmistajien antamien tietojen oikeellisuutta. Haastateltavan 5 mukaan terveydenhuollon organisaatiolla ei ole halua eikä käytännössä mahdollisuutta lähteä kyseenalaistamaan laitevalmistajien antamia tietoja, sillä se voisi haitata terveydenhuollon organisaatioiden toimintaa.

”Laitevalmistajien tietoihin luotetaan – sellaista muurahaispesää ei edes uskalla lähteä sohimaan.” – Haastateltava 3

Haastateltava 3 toi myös esille, ettei resurssien käyttämisen lisäksi laitevalmistajien tietoja uskalleta kyseenalaistaa. Haastateltavan 3 mukaan laitteita hankitaan noin 3000 laitetta joka vuosi lisää ja siksi olisikin haastavaa, mikäli laitevalmistajien laitteita ei pystyttäisikään hankkimaan. Hankinnat ovat merkittävä osa lääketieteellisten laitteiden hallintointia ja siksi on tärkeää, että laitevalmistajat pystyvät toimittamaan organisaatioiden vaatimuksia täyttäviä lääketieteellisiä laitteita sovitun mukaisesti.

Haastatteluissa oli eroja yhteistyössä palveluntarjoajien kanssa, sillä osa piti aktiivista kommunikointia ja vuorovaikutusta laitevalmistajien ja verkon toimittajien kanssa, kun taas osalla ei ollut tietämystä mitä palveluntarjoaja tarkalleen tekee ja on huolehtinut tietoturvaan liittyvistä asioista. Haastateltava 3 kertoi haastattelussaan, että palvelutoimittajiin on pystyttävä luottamaan. Hänen mukaansa isoissa versiopäivityksissä luotetaan toimittajan etäyhteyksien verkkoihin eikä niiden turvallisuutta uskalleta kyseenalaista. Samasta organisaatiosta haastateltavan 3 kanssa haastateltava 4 kertoi organisaatiolla olevan huono näkymä verkon palveluntarjoajan tekemiseen – haastateltava ei osannut sanoa oliko palveluntarjoaja tehnyt turvallisuuden arviointia tai validointia heidän toimittamalleen verkolle, joka liittyy myös tietoverkkoon liitettävien lääketieteellisten laitteiden verkon turvallisuuteen. Huono näkyvyys palveluntarjoajien tekemiseen voi johtua osittain myös haastateltavien huonosta näkyvyydestä ja siitä, ettei heillä ollut tarkempaa tietoa palveluntarjoajiin. Haastateltavan 3 organisaatiossa oli tunnistettu puolestaan toimittajien auditointien tarve, joka kattaisi myös turvallisuuden validointia ja arviointia lääketieteellisten laitteidenkin suhteen. Suunnitelmissa oli aloittaa auditoimaan toimittajia kahdesti vuodessa, mutta tämä oli vasta suunnitelmissa eikä auditointeja ollut toteutettu.

Haastateltavista organisaatioista haastateltavien 1 ja 2 edustamassa organisaatiosta nostettiin esille myös lääketieteellisiin laitteisiin liittyvää tietoturvan kehittämistä hankintojen ja laitteiden tietoturvatarkastukseen liittyen. Haastateltava 1 kertoi, että hänen edus-

tamansa organisaatio oli tehnyt tietoverkkoon liitettävän fyysisen lääketieteellisen laitteen liittyvän arvion yhteistyössä yliopiston kanssa. Yhteistyötapahtumassa lääketieteellistä laitetta oli päästy häiritsemään ja sotkemaan, joka osoittautui haastateltavan 1 mukaan yllättävänkin helposti. Yhteistyöstä organisaatiolle selvisi ja varmistui, että lääkintälaitte itsessään on hyvin haavoittuvainen ja siksi verkon suojaaminen on tärkeää ja merkityksellistä. Mikäli kyberhyökkääjät pääsisivät verkon sisälle ja koputtelemaan laitteiden portteja, niin sen jälkeen laitteeseen tunkeutuminen on helppoa ja hyvinkin nopeasti mahdollista.

”Tietoverkkoon liitettävä fyysinen lääketieteellinen laite on itsessään haavoittuva ja siksi verkon suojaaminen on erityisen tärkeää.” – Haastateltava 1

Haastateltavan 1 organisaatiossa nähdään lääketieteellisen laitteen olevan itsessään hyvin haavoittuva. Tämän vuoksi haastateltavan 1 mukaan lääketieteellisiä laitteita on pystyttävä suojaamaan käyttäjäorganisaation mahdollisilla keinoilla. Haastateltavan 1 organisaatiossa lääketieteellisten laitteiden haavoittuvaisuus on otettu huomioon teknisillä tietoturvatkaisuilla ja -palveluilla sekä esimerkiksi verkon suojaamisen kautta.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Hankinta, asennus ja käyttöönotto	Turvallisuusarviointi	H1, H2, H3, H4, H5
	Hankintoihin liittyvän tietoturvan työryhmän käyttäminen	H1, H2, H3, H4, H5
	Erikoisasiantuntijoiden käyttö	H1, H2
	Laitteiden testaukset ja ympäristöjen rakentaminen	H1, H2, H3, H4, H5
Käyttövaihe	Ulkoverkon skannaukset ja/tai penetraatiotestaukset	H1, H2
	Sisäverkon testaukset	H1, H2
	Kriittisten järjestelmien testaukset	H1, H2
	Laitteiden testaukset	H1, H2
	Kokonaisvaltainen tietoturvatestaaminen	H1, H2
Laitetoimittaja	Sertifikaatit	H1, H3, H4, H5
	Laitteiden vaatimukset ja turvallisuustiedot	H1, H3, H4, H5
Palveluntoimittajat ja muut kolmannet osapuolet	Yhteistyö, vuorovaikutus ja läpinäkyvyys toimittajien tuottamiin palveluihin	H1, H2
	Yhteistyö ja vuorovaikutus kehitystyön tekemiseksi kolmansien osapuolien kanssa	H1, H2
	Toimittajien auditointi ja validointi	H3* (suunniteltu)

Taulukko 10. Haastateltavien päähavainnot ja -nostot laitteiden turvallisuuden arviointitavoista ja -käytännöistä.

Haavoittuvuuksien hallinta laitteiden elinkaaren aikana – Lääketieteellisten laitteiden haavoittuvuuksien hallinta koostuu pääasiassa käytön aikana laitevalmistajan ja -toimitajan päivityksistä sekä käyttäjäorganisaatioiden osalta työasemien ja joidenkin lääketieteellisten laitteiden haavoittuvuuksien hallintatoimista. Haastatteluista selvisi, että haavoittuvuuksien hallinnalliset toimet ja prosessit vaihtelevat organisaatioittain. Kaikissa haastatelluissa organisaatioissa kolmannet osapuolet olivat vahvasti mukana haavoittuvuuksien hallinnassa riippuen organisaation ostamista palveluista. Yhteenveto haastateltavien päähavainnoista ja -nostoista laitteiden haavoittuvuuksien hallinnasta koko elinkaaren ajalta on koottu taulukkoon 12.

Haastatteluista kävi ilmi, että lääketieteellisten laitteiden haavoittuvuuksien hallinnassa laitevalmistajilla ja -toimittajilla on merkityksellinen rooli laitteiden käytön aikana. Haastatteluista selvisi, että organisaatiot eivät pysty tekemään päivityksiä itsenäisesti laitteisiin ja siksi laitevalmistajien haavoittuvuuksien hallinnan ajantasaisuus ja yhteistyö kyberturvallisuustahojen kanssa on merkityksellistä laitteiden haavoittuvuuksien mahdollisimman nopeaan reagoimiseen. Laitevalmistajat määrittävät, miten laitteita päivitetään ja kuinka usein päivityksiä tehdään. Haastateltavan 4 mukaan laitevalmistajat lähettävät tiedon, kun lääketieteelliseen laitteeseen tai laitejoukkoon halutaan asentaa päivityksiä. Päivitystarpeiden kommunikointi tapahtuu siis laitetoimittajalta tai -valmistajalta terveydenhuollon organisaatioon päin. Valmistajan määrittämistä päivitystarpeista riippuen terveydenhuollon organisaatiot toimivat päivitysmääritysten mukaisesti joko niin, että laitetoimittaja tuottaa päivityksen esimerkiksi etäyhteydellä tai paikan päällä tai organisaatio tekee yhteistyössä palveluntarjoajan kanssa päivitykset.

”Perustoimintojen päivitysvaatimukset tulevat lain velvoittamana laitetoimittajille ja sen lisäksi tietoturvan yleiset verkon ja Microsoftin päivitykset pyörivät omien syklien mukaan.” – Haastateltava 1

Haavoittuvuuksien hallinnasta ja muista vastuista ja rooleista sovitaan palveluntoimittajan kanssa sopimuksissa, joissa määritellään vastuut tiettyjen laitteiden tai laitetyyppien haavoittuvuuksista ja päivityksistä. Haastateltavan 1 mukaan perustoimintojen päivitysvaatimukset tulevat lain kautta valmistajille. Haastateltava 1 kertoi haastattelussaan, ettei laitteistoihin tule monia päivityksiä laitteen elinaikana, kun sitä käytetään. Laitetoimittajien päivitysten lisäksi yleiset tietoturvapäivitykset pyörivät käyttäjäorganisaation omien syklien mukaan. Haastateltavan 4 mukaan laitteiden käyttöaika on laitteesta riippuen noin 6-12 vuotta. Haastateltavan 4 organisaatiossa laitetoimittajat ja -valmistajat

kommunikoivat organisaatioon, mikäli laitteisiin on noussut kohdistuneita uhkia tai haavoittuvuuksia löydetty. Tämän jälkeen laitevalmistajat voivat joko itse toteuttaa päivitykset esimerkiksi etäyhteydellä tai huoltotapahtumissa, tai terveydenhuollon organisaatiot huolehtivat haavoittuvuuksien korjauksista itsenäisesti tai yhteistyössä palveluntarjoajien kanssa.

Haastateltavat kertoivat organisaatioilla olevan käytössä palveluntarjoajilta SOC (Security Operations Center) eli tietoturvapalvelukeskuksen palveluita, joihin kuului haastatelluilla organisaatioilla myös muun muassa haavoittuvuuksien koordinoitua. Näiden SOC-palveluiden avulla haastateltava 2 kertoi hänen edustamansa organisaation pystyvän hallitsemaan haavoittuvuuksia ja sieltä tulevia hälytyksiä myös liittyen lääketieteellisiin laitteisiin. Haastateltava 2 kertoi, että mikäli valmistaja havaitsee haavoittuvuuden lääketieteellisessä laitteessa, niin siitä ilmoitetaan eteenpäin ja SOC voi katsoa koskettaako haavoittuvuus haastateltavan organisaatiota. Tämän jälkeen haavoittuvuudesta voidaan pitää palavereja ja keskusteluja, kuinka haavoittuvuutta hoidetaan.

Haastateltavissa organisaatioissa tehtiin myös organisaatioiden sisällä omaa haavoittuvuuksien hallintaa lääketieteellisiin laitteisiin. Haastateltavan 1 organisaatiossa on joihinkin lääketieteellisiin laitteisiin, kuten kuvantamislaitteisiin, pystytty liittämään haittaohjelmistojen ja virusten torjuntakomponentteja. Lääketieteellisten laitteiden lisäksi niihin liitettyihin työasemiin on voitu asentaa organisaation sisäisesti tarvittavia tietoturvaohjelmia ja päivityksiä. Haastateltava 1 kertoi esimerkiksi, että kuvantamislaitteisiin on pystytty liittämään tietoturvaohjelmien komponentteja, mutta taas esimerkiksi ultraäänilaitteisiin ei itsessään ole ollut mahdollista näin tehdä, mutta siihen liitettyyn työasemaan on voitu asentaa muun muassa virustentorjuntakomponentteja. Haastatelluissa organisaatioissa työasemien ja muita tietoturvan haavoittuvuuksien hallintaa suoritettiin erilain tavoin ja keinoin. Haastateltava 2 kertoi hänen edustamansa organisaation huolehtivat työasemien haavoittuvuuksien hallinnasta esimerkiksi Microsoftin haavoittuvuuksien korjaustiedostoilla, joita Microsoft julkaisee säännöllisesti käyttöjärjestelmälle ja ohjelmille. Haastateltavan 1 mukaan myös verkon valvonta on merkityksellisessä asemassa haavoittuvuuksien hallintaa, sillä verkkoliikenteen poikkeamat voivat paljastaa lääketieteellisiinkin laitteisiin kohdistuvia kyberhyökkäyksiä.

Haastattelussa selvisi, että laitevalmistajat ja -toimittajat tekevät myös turvallisuustiedotteita organisaatioille. Haastateltavan 4 mukaan turvallisuustiedotteet käsittelevät kuitenkin yleisesti käyttöön liittyvää turvallisuutta eivätkä kyberturvallisuuden näkökulmasta laitteiden käyttöä. Haastateltava 5 kertoi tiedotteita tulevan tietoturvaan liittyen laitevalmistajilta, jos mahdollisia uhkia on ollut lääketieteellisiin laitteisiin liittyen. Tiedotteiden vastaanottamisen jälkeen organisaatiossa vastuussa on tietohallinto, jonka tehtävänä on

huolehtia, että käytössä ovat ajankohtaiset ja päivitetyt suojausmekanismit uhkien torjumiseen. Laitevalmistajien tiedotusten lisäksi uhkakuvaa seurataan viranomaisten lähdemateriaaleista. Haastateltava 5 mainitsi myös mahdollisten haavoittuvuuksien havaitsemisesta tiedon kulkevan nopeasti Suomen sisäisesti verkostojen kautta, jotka haastateltavan mukaan toimivat hyvin asiantuntijoiden tuntiessa toisensa ammatillisesta näkökulmasta.

”Laitteita on paljon ja erilaisia, jolloin kehitystyötä tarvitaan jatkuvasti.” – **Haastateltava 2**

Haavoittuvuuksien hallintaan liittyen haastateltavat peräänkuuluttivat yhteistyötä palvelutoimittajien ja laitevalmistajien kanssa. Haastateltava 2 kertoi haastattelussaan, että lääketieteellisiä laitteita on paljon ja erilaisia, jolloin kehitystyötä tarvitaan jatkuvasti. Haastateltavan 2 mukaan hänen edustamassaan organisaatiossa yhteistyötä ja kehitystyötä on pyritty luomaan esimerkiksi palveluntoimittajien kanssa pidettävillä uhkapalaverieilla, joissa yhtenä keskustelun aiheena on muun muassa haavoittuvuuksien hallinta.

Haastateltavien haavaintojen teemat	Haastateltavien päähavainnot	Maininnat
Haavoittuvuuksien hallinta	Laitetoimittajien päivitykset	H1, H2, H3, H4, H5
	Turvallisuustiedotteet laitevalmistajalta	H4, H5
	Verkon valvonta ja haavoittuvuuksien hallinta	H1, H2, H3, H4, H5
	Työasemien päivitykset	H1, H2, H3, H4, H5
	Laitteiden omat tietoturvakomponentit	H1
	Haavoittuvuuksien hallinta palveluntoimittajalta tai yhteistyössä palveluntoimittajan kanssa	H1, H2, H3, H4, H5
	Kehitystyö	H2
	Viranomaisten tuottamat tilannekuvat ja -raportit	H5
	Kansallisen asiantuntijaverkoston yhteistyö ja vuorovaikutus	H5

Taulukko 11. Haastateltavien päähavainnot ja -nostot haavoittuvuuksien hallinnasta.

Lääketieteellisten laitteiden pääsynhallinta ja -valvonta – Haastatteluista selvisi, että haastateltavien organisaatioissa tietoverkkoon liitettävien lääketieteellisten fyysisten laitteiden pääsynhallintaa valvotaan ja kontrolloidaan pääasiallisesti laitteiden kirjautumisten ja etäyhteyksien käytön hallinnalla sekä fyysisen toimitilaturvallisuuden avulla. Haastatteluiden perusteella kaikki organisaatiot hallinnoivat lääketieteellisten laitteiden pääsynhallintaa, mutta toimintatavat ja -keinot sekä hallintatasot poikkesivat toisistaan.

Haastateltavat kertoivat tietoverkkoon liitettävien lääketieteellisten laitteiden pääsynhallintaa kehitettävän pääasiassa riski- ja tietoturva-arviointien kautta. Haastatteluista ilmeni myös, että uudemmat lääketieteelliset laitteet ovat pääsääntöisesti tietoturvallisempia ja niissä myös pääsynhallinta on kehittyneempää. Yhteenveto haastateltavien päähavainnoista ja -nostoista laitteiden pääsynhallinnasta ja -valvonnasta on koottu taulukkoon 13.

Tietoverkkoon liitettävien lääketieteellisten laitteiden osalta pääsynhallinnassa on otettava huomioon etäyhteydet, joiden kautta laitteet ovat yhteydessä tietoverkkoihin. Haastateltavan 4 organisaatiossa tietoverkkoon liitettävien lääketieteellisten laitteiden osalta laitetoimittaja ja verkon tarjoaja loivat laitteisiin putken, joka on määritelty turvallisesti ja vaatimuksien mukaiseksi. Haastateltavan 1 organisaatiossa etäyhteydet olivat tehty käyttäjäorganisaation vaatimusten mukaisesti ja ennestään tuntemattomat etäyhteydet sallittiin erikseen.

”Etäyhteydet ovat luotu ja ovat olemassa organisaation vaatimusten mukaisesti – kuitenkin kaikki laitevalmistajat eivät pysty toteuttamaan vaatimuksia.” – Haastateltava 1

Haastateltava 1 kertoi haastattelussaan, että haasteita tuottavat lääketieteelliset laitteet, jotka eivät täytä yhteyksien vaatimuksia, jotka organisaatiossa on tehty lääketieteellisille laitteille. Haastateltava 1 koki hänen organisaatiossaan kriteerien olevan jopa niin tiukat, että todellisena ongelmana on laitevalmistajien kyvyttömyys toteuttaa organisaation määrittämiä vaatimuksia pääsynhallinnassa. Laitevaatimusten lisäksi haastateltava 1 kertoi organisaation tavasta tunnistaa etäyhteyksiä. Jos organisaatio tunnistaa etäyhteyden olevan tuttu, niin kerran tehty hyväksyntä riitti yhteyden käyttämiseen. Haastateltavan 3 organisaatioissa toimittajat ottivat yhteyttä etäyhteysportaalin kautta, jotka vaativat käyttäjän luvan hyväksymisen kohteeseen. Haastateltava 2 mainitsi tietoverkkoihin liityen, etteivät lääketieteelliset laitteet saaneet olla yhteydessä avoimeen internettiin. Yhteyksien osalta haastateltava 4 kertoi, etteivät käyttäjäorganisaatiot valvo etäyhteyksiä vaan valvominen on palveluntarjoajan vastuulla. Yhteyksien ja verkkojen valvomisesta voidaan saada dataa ja tehdä tarvittavia korjaustoimenpiteitä sen perusteella.

”Lääketieteellisten laitteiden pääsynhallintaa pohditaan laitteiden kriittisyyden kautta, joita voidaan arvioida esimerkiksi riskien ja tietoturva-arviointien avulla.” – Haastateltava 2

Erityyppisten lääketieteellisten laitteiden osalta pääsynhallintaa tehdään haastattelujen perusteella erilaisin keinoin. Haastateltavan 2 mukaan lääketieteellisten laitteiden pääsynhallinta ja -valvonta perustuu laitteiden kriittisyyteen. Laitteiden kriittisyyttä pystytään

haastateltavan 2 edustamassa organisaatiossa arvioida muun muassa tietoturva-arviointien ja riskien kartoitusten avulla. Haastateltavan 2 mukaan uudemmissa lääketieteellisissä laitteissa pääsynhallinta on otettu paremmin huomioon ja käyttöä voidaan hallita tietoturvasemminkin. Koska laitteissa pääsynhallintakeinot ovat erilaisia, haastateltavan 2 organisaatiossa pääsynhallintaa pohdittiin laitteen kriittisyyden perusteella pohjautuen tietoturva- ja riskiarviointeihin.

Haastateltavan 2 organisaatioissa lääketieteellisissä laitteissa kirjautuminen tapahtui pääsääntöisesti tavallisessa käytössä henkilökohtaisilla tai yhteisillä tunnuksilla sekä käytön hallinnan osalta admin-tunnuksilla. Henkilökohtaisia tunnuksia pyrittiin käyttämään aina, kun laitteessa on kirjautumismahdollisuus, jotta pääsynhallinnan ja lokienhallinnan osalta tiedot tapahtuisivat ja tallentuisivat oikein. Haastateltava 4 kertoi laitteista riippuen olevan jonkinlainen salasanaikäytäntö pääsynhallitsemiseksi – joissakin laitteissa käytössä oli käyttäjäkohtaiset tunnukset ja salasanat, ja toisissa laitteissa admin-käyttäjätunnukset yhteiskäyttöön. Myös haastateltavan 2 mukaan oli kuitenkin olemassa käyttötapauksia, joissa yhteiskäyttötunnuksia tarvitaan monien käyttäjien yhteiseen käyttöön. Molempien haastateltavien organisaatioissa pääsynhallinnan näkökulmasta on pyritty valitsemaan aina henkilökohtaiset käyttäjätunnukset yhteiskäyttäjätunusten tai vapaan käytön sijasta, mutta aina tunnistautuminen käyttäjäkohtaisesti ei ole mahdollista etenkin vanhemmissa lääketieteellisissä laitteissa.

Lääketieteellisten laitteiden teknisten pääsynhallinnan kontrollien ja valvonnan ominaisuuksien lisäksi laitteiden pääsynhallintaa voidaan valvoa fyysisellä turvallisuudella. Kaikissa organisaatioissa fyysinen turvallisuus koettiin merkitykselliseksi pääsynhallinnan valvomisen keinoksi. Haastateltavan 4 mukaan fyysinen turvallisuus on tärkeä osa hänen edustamansa organisaation lääketieteellisten laitteiden pääsynhallintaa, sillä laitteiden turvallinen käyttö perustuu myös siihen, ettei laitteiden luokse pääsisi ulkopuoliset eivätkä ne olisi vapaassa käytössä. Hänen edustamassaan organisaatiossa fyysinen turvallisuus oli yhdistettynä kuluvalvontaan kuten muissakin organisaatioissa. Kulunvalvonnassa oli myös huomioitu miten ja minne laite oli sijoitettu. Haastateltava 3 kertoi lääketieteellisten laitteiden olevan lukituissa tiloissa ja tilojen pääsynhallintaa tehdään ja valvotaan. Haastateltava 1 organisaatiossa käytössä oli kulkukortit, joiden avulla voidaan pääsyä henkilöstöltä ja muilta henkilöiltä rajata tietyille osastoille ja huoneisiin. Lisäksi haastateltava 1 kertoi konehuoneiden ja tekniikkatilojen olevan erikseen lukittujen ovien takana.

Pääsynhallintaan liittyvät tietoturvauhat ja -riskit kulminoituvat usein laitteiden vajavaisiin tietoturvaominaisuuksiin ja käyttäjäorganisaatioiden käyttäjien toimintaan. Haastatelta-

van 1 mukaan laitehankintojen yhteydessä hänen edustamansa organisaatio on aikaisemmin joutunut tilanteisiin, joissa ongelmana on valmistajien kyvyttömyys vastata käyttäjäorganisaation tietoturva-vaatimuksiin. Tällöin organisaation tulee joustaa vaatimuksesta laitteiden hankinnan osalta, mutta pyrkivät korvaamaan vaatimustenmukaisuutta esimerkiksi vahvistamalla teknisiä kontroleja verkkojen osalta, jotka ovat terveydenhuollon organisaatioiden määritettävissä.

Fyysisessä pääsynhallinnassa haasteita tuovat myös laitteiden huoltotapahtumat, joita ei haastateltavan 3 mukaan pystytä valvomaan tarpeeksi hyvin. Huoltotapahtumien aikana ei tiedetä tarkemmin mitä huoltohenkilöt tekevät laitteilla eikä laitteen luokse päästettäviä henkilöitä välttämättä tarkasteta tai valvota riittävällä tasolla. Haasteena haastateltava 3 näkee sen, ettei huoltohenkilön henkilöllisyyttä tarkasteta tai huoltotapahtumien prosesseista ole ohjeistuksia ja toimintamallia, jonka avulla henkilökunta voisi paremmin valvoa huoltotapahtumaa. Haastateltavan 5 mukaan huoltotilanteissa käytännössä vain laitehuoltokoulutuksen käyneet ja henkilöt, joilla on lupa huoltoon, eli lähiesihenkilöt, voivat tehdä huoltotoimenpiteitä. Huolloista noin 70% tehtiin haastateltavan 5 organisaatiossa sisäisesti ja noin 30% tuotettiin muualta ostettuna. Pääsynhallintaa edistetään laitevalmistajien huoltokoodin avulla, joka saadaan laitevalmistajalta ja tulee kysyä ennen huollon suorittamista. Haastateltava 5 kertoi, että huoltoavaimia oli annettu lähiesihenkilöille lääketieteellisiin laitteisiin, joita organisaatiossa on isoja määriä. Näin ollen huoltoavainten on mahdollista päätyä väriin käsiin myös organisaation henkilöiden kautta.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Pääsynhallinnan ja -valvonnan keinoja	Luotettavat etäyhteydet laitetoimittajalta	H1, H2, H3, H4, H5
	Organisaation tietoturva-vaatimuksiin vastaavat lääketieteelliset laitteet	H1, H2
	Verkon tietoturvan ja teknisten kontrollien vahvistaminen	H1, H2, H3, H4, H5
	Etäyhteyden tunnistus yhteyden muodostuksessa	H1, H3
	Suljettujen verkkojen käyttö laitteiden yhteydessä	H2
	Organisaation tarvittavan tiukat vaatimukset etäyhteyksien muodostamiseen	H1
	Pääsynhallinnan vaatimusten luominen laitteiden kriittisyyteen ja tietoturva-arvioiteihin perustuen	H2
	Käyttäjien koulutus	H1
	Tilojen kulun- ja pääsynhallinta	H5
	Laitteiden turvallinen sijoittaminen	H1, H3, H5

	Kulkukortit	H1, H3, H4
	Huoltotapahtumien valvominen ja hallinnointi	H3, H5

Taulukko 12. Haastateltavien päähavainnot ja -nostot pääsynhallinnan ja -valvonnan keinoista.

Turvallisuuspoikkeamien hallinta ja havainnointi – Lääketieteellisten laitteiden turvallisuuspoikkeamien hallintaan liittyen haastatteluissa selvisi, että organisaatioissa turvallisuuspoikkeamien hallintaa tapahtuu joko palveluntarjoajan palveluiden tuottamana kokonaan tai yhdessä oman tietohallinnon ja palveluntarjoajan kautta tuotettuna. Yhdessä organisaatiossa turvallisuuspoikkeamien hallintaa oli tuotettu kokonaan organisaation sisäisenä palveluna, mutta jouduttu kuluneen vuoden aikana siirtymään osittain palveluntarjoajan piiriin oman organisaation sisäisten henkilöstövaihdosten vuoksi. Kaikilla haastatelluilla organisaatioilla käytössä oli ulkopuolisia palveluita ja ohjelmistoja, joilla pystyttiin valvomaan ja seuraamaan jatkuvaa liikennettä. Ulkopuolisten palveluntarjoajien käyttö tietoturvaluissa oli välttämätöntä kaikille organisaatioille. Yhteenveto haastateltavien päähavainnoista ja -nostoista laitteiden turvallisuuspoikkeamien hallinnasta ja havainnoinnista on koottu taulukkoon 14.

”Tietoturvapoikkeamien havainnointiprosessit eivät ole erilaisia lääketieteellisille laitteille eli kaikille laitteille on samanlainen poikkeamien ilmoitusprosessi.” –

Haastateltava 2

Tietoturvapoikkeamien havainnointi lääketieteellisissä laitteissa ei poikennut toimintatavoissa tai prosesseissa muista tietoturvapoikkeamien havainnoimisesta eli organisaatioilla oli sisäisesti käytössä olevat yleiset käytännöt, joissa organisaation mukaisesti tietoturva-asiantuntijat ja muut nimetyt henkilöt olivat mukana selvittämässä havaintoja. Haastateltava 2 kertoi, että kaikille laitteille on olemassa samanlainen poikkeamien ilmoitusprosessi, joka käynnistää sovitut toimintatavat ja käytänteet. Lääketieteellisten laitteiden kyberturvallisuuspoikkeamissa on mukana lääkintätekniikan lisäksi tietoturva-asiantuntijoita. Haastateltava 2 toi haastattelussaan ilmi, ettei näkisi järkeä olla omaa erillistä tietoturvahavaintojen hallintaprosessia lääketieteellisille laitteille, vaan hänen mukaansa tulisi ennemmin huolehtia koko organisaation kattavien prosessien toimivuudesta ja sisällyttää tietoturva tarvittavissa määrin mukaan.

Kaikki haastateltavat kertoivat tietoturvapoikkeamien valvomista toteutettavan kokoaikaisesti palveluntarjoajien avulla. Haastateltavien 1,2,3 ja 4 organisaatiot olivat ulkoistaneet tietoturvapoikkeamien ja -havaintojen hallinnoimisen kokonaan palveluntarjoajalle,

jolloin palveluntarjoajan vastuulla oli kokonaisuudessaan poikkeavan liikenteen havainnointi ja valvominen. Haastateltavan 5 organisaatiossa tietoturvapoikkeamien hallinnointi tapahtui tietohallinnon ja palveluntarjoajan yhteistyössä.

”Verkkovalvonta on jatkuvan valvomisen alla ja tietoverkkoon liitettävät lääketieteelliset laitteet ovat osana verkkoa.” – Haastateltava 1

”Valvontaa tietoverkkoon liitettäville lääketieteellisille laitteille on koko ajan.” – Haastateltava 3

Haastateltavien organisaatioissa tietoturvapoikkeamien valvontaa suoritettiin pääasiassa verkkovalvonnan kautta. Haastateltavien 1 ja 3 organisaatioiden tapaan myös haastateltavan 5 organisaatiossa verkkovalvontaa toteutettiin kokoaikaisesti. Haastatteluiden perusteella organisaatioilla oli olemassa erilaisia ohjelmistoja ratkaisuna jatkuvaan liikenteen seuraamiseen sekä kokoaikaiseen verkkovalvontaan. Näiden ohjelmistojen ja ohjelmien avulla seurattiin liikennettä verkoissa, joissa myös tietoverkkoon liitettävät lääketieteelliset laitteet olivat. Haastatteluiden mukaan lääketieteellisten laitteiden verkkovalvonta tapahtui noudattaen samanlaista kaavaa kuin muidenkin verkossa liitettävien laitteiden valvonta. Lääketieteelliset laitteet ovat jatkuvassa valvonnassa, kun laitteet ovat osana tietoverkkoa. Kaikissa haastateltavien organisaatiossa valvontaa järjestettiin jatkuvan liikenteen seurannalla 24x7 periaatteella. Tietoverkkoon liitettävien lääketieteellisten laitteiden näkökulmasta poikkeavan liikenteen valvominen, erityisesti ulospäin suuntautuvaa liikenteen, on erityisen tärkeää, jotta tilanteeseen voidaan puuttua mahdollisimman nopeasti palveluntoimittajien kanssa ja kytkeä laitteet mahdollisuuksien mukaan pois verkosta.

Haastateltava 1 kertoi, että jos poikkeama huomataan verkossa, niin silloin siitä laitetaan eteenpäin tieto erikseen nimetyille vastuuhenkilöille organisaatiossa. Haastateltava 2 kertoi, että vastuuhenkilöiden tiedottamisen jälkeen perustetaan kriittisyydestä riippuen organisaation prosessien mukaisesti toiminta käyntiin ja järjestetään tietoturvaryhmän kokoontumisia, mikäli havainto sitä vaatii. Isoissa poikkeamatilanteissa organisaatioilla kerrottiin olevan olemassa MIM-prosessit eli laajavaikutteisten häiriöiden prosessit (Major Incident Management), jotka sisältävät vastuuhenkilöt, kirjaajat, tilannekuvat ja yhteydenotot eri tahoihin tarkasti määriteltynä. Lisäksi haastateltavan 1 organisaatioissa voidaan lähettää tiedotteita henkilöstölle intrassa tai tekstiviestillä sekä käyttää Microsoft Teams -hälytyskutsuja. Haastateltavien 1 ja 2 organisaatiossa poikkeamista järjestettäviä uhkapalavereja järjestettiin 10 kertaa vuoden 2021 aikana. Haastateltavien 3 ja 4

organisaatiossa oli toteutuneiden poikkeamien avulla pystytty toteuttamaan poikkeamista käynnistyviä prosesseja ja näin kehittämään toimintatapoja yleisesti sekä erityisesti lääketieteellisten laitteiden osalta.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Tietoturva-poikkeamien hallinta	Organisaatiolla on olemassa verkkoon liitettyjen laitteiden jatkuva liikenteen valvonta 24x7.	H1, H2, H3, H4, H5
	Organisaatiolla on olemassa tietoturvapoikkeamille prosessi, jota käytetään myös lääketieteellisille laitteille.	H1, H2, H3, H4
	Organisaatiolla on olemassa MIM-prosessi olemassa.	H1, H2, H3, H4, H5
	Organisaatiot käyttävät ulkopuolisia palveluntarjoajia turvallisuuspoikkeamien hallintaan.	H1, H3, H5

Taulukko 13. Haastateltavien päähavainnot ja -nostot tietoturvapoikkeamien hallinnomisesta.

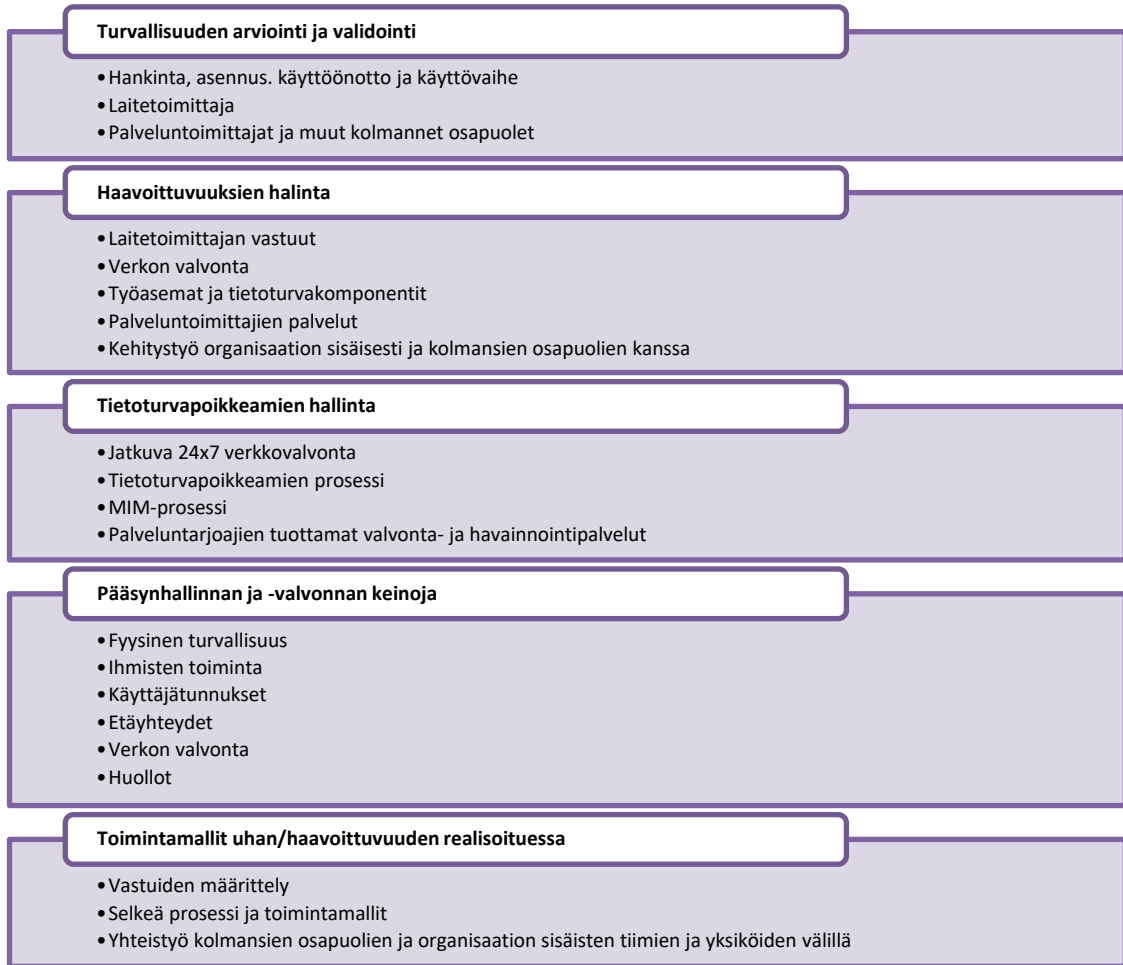
Toimintamallit kyberuhan tai -haavoittuvuuden realisoituessa - Haastatteluista selvisi, että jokaisessa organisaatiossa on olemassa omat toimintatavat, joita noudatetaan kyberturvallisuusuhan tai -haavoittuvuuden realisoituessa erilaisissa tilanteissa ja tapah- tumissa. Haastateltavien mukaan erillisiä toimintamalleja ei ole olemassa tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuusuhkien ja -haavoittuvuuksien va- ralle. Kaikilla organisaatioilla oli haastateltavien mukaan olemassa jonkinlainen proto- kolla, prosessit tai joukko toimintatapoja yleisesti kyberturvallisuusriskien ja -haavoittu- vuuksien realisoitumisten varalle. Näitä yleisiä prosesseja sovellettiin haastateltavien mukaan lääketieteellisiin laitteisiin kohdistuviin uhkiin ja riskeihin tarvittaessa.

Haastattelujen perusteella organisaatioissa lääketieteellisistä laitteista pääasiallisesti vastuussa ovat lääkinnällisten laitteiden yksiköt sekä lääketekniikan parissa työskente- levät henkilöt. Lääkinnällisten laitteiden yksiköiden vastuuhenkilöiden rooliin kuului muun muassa huoltojen sekä kliniseen työskentelyyn liittyvän toiminnan ohjeistaminen. Tieto- hallinto puolestaan vastasi kokonaisuudessaan tietoturvasta ja niiden tilanteiden johta- misesta. Haastatteluista selvisi, että tietoturvan ja lääkintätekniikan tiimit toimivat yhteis- työssä lääketieteellisten laitteiden kyberturvallisuuden edistämässä, mutta yhteis- työssä on silti kehitettävää ja sitä tulee edistää.

Haastateltava 1 kertoi omassa haastattelussaan, etteivät toimintamallit kyberuhan to- teutuessa ole yksiselitteisiä tietoverkkoon liitettävissä fyysisissä lääketieteellisissä lait- teissa. Myös haastateltava 3 kertoi, ettei organisaatiossa ole olemassa lääketieteellisille laitteille erillistä omaa protokollaa kyberuhkien varalle. Samasta organisaatiosta haasta- teltava 4 kertoi kuitenkin jonkinlaisten toimintamallien olemassaolosta. Haastateltava 5 kertoi puolestaan organisaatiossa olevan protokolla yleisesti sovellettavaksi kyberuhkiin sekä protokollaan liittyviä keskusteluja ja läpikäynnit kahdesti vuodessa.

Vastuiden epäselvyys johtuu pääasiassa rajanvedosta liittyen lääketieteellisten laitteiden kuulumisesta lääkintätekniikkaan ja toisaalta kyberuhkien ja -haavoittuvuuksien liittymisestä vahvasti tietoturvan ja sitä kautta tietohallinnon toimintaan. Haasteiksi haastateltavat näkivät, ettei lääketieteellisten laitteisiin liittyen ole selkeitä tai ollenkaan määriteltyjä tietoturvavastuita. Haastateltavan 1 organisaatiossa tietoturvasta vastaa loppukädessä tietohallintojohtaja, mutta lääketieteellisten laitteiden tietoturvavastuita ei erikseen ole määritelty. Haastateltava 5 painotti, että on erityisen tärkeää, että kaikilla osapuolilla on riittävä ja tarvittava tieto, kuinka toimia erilaisissa tilanteissa. Vastuiden ja roolien näkökulmasta haastateltava 5 oli sitä mieltä, että toimintamallien luonti ja läpikäynti koskettaa enemmän tietohallintoa kuin lääkintätekniikkaa itsessään.

Yhteenveto tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arvioinnista, valvonnasta ja hallinnasta – Haastattelujen päähavainnot eri alateemoista riskienhallintaan ja riskeihin on koottuna kuvaan 4. Haastatteluista selvisi, että turvallisuuden arviointia ja validointia tehdään pääasiassa hankinta-, asennus-, käyttöönoton ja käyttövaiheissa. Turvallisuutta arvioitiin myös laitetoimittajien, palveluntuottajien ja muiden kolmansien osapuolien osalta esimerkiksi organisaation omiin vaatimuksiin vertaamalla. Haavoittuvuuksien hallinnassa haastateltavat nostivat esiin erityisesti laitetoimittajan vastuut sekä verkon valvonnan, työasemien ja komponenttien suojaamisen. Lisäksi haavoittuvuuksien hallinnassa merkittävä rooli oli kolmansilla osapuolilla ja palveluntuottajille, joilta organisaatiot ostivat tietoturvapalveluita.



Kuva 4. Yhteenveto haastateltavien nostamista aiheista tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arvioinnista, valvonnasta ja hallinnasta.

Haastateltavat nostivat tietoturvapoikkeamien hallinnasta jatkuvan verkkovalvonnan toteutettuna palveluntoimittajien kanssa, MIM- ja tietoturvapoikkeamien prosessit sekä muut palveluntarjoajien tuottamat valvonta- ja havainnointipalvelut. Pääsynhallinnan ja -valvonnan keinoista nousivat esille erityisesti fyysinen turvallisuus, ihmisen toiminta, käyttäjätunnukset, etäyhteydet, verkon valvonta sekä huoltotapahtumien valvominen ja hallinnointi. Toimintamallien tärkeydestä uhan tai haavoittuvuuden realisoituessa nostettiin esille selkeiden prosessien ja toimintamallisen olemassaolo ja kommunikointi, sekä vastuiden määrittelyt ja yhteistyö kolmansien osapuolien kanssa.

5.3 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hankinnat ja niissä tehtävä yhteistyö

Kyberturvallisuuteen liittyvä yhteistyö laitevalmistajien kanssa - Kaikissa haastatelluissa organisaatioissa tehtiin kaikissa jonkintasoista yhteistyötä laitevalmistajien

kanssa, mutta yhteistyön laajuus ja määrä sekä tavat vaihtelivat organisaatioittain. Keskusteluja on käyty esimerkiksi laitteisiin liittyvistä vaatimuksista ja esille nostettuja kysymyksiä liittyen laitevaatimusten mahdollisuuksista. Yhteistyö laitevalmistajien ja -toimittajien kanssa ei ollut kaikissa organisaatioissa jatkuvaa tai systemaattista, eikä välttämättä kyberturvallisuuteen suoraan liittyvää. Yhteenvedo haastateltavien päähavainnoista ja -nostoista kyberturvallisuuteen liittyvästä yhteistyöstä laitevalmistajien kanssa on koottu taulukkoon 15.

Organisaatioiden ja laitevalmistajien välinen yhteistyö keskittyi kaikissa organisaatioissaan erityisesti hankintoihin ja huoltoihin. Haastateltavat olivat sitä mieltä, että vaikka yhteistyötä on olemassa, tulisi sitä edelleen kehittää, lisätä ja parantaa. Yhteistyön haasteena nähtiin yleisesti rajapintojen olemattomuus tietoturvan ja laitevalmistajien kanssa, sekä yhteistyön kehittäminen.

”Yhteistyötä tehdään terveydenhuollon organisaatioiden ja laitevalmistajien välillä. Hankinnat ovat tiedossa ja niiden perusteella voidaan tehdä markkinakatsauksia ja kyselyitä ennakkoon. Lisäksi laitevalmistajilta voidaan tiedustella, minäkälaisia toimintoja on mahdollista saada laitteisiin.” – Haastateltava 1

Haastateltavat tunnistivat lääketieteellisten laitteiden hankintojen yhteydessä tapahtuvan yhteistyötä laitevalmistajien kanssa. Haastateltava 1 kertoi yhteistyötä tehtävän terveydenhuollon organisaatioissa laitevalmistajien kanssa yleisesti samoin kuin hänen edustamassaan organisaatioissa ja laitevalmistajien välillä. Haastateltava 1 toi esille yhteistyötä tehtävän erityisesti lääkintäteknikan yksikössä hänen edustamassaan organisaatiossa. Yhteistyötä tehtiin erityisesti hankintojen suhteen ennakoiden markkinakatsauksien, kyselyiden ja laitevalmistajien keskustelujen avulla.

Haastateltava 2 kertoi edustamansa organisaation määritelleen ja jalkauttaneen lääketieteellisille laitteille vaatimukset laitetoimittajille. Vaatimusten määrittelyssä ja jalkautuksessa mukana oli myös palveluntarjoaja, joka oli haastateltavan 2 organisaatiossa mukana koko laitevaatimusprosessissa. Haastateltava 2 kertoi, että vaatimuksia käydään läpi yhdessä toimittajien kanssa laitehankintojen yhteydessä samanaikaisesti sopimusten hallinnoinnin kanssa. Haastateltavan 5 mukaan laitevalmistajien kanssa on käyty vaatimuksia läpi lääketieteellisille laitteille. Haastateltavan 5 mukaan laitevalmistajat ovat pystyneet vastaamaan vaatimuksiin ja olleet samaa mieltä organisaation tekemistä vaatimuslistoista laitteille. Haastateltava 5 kertoi laitevalmistajien toimintaan olevan helppo luottaa erityisesti tietosuojan osalta, sillä laitevalmistajat ovat monesti Yhdysvaltaisia yrityksiä, joissa haastateltava koki tietosuojan olevan korkealla ja tarvittavalla tasolla.

Haastateltava 3 kertoi laitetoimittajien kanssa olleen keskusteluja laitteiden kyberturvallisuuteen liittyvistä kysymyksistä ja vastauksista. Haastateltavan 3 mukaan kysymykset ovat herätelleet toimittajia ja valmistajia laitteisiin liittyvistä vaatimuksista ja ominaisuuksista, joita laitteisiin kaivataan.

Hankintoihin liittyen haastateltavissa organisaatioissa hyödynnettiin ulkopuolisia palveluntarjoajia ja heidän palveluitaan. Haastateltava 2 kertoi hankintojen yhteydessä käytettävän vaatimuslistojen lisäksi palveluntarjoajaa myös ostajana isommille laitteille. Haastateltava kertoi tällaiseksi isoimmiksi laitteiksi esimerkiksi kuvantamisen laitteet. Mikäli palveluntarjoajaa käytetään ostajana isommalle laitehankinnalle, niin tarjoajataho tekee myös tietosuoja ja -turvasopimuksen. Jos taas haastateltavan 2 edustama organisaatio ostaa laitteen, niin organisaatio tekee itsenäisesti tietosuoja ja -turvasopimuksen. Haastateltava 4 nosti esille myös satunnaisen yhteistyön verkon toimittajan kanssa, jonka kautta on kommunikoitu myös laitevalmistajille vaatimuksista esimerkiksi segmentointien suhteen.

Hankintoihin liittyvän yhteistyön lisäksi haastateltavat tunnistivat laitteiden elinkaaresta huoltojen yhteydessä tapahtuvat yhteistyötä laitetoimittajien ja -valmistajien kanssa. Haastateltava 5 kertoi yhteistyötä tapahtuvan ja tehtävän huoltojen ja hankintojen yhteydessä hänen edustamassaan organisaatiossa. Haastateltava 5 kertoi myös, että uuden MDR-asetuksen mukaisesti laitevalmistajien tulee valvoa elinkaaren aikaista koulutusta eli yhteistyön lisääntymistä voidaan odottaa. Haastateltava 5 koki yhteistyön lisääntymisen olevan toivottua ja tarvittavaa lääketieteellisten laitteiden kyberturvallisuuden kehittämiseksi.

”Yhteistyötä laitevalmistajien kanssa on, mutta yhteistyön tarkoista tavoista ei ole tietoa tietohallinnossa, sillä suoraa rajapintaa tietohallinnosta ei ole laitevalmistajiin.” – Haastateltava 2

Laitevalmistajien ja -toimittajien yhteistyöstä nostettiin esille haasteita, joita haastateltavat kokivat yhteistyöhön liittyvän. Haastateltava 2 nosti esille haasteeksi rajapintojen puuttumisen ja olemattomuuden, jolloin yhteistyön tarkasta tekemisestä ja teemoista ei haastateltavalla ollut tietoa. Haastateltava 2 kertoi haastattelussaan, että yhteistyötä laitevalmistajien kanssa tehdään lääketieteellisiin laitteisiin liittyen, mutta rajapinnan puuttuminen tietohallinnon ja laitevalmistajien kanssa tunnistettiin haasteeksi. Rajapinnan puuttuminen näkyi haastateltavalle 2 erityisesti läpinäkymättömyytenä laitevalmistajan kanssa tehtäviin tarkkoihin yhteistyötehtäviin ja -tapoihin. Haastateltava 2 tunnisti kuitenkin hankintojen kautta tehtävää yhteistyömuotoja, joihin liittyvät myös tietohallinnon työ-

tehtävät ja vastuut. Rajapintojen puuttumisen haaste liittyi kuitenkin enemmän organisaation sisäiseen toimintaan ja järjestelyyn, sillä yhteistyötä haastateltavan organisaation ja laitetoimittajien kanssa harjoitettiin.

Haastateltavat toivat esille myös säännönmukaisuuden puuttumisen laitevalmistajien kanssa tehtävästä yhteistyöstä. Haastateltavat 1 ja 3 olivat yhdessä haastatteluisaan samoilla linjoilla, että keskustelua yhteistyöstä tapahtuu ajoittain, mutta ei säännöllisesti tai kaikkien toimittajien kanssa. Haastateltavan 3 mukaan vain yhden toimittajan kanssa on ollut enemmän vuoropuhelua ja keskustelua. Haastateltavien 2 ja 3 näkökulmasta yhteistyötä erityisesti kyberturvallisuuden näkökulmasta olisi syytä kehittää ja parantaa ja yhteistyöstä tehdä säännöllisempää.

”Tietoturvaluus ei ohjaa hankintoja, vaan kliininen käyttö on ykkösasia potilaan hyvän hoidon takaamiseksi.” – Haastateltava 1

Laitevalmistajien kanssa tehtävää kyberturvallisuuteen liittyvää yhteistyötä haastaa kliinisen työn huomioiminen. Haastateltavan 1 mukaan kliinisen työn varmistaminen ja potilaan hyvä hoito ovat lääketieteellisten laitteiden pääprioriteetteja. Tällöin kyberturvallisuus ei voi ohjata lääketieteellisten laitteiden hankintoja, jolloin kaikkia kyberturvallisuuteen liittyviä toimintoja ei voida turvallisuuden näkökulmasta toteuttaa kliinisen työn turvaamiseksi.

Haastateltavien haavaintojen teemat	Haastateltavien päähavainnot	Maininnat
Laitevalmistajien yhteistyömuodot	Yhteistyö laitevalmistajien kanssa hankintojen yhteydessä.	H1, H2, H3, H4, H5
	Yhteistyö laitevalmistajien kanssa laitehuoltojen yhteydessä.	H1, H3, H5
	Yhteistyö organisaation tiimien ja yksiköiden välillä.	H1
	Laitevaatimusten läpikäyntiä ja keskustelua laitevalmistajan kanssa.	H3, H5
Laitevalmistajien yhteistyön haasteita	Organisaation sisäisten yksiköiden ja tekemisen läpinäkymättömyys ja rajapintojen puuttuminen.	H2
	Yhteistyö laitevalmistajien kanssa ei ole säännöllistä tai systemaattista	H1, H2, H3
	Kliinisen työn priorisoiminen yli tietoturvan vaatimusten	H1

Taulukko 14. Haastateltavien päähavainnot ja -nostot laitevalmistajien kanssa tehdystä yhteistyöstä ja siihen liittyvistä haasteista.

Kyberturvallisuusriskien huomiointi hankinnoissa – Haastateltavilta kysyttiin kyberturvallisuusriskien huomioinnista lääketieteellisten laitteiden hankinnoissa. Kaikissa haastateltavissa organisaatioissa hankintoihin liittyi organisaation sisäinen prosessi ja siihen liittyviä toimenpiteitä. Yhteenvedo haastateltavien päähavainnoista ja -nostoista kyberturvallisuusriskien huomioinnista hankinnoissa on koottu taulukkoon 16.

Hankintojen prosessit ja niihin liittyvät vaiheet vaihtelivat sisällöltään organisaatioista riippuen. Yhteistä kaikille organisaatioille oli kuitenkin tietoturva- ja suojavaatimusten läpikäyminen osana hankintojen prosessia. Hankintojen yhteydessä tehtävää kyberturvallisuusriskien hallintaa toteutettiin haastateltavissa organisaatioissa pääsääntöisesti yhteistyössä laitevalmistajien ja -toimittajien sekä muiden terveydenhuollon organisaatioiden kanssa. Organisaatioiden hankinnan sisäisiin prosesseihin osallistuu monia eri tiimejä ja yksiköitä, jotka tuovat omia näkökulmia ja osaamisalueistaan huomioita esille hankintojen tarpeisiin ja vaatimuksiin.

Kyberturvallisuusriskejä oli pyritty huomioimaan hankintojen yhteydessä haastatelluissa organisaatioissa kattavasti tietoverkkoon liitettävien lääketieteellisten laitteiden tietoturvavaatimusten avulla. Hankintojen yhteydessä kaikkien haastateltavien organisaatioiden laitevaatimusten lisäksi oli määritelty myös tietoturva ja -suojaliitteet. Haastateltava 4 kertoi heillä olevan tietyt määritellyt vaatimukset laitteille ja kun ne täyttyvät, niin laite tai liitteet katsottiin voitavan hankkia.

”Hankinnoissa on olemassa tietyt vaatimukset, ja kun ne täyttyvät, niin sitten hankinta voidaan katsoa tehtäväksi.” – Haastateltava 4

Haastateltavan 4 mukaan hankinnoissa käytettävät vaatimukset nähdään riittäviksi hankintojen tekemiseksi. Haastateltava 4 kertoi, ettei ollut itse vaatimusten tekemisen jälkeen arvioinut uudelleen tai päivittänyt vaatimuksia ja niiden käytettävyyttä. Haastateltava 5 kertoi hänen edustamallaan organisaatiolla olevan hankintoihin liittyen excel-tiedosto, jossa on erilaisia kriteerejä ja vaatimuksia sekä mahdollisia muita huomioon otettavia asioita. Haastateltavan 5 organisaatiossa käytettävä vaatimustiedosto perustui Kyberturvakeskuksen tuottamaan listaukseen.

”Kyberturvallisuus on pakottavissa vaatimuksissa osana sopimusehtoja.” – Haastateltava 5

Haastateltavan 5 mukaan pakottavissa vaatimuksissa kyberturvallisuus on otettu mukaan sopimusehtoihin. Kyberturvallisuuden huomioiminen hankinnoissa ei siis ollut pakollinen huomioitava asia kaikissa tapauksissa. Haastateltavan 3 organisaatiossa tietoturva ja -suojaliitteiden lisäksi kyberriskit lääketieteellisissä laitteissa oli huomioitu toimittajan kyvyssä vastata organisaation verkkoon. Lisäksi haastateltava 3 kertoi, että kyberriskien huomiointia on sisällytetty toimittajan vaatimukseen pystyä kertomaan tietoliikenneyhteydet ja yleisesti tietoverkkoon liittyvistä asioista ja ylläpidosta ratkaisuja.

Tietoturvavaatimuksista ja niiden mahdollisista poikkeamista keskusteltiin organisaatioiden eri asiantuntijoista muodostuvissa ryhmissä. Haastateltavan 5 organisaatiossa hankintojen yhteydessä muodostettiin noin 7-15 henkilön hankintaryhmiä lääketieteellisestä

laitteesta ja sen käytöstä riippuen. Kyberturvallisuusuhkien ollessa tunnistetusti vähäisiä tai pieniä tiettyjen laitteiden kohdalla, kuten esimerkiksi verenpainemittarien, ei asiantuntijaryhmää oteta mukaan valmisteluun. Fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kohdalla asiantuntijaryhmä on kuitenkin aina mukana, sillä näissä hankinnoissa yhdistyy laitteiden kyky siirtää dataa ja olla liitettynä verkkoon.

Kaikki haastateltavat organisaatiot tunnistivat kyberturvallisuusriskien huomioimisen olevan tärkeää lääketieteellisten laitteiden hankinnassa, mutta kyberturvallisuuden huomiointi ja kehittäminen hankinnoissa ei ole yksiselitteistä. Haasteena kyberriskien huomioimisessa on kuitenkin lääketieteellisten laitteiden tarve toteuttaa ja mahdollistaa ensisijaisesti kliininen työ. Haastateltava 1 mainitsi haastattelussaan, ettei kyberturvallisuus ohjaa hankintoja vaan pääasiallisesti kliininen työ, jonka pääasiana on potilaan oikeanmukaisen ja hyvän hoidon takaaminen. Kliinisen työn mahdollisimman toimiva ja tehokas toimiminen voi kuitenkin olla ristiriidassa kyberturvallisten käytäntöjen ja parhaiden toimenpiteiden kanssa.

Organisaatiot ovat törmänneet hankinnoissa tiettyjen kyberturvallisten ominaisuuksien ja ratkaisuiden käyttämisen olevan mahdottomia, sillä tiettyjä kyberturvallisuusvaatimuksia ei ole kehitetty tietoverkkoon liitettäviin lääketieteellisiin laitteisiin vielä tai ne eivät tue kliinisen työn käyttöä. Haastateltava 1 kertoi haastattelussaan, ettei hänen edustamansa organisaation tietoturva-vaatimukseen ole aina pystytty vastaamaan. Tällöin osasta vaatimuksista on jouduttu luopumaan ja kehittämään luovuttujen tietoturva-vaatimusten tilalle suojausta esimerkiksi vahventamalla verkon suojauskäytäntöjä. Haastateltava 3 kertoi puolestaan, että työasemat ovat kehittyneet vuosien varrella paljon nopeammin kuin fyysiset tietoverkkoon liitettävät lääketieteelliset laitteet. Tämä on johtanut haasteisiin, joissa teknisesti lääketieteelliset laitteet eivät pysty vastaamaan ICT-toimittajien luomiin vaatimuksiin kyberturvallisista käytännöistä. Tällöin haastateltavan 3 organisaatiossa on jouduttu rakentamaan digitaalinen ympäristö vastaamaan laitteiden tarpeisiin, jotka muodostuvat heikoista kyberturvallisuuden ominaisuuksista.

Hankintojen kyberturvallisuusriskien hallitsemista toteutetaan myös yhteistyössä laitevalmistajien ja -toimittajien kanssa. Haastateltava 1 kertoi haastattelussaan, että yhteistyötä tehdään laitevalmistajien sekä muiden terveydenhuollon organisaatioiden kanssa kyberriskeistä lääketieteellisissä laitteissa. Haastateltavan 1 organisaatiossa hankinnat ovat tiedossa yleensä etukäteen ja näin hankintojen yhteydessä tehdään markkinakatsauksia sekä kyselyitä ennakkoon laitetoimittajille. Mikäli laitteisiin liittyvien vaatimusten tunnistetaan olevan haasteellisia tai erityisen vaativia, voidaan laitetoimittajiin ja -valmistajiin olla yhteydessä ennakkotiedoilla ja kysyä heiltä mielipiteitä ja ajatuksia niistä. En-

nakkotietojen lähettämisen avulla haastateltavan 1 organisaatio on pystynyt tiedustelemaan laitetoimittajien kykenevyyksiä vastata kyberturvallisuuttakin käsitteleviin vaatimuksiin.

Laitetoimittajien kanssa tehtävän yhteistyön lisäksi haastateltava 4 toi esille hankintatoimiston kanssa tehtävän yhteistyön. Haastateltavan 4 organisaatiossa hankintatoimisto vastaa hankintojen tekemisestä, jolloin hankintatoimiston vastuulla on erilaisten dokumenttien tekeminen. Hankintatoimiston kanssa tukena hankinnoissa on haastateltavan 4 edustaman organisaation kliinisen ja teknisen työn asiantuntijoita. Hankintatoimiston ja organisaation eri asiantuntijoiden avulla hankinnoissa otetaan myös kyberturvallisuusriskit huomioon.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Hankinnassa tapahtuva kyberriskien huomiointi	Tietoturva- ja suojaliite osana hankinnan prosessia.	H1, H3, H4, H5
	Tietoturva-vaatimusten laatiminen.	H1, H4, H5
	Palveluntarjoajien, laitetoimittajien ja muiden kolmansien osapuolien kanssa tehtävä yhteistyö kyberriskien huomioinnista ja vaatimuksista laitteiden toiminnalle sekä ympäristölle.	H1, H5
	Asiantuntijoiden osallistuttaminen organisaatiossa osana hankintojen prosessia.	H5
	Organisaation reagoiminen erityisvaatimusten tai -suojausten toteuttamiseksi laitteille, jotka eivät täytyä vaatimuksia.	H1, H2, H3
	Ennakoiva yhteistyö ja kehitysyhteistyö laitevalmistajien kanssa.	H1
	Markkinakatsaukset laitevaatimuksista ja -ominaisuuksista.	H1

Taulukko 15. Haastateltavien päähavainnot ja -nostot kyberturvallisuusriskien huomioinneista hankinnoissa.

Yhteenveto tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden yhteistyöstä laitevalmistajien kanssa ja hankinnan prosesseissa – Haastattelujen päähavainnot eri alateemoista laitevalmistajien kanssa tehtävästä yhteistyöstä ja kyberturvallisuusriskien huomioinnista hankintojen yhteydessä on koottuna kuvaan 5. Laitevalmistajien kanssa tehtävä yhteistyö nousi suurimmaksi yhteistyömuodoksi haastateltujen organisaatioista. Laitevalmistajien kanssa tehtiin yhteistyötä osana hankintaprosessia ja huoltotapahtumia, mutta joissakin tapauksissa myös ennakoivasti. Laitevalmistajien kanssa tehtävässä yhteistyössä nostettiin esille myös kehityskohteita ja tarpeita tehdä entistä vahvemmin ja systemaattisemmin yhteistyötä organisaation ja laitevalmistajien kanssa.

Kyberriskien huomiointia tapahtui kaikissa organisaatioissa osana hankintoja ja niiden prosesseja. Hankinnoissa kyberriskien huomiointi korostui erityisesti organisaation sisäisissä toimintatavoissa ja vaatimuksissa hankittaville laitteille sekä laitteiden käytön aikaisissa prosesseissa. Käytön aikaisia kyberriskejä hallittiin myös ja huomioitiin palveluntarjoajien ja muiden kolmansien osapuolien kanssa ostetuilla palveluilla. Pääasiallisesti haastateltavat korostivat kuitenkin laitevalmistajien vastuuta laitteiden teknisten kyvykkyyksien huomiointissa sekä käytön aikaisesti päivityksissä ja huolloissa.

Hankinnat ja niissä tehtävä yhteistyö

Laitevalmistajien ja hankinnan prosesseissa toteutettava yhteistyö

Yhteistyömuodot laitevalmistajien kanssa
Haasteet ja kehityskohteet yhteistyössä laitevalmistajien kanssa

Kyberriskien huomiointi osana hankintoja ja hankintojen prosessia

Organisaation sisäiset toimintatavat
Kolmansien osapuolien kanssa tehtävä yhteistyö
Laitevalmistajien vastuu

Kuva 5. Yhteenvedo haastateltavien nostamista aiheista tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hankintaprosessista ja laitevalmistajien kanssa tehtävästä yhteistyöstä.

5.4 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuut ja seuranta

Lääketieteellisten laitteiden turvallisuuteen liittyvät vastuut – Haastatelluissa organisaatioissa tietoverkkoon liitettävien lääketieteellisten laitteet kuuluivat osaksi lääketieteellisiä laitteita ja niitä käsiteltiin yhtenäisenä joukkona turvallisuuden näkökulmasta. Haastatteluista selvisi, että lääketieteellisiin laitteisiin liittyvät vastuut eivät ole selkeitä ja eri yksiköiden ja tiimien välinen työnjako lääketieteellisten laitteiden kyberturvallisuudesta, tai ylipäätään turvallisuudesta, ei ole yksiselitteinen. Lisäksi laitteiden turvallisuuden osa-alueet nähtiin kuuluvan eri yksiköille ja tiimeille organisaatioista riippuen, jolloin vastuuden rajat saattoivat olla häilyviä. Yhteenvedo haastateltavien päähavainnoista ja -nostoista laitteiden turvallisuuteen liittyvistä vastuista on koottu taulukkoon 17.

Turvallisuuteen liittyvät vastuut jakaantuivat organisaatioissa pääasiallisesti laitevalmistajien sekä tietoturvan, lääkinnällisten laitteiden, klinisen työn yksiköiden välille. Haastateltavat kertoivat, että vaikka lääketieteellisten laitteiden päävastuu on tietohallinnon ja

lääketekniikan yksiköissä, on silti vastuuta myös klinisen työn ja hankinnan puolella. Lääketieteellisten laitteiden ja niiden kyberturvallisuuden vastuut eivät kuitenkaan olleet haastattelujen mukaan selkeitä organisaation sisällä. Haastateltavan 4 mukaan ei ole olemassa henkilöä, joka olisi suoranaisesti vastuussa laitteiden kyberturvallisuudesta. Hänen näkökulmastaan vastuu on jakautunut organisaatiossa eri henkilöille eri puolelle organisaatiota, mutta yksiselitteistä tai sovittua vastuuhenkilöä ei ole määritelty. Toisaalta taas vastuiden nähtiin noudattavan sovittuja protokollia ja prosesseja liittyen kyberturvallisuuteen tai lääketieteellisiin laitteisiin, joissa vastuut on voitu jollakin tavalla määrittää. Haasteena nähtiin niiden toteutuminen ja yksityiskohtaisuus, jotka eivät välttämättä toteudu henkilötasolla.

Haastatelluissa organisaatioissa tietoturvan johtaminen ja sen vastuu on tietohallinnolla ja viimekädessä organisaation tietoturvajohtajalla. Vaikka tietoturvalla ja tietohallintojohtajalla on selkeä vastuu ja johtamisrooli tietoturvallisuudesta, kertoo haastateltava 1 silti, etteivät vastuut ole selkeitä lääketieteellisten laitteiden suhteen. Lisäksi haastateltavan 1 mukaan lääkintälaitteille ei ole määritelty erillisiä tietoturvavastuita, vaan niihin sovelletaan yleisiä tietoturvan toimintamalleja ja -prosesseja, mikäli jotakin poikkeavaa tapahtuu.

”Vastuut eivät ole aivan selkeitä – tietoturvasta vastaa tietohallintojohtaja, mutta tietoturvavastuita ei ole erikseen määritelty lääkintälaitteisiin.” – Haastateltava 1

Haastateltavan 1 mukaan vastuiden epäselvyys johtuu pääsääntöisesti tietoturvavastuiden puuttumisesta kohdistettuna erityisesti lääkintälaitteisiin. Hankintoihin liittyvissä tietosuoja- ja tietoturva-asioissa tietoturvallisuuden kehittämistä vastasi haastateltavan 1 mukaan tietoturvavastaava. Tietoturvavastaava vastasi prosessimaisesti niiden ylläpitämisestä hankintojen yhteydessä. Tietoturvavastaavan rooliin kuului haastateltavan 1 organisaatiossa myös ylläpitää ja päivittää prosessin mukaisesti hankintavaatimuslistaa.

Tietoturvan ja tietohallinnon lisäksi lääketieteelliset laitteet ja niiden kyberturvallisuus oli vahvasti osana lääkintäteknikkaa haastatelluissa organisaatioissa. Haastateltavien organisaatioissa lääkintäteknikka oli vastuussa kaikista organisaation lääkinnällisistä laitteista. Haastateltavan 5 organisaatiossa lääkintäteknikan puolella nimetty vastuuhenkilö oli vastuussa kaikista lääkinnällisistä laitteista. Lisäksi organisaatiossa kerrottiin toimivan huoltomestareita, jotka huolehtivat pienistä elektroniikka- ja kuvantamisen laitteista. Haastateltavan 5 organisaatiossa lääketieteellisten laitteiden poikkeamatilanteessa tilannetta lähtee käsittelemään lääkintäteknikan vastuuhenkilö, joka vie asian tarvittaessa eteenpäin huoltomestarille poikkeaman korjaamiseksi.

Lääkintätekniiikan lisäksi organisaatioiden klinisen työn vastuut nostettiin esille haastatteluissa. Haastateltavan 3 mukaisesti lääketieteellisten laitteiden käytöstä on vastuussa käyttävät yksiköt ja käyttäjät. Haastateltava 5 kertoi, että lähtökohtaisesti laitteiden käytön vastuu on kliinisessä työssä toimivalla lääkäriellä, mikäli lääketieteellistä laitetta käytetään valmistajan määrittämään käyttöön. Haastateltava 4 oli haastateltavan 5 kanssa samaa mieltä ja hänen edustamassaan organisaatiossa vastuussa klinisestä työstä ja siellä käytettävistä laitteista oli ylläkäriellä.

Haastateltavat nostivat haastatteluissaan ilmi laitetoimittajien ja -valmistajien vastuun lääketieteellisten laitteiden kyberturvallisuuden kehittämisestä sekä ohjeistamisesta. Haastateltava 4 toi ilmi haastattelussaan, että laitetoimittajalla on pääasiallinen vastuu laitteiden turvallisuudesta. Hänen edustamassaan organisaatiossa ei ollut nimetty henkilöä tai roolia, joka olisi koettu olevan suoranaisesti vastuussa lääketieteellisten laitteiden turvallisuudesta. Haastateltava 3 kertoi, että laitevalmistajan vastuulla on käyttäjien ohjeistaminen. Haastateltavan 3 mukaan laitevalmistajien tulisi toimittaa kattavampia ohjeistuksia, jotka sisältäisivät myös kyberturvallisuuteen liittyviä ohjeita ja toimenpiteitä. Haastateltavan 4 mukaan vastuu turvallisuudesta on monen henkilön summa, mutta varsinaisia tietoturvastuita organisaatiossa ei ollut määritelty lääketieteellisiin laitteisiin. Haastateltavien 4 ja 5 mukaan laitetoimittajilla on myös iso vastuu laitteiden kehityksestä ja jatkuvuudesta.

”Lääkinnällisissä laitteissa on vahvasti määritellyt vastuut ja siksi valmistajien on hallinnoitava niitä itse. Laitetoimittajat määrittelevät monia asioita lääketieteellisten laitteiden turvallisuudessa, jolloin käyttäjäorganisaatiolle jää turvallisuuden ylläpitäminen ja oman verkon tekeminen ja siitä huolehtiminen.” – Haastateltava 4

Haastateltavan 4 mukaan lääkinnällisten laitteiden vastuut ovat määriteltyjä, ja näiden vahvasti määriteltyjen vastuiden takia valmistajat hallinnoivat ja määrittelevät niitä itse. Hänen mukaansa laitteiden valmistajavastuiden toteutumiseksi valmistajat haluavat ja niiden tulee itse valvoa ja hallinnoida turvallisuuteen liittyviä asioita. Tämä aiheuttaa haasteen kuitenkin käyttäjäorganisaatioille, mikäli ne haluaisivat toteuttaa tietoturvaa lääketieteellisissä laitteissa korkeammilla suojausmenetelmillä kuin mitä valmistaja on laitteeseen määritellyt.

Organisaatioiden sisäisten toimijoiden, tietohallinnon, lääkintätekniiikan ja klinisen työn, sekä laitevalmistajien vastuiden lisäksi haastateltava 5 nosti esille muut organisaation ulkopuoliset sidosryhmät. Haastateltava 3 kertoi ICT-toimittajan olevan vastuussa verkon toimittamisesta ja sen ylläpitämisestä. ICT-toimittajan vastuut ovat kirjattuna sopi-

muksissa. Haastateltava 5 nosti vastuuden kohdalla esille myös Fimean, lääkealan turvallisuus- ja kehittämiskeskuksen, joka laatii omissa tarkastuksissaan ohjeistuksia tiettyihin laitteisiin. Fimea valvoo ja vaatii laitteiden rekisteröimistä erityisesti sellaisiin laitteisiin, jotka lähettävät mittadataa ja joita potilaat voivat saada kotihoitoon. Fimealla on vastuullaan ohjeistaa lääketieteellisten laitteiden seuraamista sekä on mukana laitteiden poikkeamailmoituksissa, joita käyttäjät voivat tehdä ilmoittaakseen laitteen poikkeamasta, uhasta tai ongelmasta

Tietoturvan kehittämisestä haastateltava 4 koki päävastuussa olevan laitetoimittajat. Laittevalmistajat määrittävät minkälaisia muutoksia laitteisiin voidaan tehdä niiden elinkaaren aikana ja siten ovat vahvasti laitteiden kehittämisen määrittelijöitä. Toisaalta laitevalmistajat ovat roolissa, jossa voivat kehittää uusien laitteiden turvallisuutta kehittämällä laitteiden ominaisuuksia ja teknisiä kontrolleja. Haastateltavan 2 mukaan vastuu kehittämisestä ja jatkuvuudesta on myös käyttäjillä ja käyttävillä yksiköillä.

Haastateltavilta kysyttiin myös laitteisiin liittyvästä raportoinnista ja seurannasta. Lääketieteellisten laitteiden seuranta tapahtui organisaatioissa ohjelmistojen tai laitelistausten avulla, joiden kautta pystytään hallinnoimaan olemassa olevia laitteita. Haastateltava 3 kertoi haastattelussaan, että seurantajärjestelmä, joka pitää sisällään kaikki lääketieteelliset laitteet organisaatiossa, pitää sisällään suhteellisen kattavaa tietoa, mutta esimerkiksi haavoittuvuuksien seuraamista listauksessa ei ole mahdollista tunnistaa. Haastateltavan 4 mukaan tietyt vastuuhenkilöt tekevät raportointia, mutta lähinnä päivitysten muodossa eli jos jokin asia muuttuu, niin silloin vastuuhenkilöt päivittävät dokumentteja. Haastateltavan 3 mukaan vaaratilanteissa tulisi kirjata vaaratilannejärjestelmään tieto laitteesta. Haastateltavan 3 haastattelussa kävi kuitenkin ilmi, ettei vaaratilanteita todennäköisesti raportoida niin paljoa, kuin tapahtumia on ollut johtuen vaaratapahtuman johtamisesta laitteen käyttökieltoon. Haastateltavien kautta ei kuitenkaan saatu tietoa siitä, tapahtuuko organisaation sisäisesti lääketieteellisistä laitteista raportointia toisiin yksiköihin riskienhallinnan hallintamallin mukaisesti. Systemaattisesti raportointia ei kuitenkaan tapahdu, ellei dokumentteihin tule päivityksiä tai poikkeamia.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Käyttäjäorganisaation vastuut	Käyttöorganisaatiossa lääketieteellisten laitteiden kyberturvallisuudesta vastuu on tietohallinnolla, lääkintäteknikalla ja kliinisen työntekijöillä.	H1, H2, H3, H4, H5
	Käyttäjäorganisaatiossa kliininen työ ja käyttäjät ovat vastuussa lääketieteellisten laitteiden käytöstä.	H3, H4, H5
	Laitteiden seuranta ja raportointi kuuluu käyttäjäorganisaatiolle.	H3, H4

	Käyttäjäorganisaatiossa kliinisessä työssä käyttäjillä on vastuu laitteiden jatkuvuudesta ja käytön kehittämisestä.	H2
Laitevalmistajan ja -toimittajan vastuut	Laitevalmistajan vastuulla on valmistaa kyberturvallisia lääketieteellisiä laitteita.	H4
	Laitevalmistajan vastuulla on huolehtia laitteiden huolloista ja päivityksistä.	H4
	Laitevalmistajalla on vastuu ohjeistaa käyttäjiä ja tehdä ohjeistuksia.	H3
	Laitevalmistajan vastuulla on huolehtia laitteiden kyberturvallisuuden kehittämisestä.	H2, H4, H5
Palveluntoimittajien ja muiden kolmansien osapuolien vastuut	Palveluntoimittajilla on vastuu toimittaa lääketieteellisiin laitteisiin liittyvää sovittua ja määriteltyä palvelua kuten esim. verkon ylläpitoa ja tietoturvapoikkeamien havainnointia.	H3, H5
	Viranomaisorganisaatiot valvovat laitteiden rekisteröimistä ja käyttöä.	H3, H5
Laitteiden vastuisiin liittyvät haasteet	Lääketieteellisten laitteiden kyberturvallisuuden vastuut eivät ole selkeät käyttäjäorganisaatioissa.	H1
	Sovittujen prosessien ja protokollien toteuttaminen.	H1, H4
	Lääketieteellisten laitteiden kehitys tapahtuu laitetoimittajien kautta eikä käyttäjäorganisaatiot pysty vaikuttamaan laitteiden ominaisuuksiin suoraan.	H2, H4, H5
	Laitetoimittajat päättävät huolloista ja päivityksistä, sekä laitteeseen mahdollistettavista suojausmenetelmistä.	H4

Taulukko 16. Haastateltavien päähavainnot ja -nostot turvallisuuteen liittyvistä vastuista lääketieteellisten laitteiden osalta.

Vastuut hoitohenkilökunnan ja potilaiden informoisesta kyber- ja tietosuojariskeistä – Haastatteluista selvisi, että hoitohenkilökuntaa informoidaan yleisesti kyberturvallisuus- ja tietosuojariskeistä organisaatioiden toimintaan liittyen. Kuitenkaan kohdistettua kyberturvallisuuteen liittyvää informointia ei ole lääketieteellisiin laitteisiin. Haastateltava 1 kertoi haastattelussaan, että organisaation henkilökunnalle viestitään intran kautta materiaaleista ja uutisista, joita voidaan käyttää hyödyksi myös kyberturvallisuus- ja tietosuoja-aiheisten teemojen esiintuomisessa. Intran kautta ei kuitenkaan aktiivisesti viestitä erityisesti lääketieteellisten laitteiden riskeistä. Intra-uutisten lisäksi haastateltava 1 mainitsi myös mahdolliset seminaarit ja tietyille kohderyhmille järjestettävät tiedotustilaisuudet, joissa voidaan käsitellä kyber- ja tietosuojariskejä. Haastateltavan 4 mukaan kyberturvallisuuteen liittyvistä asioista ei juurikaan tiedoteta henkilökunnalle. Lisäksi haastateltava 4 koki lääketieteellisten laitteiden ja yleisesti kyberturvallisuusriskien tiedottamisen kuuluvan kliinisen työn tekijöille.

Organisaatioilla oli käytössä yleinen, pakollinen tietoturvakoulutus, joka kuului käytännössä kaikille organisaatioissa työskenteleville henkilöille. Haastateltava 4 kertoi henki-

lökunnalle osoitetun tietoturvakurssin sisältävän pääasiassa ohjeita turvallisesta käyttäytymisestä, tietokoneiden käytöstä ja poikkeamien ilmoitusprosessista. Lisäksi organisaatioissa pidettiin koulutuksia lääketieteellisten laitteiden käytöstä, jotka kattoivat asioita esimerkiksi sähkö- ja paloturvallisuudesta. Haastateltavan 5 mukaan kyberturvallisuus on laitekoulutuksissa otettu huomioon joidenkin esimerkkien avulla. Koulutettavilla henkilöillä on velvollisuutena opettaa ja kouluttaa muita henkilöitä omassa yksikössä.

Haastateltavien haasteena liittyen lääketieteellisten laitteiden kyber- ja tietosuojariskien tiedottamiseen oli huono näkyvyys ja tietoisuus klinisen puolen työstä ja siellä tapahtuvasta kyberturvallisuustoimista. Haastateltavat eivät osanneet juurikaan sanoa minkälaisia kysymyksiä potilailta tai hoitohenkilökunnalta tulee kyber- ja tietosuojariskeistä, jos niitä tulee ollenkaan. Haastateltava 3 mainitsi omassa haastattelussaan potilaiden kyselleen lääketieteellisiin laitteisiin liittyen tietosuojasta ja potilastietojen siirtymisestä laitteista järjestelmiin. Henkilökunnan keskusteluista ja kysymyksistä ei ollut tietoa, sillä keskustelut käydään klinisen työn yhteydessä. Haastateltavien mukaan varsinaisia kyberturvallisuusriskejä ei käsitellä lääketieteellisten laitteiden koulutuksissa eikä niitä käydä läpi tietoturvakoulutuksissa. Riskeistä voidaan kertoa joissakin tilaisuuksissa, mutta tiedottaminen ei ole säännöllistä tai systemaattista, ja niistä keskusteleminen perustuu henkilökunnan oman kiinnostuksen ja osaamisen varaan.

Haastateltavien havaintojen teemat	Haastateltavien päähavainnot	Maininnat
Kyberturvallisuus- ja tietosuojariskien viestiminen	Yleisistä riskeistä voidaan viestiä hoitohenkilökunnalle yleisten organisaatiokanavien kautta.	H1, H4
	Yleisistä riskeistä voidaan viestiä hoitohenkilökunnalle seminaareissa.	H1
	Yleisistä riskeistä voidaan viestiä tietyn kohderyhmän hoitohenkilökunnalle tiedotustilaisuuksissa.	H1
	Yleisistä riskeistä kerrotaan tietoturvakoulutuksessa.	H1, H4, H5
Laitteisiin liittyvistä kyberturvallisuus- ja tietosuojariskeistä viestiminen	Riskeistä voidaan kertoa laitekoulutuksissa.	H5
	Kliinisen työn ja opetuksen yhteydessä voidaan kertoa riskeistä.	H4, H5

Taulukko 17. Haastateltavien päähavainnot ja -nostot informoimisen vastuista hoitohenkilökunnalle ja potilaille kyber- ja tietosuojariskeistä.

Lääketieteellisten laitteiden listaukset ja seuranta - Kaikilla haastateltavilla organisaatioilla oli olemassa päivitetty listaukset lääketieteellisistä laitteista. Laitelistauksina toimivat laiterekisterit, jotka olivat ajantasaisia ja päivitettyjä listauksia organisaatioissa olevista lääkinnällisistä laitteista. Laiterekisterien sisältämien lääkinnällisten laitteiden nimien ja yksilöityjen tunnusten lisäksi rekistereissä säilytettiin tietoja esimerkiksi laitteiden

huoltohistoriasta ja iästä. Organisaatioiden välillä huomattu vaihtelu laiterekisterin sisältämien tietojen laajuus ja listauksen käyttötavat sekä -tarkoitukset erosivat jonkin verran toisistaan. Yhteenveto laiterekisterin käytöstä laitteiden listauksessa on taulukossa 19.

Haastateltujen organisaatioiden laiterekisterit sisälsivät perustiedoiltaan samoja asioita ja sisältöjä, mutta vaihtelivat muiden tietojen osalta organisaatioittain. Haastateltavien 4 ja 5 organisaatioiden laiterekisterien käytössä oli hyödynnetty ohjelmistoa tai järjestelmää. Haastateltava 5 kertoi hänen edustamansa organisaation kirjaavan lääketieteelliset laitteet osaksi rekisteriä, kun laitteet saapuvat tarkastusottopisteelle. Tarkastusottopisteellä laitteille suoritetaan testauksia esimerkiksi sähköturvallisuusmittauksilla ja yleisellä kuntotarkastuksella. Osana tarkastusta laite saa myös oman laitetunnuksen, jonka mukaan laitteet personoidaan laiterekisterissä. Haastateltava 1 puolestaan kertoi organisaation laiterekisterissä olevan erillinen osuus tietoverkkoon liitetyille lääketieteellisille laitteille. Näille laitteille on kirjattu myös erikseen esimerkiksi IP-osoitteet, WLAN-yhteydet ja dataportit, sekä kaikki muut tarvittavat tekniset tiedot.

”IT-verkotetuista lääkintälaitteista on erillinen lista, josta tarvittavat tiedot, esim. IP-osoitteet, WLAN-yhteydet ja dataportit löytyvät. Listan päivittäminen vaatii isoa ylläpitoa, mutta porttietoja tarvittaessa ja säätöjä tehdessä pystytään päivittämään ja kirjaamaan asetukset oikein.” – Haastateltava 1

Haastateltavan 1 organisaatiossa oli nähty vaivaa laiterekisterin rakentamiseen ja sen sisältöjen kirjaamiseen, mutta oli koettu organisaatiossa tarvittavana ja toimintaa helpottavana kehittämistoimenpiteenä. Haastateltava 1 kertoi laiterekisterin ylläpidon vaativan paljon työtä, sillä organisaatiossa kaikki laitteisiin liittyvät tiedot halutaan pitää päivitetynä yhdessä ja samassa paikassa niin, että tietoon voidaan luottaa ja sen olevan ajankohtaista. Tarkan listauksen ansiosta organisaatiossa on mahdollista selvittää nopeasti mihin kaikkialle tietty lääketieteellinen laite on yhteydessä. Näin organisaatiolla on myös hyvät mahdollisuudet kriisitilanteessa, esimerkiksi kyberhyökkäyksen yhteydessä, saada tietoon laiterekisteristä minkälaisia yhteyksiä ja verkkoyhteyksiä laitteilla on ja tehdä sen perusteella korjaavia toimenpiteitä.

Haastateltavien haavaintojen teemat	Haastateltavien päähavainnot	Maininnat
Laiterekisteri	Organisaatiolla on olemassa laiterekisteri tai -listaus.	H1, H2, H3, H4, H5
	Laiterekisterissä on olemassa listaus tietoverkkoon liitettävien laitteiden tiedoista ja yhteyksistä.	H1

Taulukko 18. Haastateltavien päähavainnot lääketieteellisten laitteiden rekistereistä ja niiden tiedoista.

Yhteenveto tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuista ja seurannasta – Haastattelujen päähavainnot eri alateemoista laitevalmistajien kanssa tehtävästä yhteistyöstä ja kyberturvallisuusriskien huomioinnista hankintojen yhteydessä on koottuna kuvaan 6. Kyberturvallisuuden vastuista lääketieteellisissä laitteissa ei ollut selkeää näkemystä tai toteutusta haastatelluissa organisaatioissa. Vastuita tunnistettiin kuuluvan käyttäjäorganisaatioissa tietohallinnon, lääkintätekniikan ja kliinisen työn henkilöstölle sekä laitetoimittajille ja kolmansille osapuolille.

Kyberturvallisuus- ja tietosuojariskien viestimistä tapahtui jollakin tasolla organisaatioissa, mutta laitteisiin liittyvästä riskien viemisestä haastateltavat eivät osanneet juurikaan sanoa. Laiteriskien viestiminen nähtiin kuuluvan osaksi kliinistä työtä, johon lääkintätekniikan ja tietohallinnon henkilöstöllä ei ollut näkyvyyttä. Yleisten kyberturvallisuus- ja tietosuojariskien informoimista voitiin tehdä organisaatioin yleisissä kanavissa, kertaluontoisissa tapahtumissa sekä osana yleistä tietoturvakoulutusta. Kaikissa haastatelluissa organisaatioissa oli käytössä laiterekisteri, jota pidettiin päivitettyinä listauksena laitteista. Organisaatioiden tavat vaihtelivat kirjattavien asioiden osalta laiterekisteriin.

Läketieteellisten laitteiden seuranta ja vastuut		
<p>Laitteisiin liittyvät vastuut:</p> <ul style="list-style-type: none"> • Käyttäjäorganisaation vastuut • Laitetoimittajan vastuut • Palveluntoimittajan vastuut • Muiden kolmansien osapuolien vastuut 	<p>Vastuut kyber- ja tietosuojariskien tiedottamisessa:</p> <ul style="list-style-type: none"> • Kyber- ja tietosuojariskeistä viestiminen • Laitteisiinkohdistuvien kyber- ja tietosuojariskien viestiminen 	<p>Laiterekisterit ja -listaukset:</p> <ul style="list-style-type: none"> • Organisaatioiden laiterekisterit ajankohtaisina laitelistauksina

Kuva 6. Yhteenveto haastateltavien nostamista aiheista tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuista ja seurannasta.

6. TULOsten ANALYSOINTI: KYBERTURVALLISUUDEN KEHITYSTARPEET JA TAVOITETILAN SAAVUTTAMINEN TIETOVERKKOON LIITETTÄVISSÄ FYYSISISSÄ LÄÄKINNÄLLISISSÄ LAITTEISSA

Tässä luvussa käsitellään tutkimuksen viidennen luvun haastattelutuloksista poimittuja keskeisiä päähavaintoja empiriasta yhdistettynä tutkimuskirjallisuuteen, jota on käsitelty tutkimuksen luvuissa kaksi ja kolme. Kuudennessa luvussa vastataan myös tutkimuskysymyksiin fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden riskienhallinnan, hallinnoimisen, havainnoinnin ja seurannan teoriasta nykytilahaastatteluiden tuloksiin. Aiempien lukujen perusteella on saatu kokonaisvaltainen näkemys tekijöistä, jotka vaikuttavat fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden hallinnointiin terveydenhuollon organisaatioissa. Tässä kuudennessa luvussa tuodaan esille näkemyksiä fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kokonaisvaltaiseen huomiointiin kyberturvallisuuden näkökulmasta terveydenhuollon organisaatioissa.

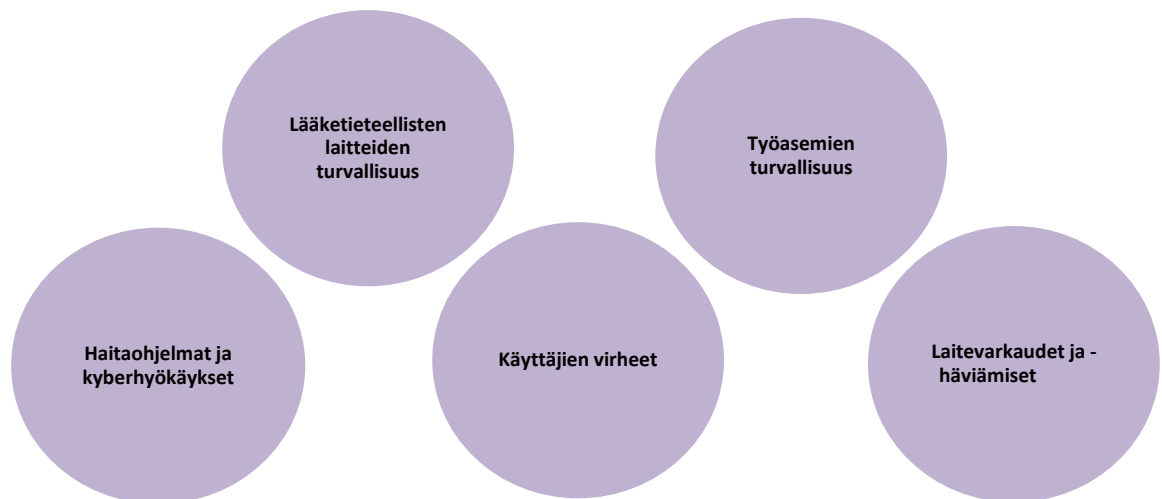
6.1 Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet ja niihin liittyvät riskit ja riskienhallinta

Kyberturvallisuuteen liittyvät riskit - Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden käyttö ja tarve ovat kasvaneet terveydenhuollon organisaatioissa ja erityisesti niin kutsutuissa älysairaaloissa (eng. smart hospitals) digitalisaation myötä. Tietoverkkoon liitettävyyden vuoksi fyysiset lääketieteelliset laitteet mahdollistavat laitteiden internet-yhteydellä kommunikoinnin muiden laitteiden ja järjestelmien kanssa sekä sitä kautta tietojen helpon siirtymisen ja saatavuuden. Kyberturvallisuuden näkökulmasta tietoverkkoon liitettävyys kohdistaa laitteisiin kyberfyysisen ympäristön uhkia ja riskejä. Laitteet ovat alttiita joutua manipuloinnin ja luvattoman käytön kohteeksi, ja siksi laitteita sekä niissä olevia tietoja tulee suojata (eHealth Suisse 2020, s.40).

Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden pääasialliset turvallisuusriskit voidaan jakaa kahteen pääkategoriaan – riskeihin, jotka liittyvät laitteiden sisältämien datojen joutumiseen väärin käsiin ja toisena riskeihin, jotka liittyvät laitteiden joutumista ulkopuolisten haltuun (Pöyhönen et al. 2019). Deloitte Center for Health Solutions (2013) mukaan tietoverkkoon liitettäviin lääkinnällisiin laitteisiin kohdistuu merkittäviä ky-

berturvallisuusriskejä, joita terveydenhuollon organisaatioiden tulee ottaa huomioon käytössä. Merkittävät riskejä tietoverkkoon liitettäville lääketieteellisille laitteille ovat sähkömagneettinen häirintä, testaamattomat tai vialliset laiteohjelmistot ja ohjelmat, laitevarkaudet ja laitteiden häviämiset, laitteiden turvallisuus, yksityisyys, asetusten luvaton muuttaminen, uudelleenohjelmointi tai haittaohjelmien tartunnat, palvelunestohyökkäykset sekä kyberhyökkäykset (Deloitte Center for Health Solutions 2013).

Haastattelututkimuksesta esille nousivat erityisesti riskit, jotka liittyvät ihmisen toimintaan, kyberhyökkäyksiin, tietoverkkoliikenteeseen, työasemiin ja fyysiseen turvallisuuden haastatelluissa organisaatioissa. Haastateluissa mainittiin laitevarkaudet ja laitteiden häviämiset, laitteiden turvallisuus, palvelunesto- ja kyberhyökkäykset, haittaohjelmat tai asetusten luvaton muuttaminen, käyttäjien virheet, tietoverkon ja sähköverkon kaatuminen, työasemien heikko suojaaminen, toimitilat, sisäisten prosessien ja suunnitelmien puuttuminen sekä kolmansien osapuolien toiminta. Kirjallisuudessa ja haastattelutuloksissa eniten mainitut riskit ovat kuvassa 7.



Kuva 7. Haastatteluista ja kirjallisuudesta nostetut isoimmat ja merkittävimmät riskit fyysisissä tietoverkkoon liitettävissä lääketieteellisissä laitteissa.

Tutkimuksen empiirisen osuuden, haastatteluaineiston läpikäynnistä voidaan havaita, että fyysisille tietoverkkoon liitettäville lääketieteellisille laitteille riskit ovat kokonaisuudessa samankaltaisia ja verrattavissa kirjallisuudessa mainitsemiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin. Kirjallisuudessa ja empiirisessä osuudessa tunnistettiin laitteisiin liittyviksi riskeiksi laitevarkaudet ja laitteiden häviämiset, laitteiden turvallisuus, palvelunesto- ja kyberhyökkäykset sekä haittaohjelmat ja asetusten muuttaminen. Kirjal-

lisuudesta löytyneitä testaamattomia tai virheellisiä laiteohjelmistoja ja sähkömagneettista häirintää ei suoraan haastatteluissa mainittu. Toisaalta haastatteluissa mainittiin laitteiden turvallisuus ja toimiminen, johon voidaan ajatella myös viallisten laiteohjelmistoiden kuuluvan. Sähkömagneettista häirintää ei haastatteluissa kerrottu, mutta sen sijaan eräs haastateltava nosti esille sähköjakelujärjestelmien toimimattomuuden ja kaatumisen välillisenä lääketieteellisten laitteiden riskinä. Yksityisyys mainittiin haastatteluissa uhkana potilastietojen eheyden ja saatavuuden sekä tietojen myymisen ja leviämisen näkökulmasta. Nämä haastattelumaininnat luokiteltiin kirjallisuuden yksityisyyden teemaan.

Riskienhallinta – Terveysthuollon organisaatioiden riskienhallintaa on pidettävä erityisen merkityksellisenä toimialan kriittisyyden näkökulmasta (Tapx Labs 2015). Laitteiden käyttäjinä, terveydenhuollon organisaatioiden tulisi kokonaisvaltaisen riskienhallinnan huolehtimiseksi ottaa lääketieteelliset laitteet osaksi käyttäjäorganisaatioiden riskienhallintaa ja sen prosesseja ja suunnitelmia. Lääketieteellisille laitteille tulisi tehdä kyberturvallisuuden uhkien ja haavoittuvuuksien hallitsemiseksi sekä turvallisuuden ja tehokkuuden edistämiseksi riskienhallintaa tulisi toteuttaa systemaattisesti ja arvioida riskejä sekä toteuttaa niihin hallintatoimenpiteitä koko käyttövaiheen ajan (IMDRF 2019).

Terveysthuollon organisaatioissa lääketieteellisille laitteille ei ollut omia riskienhallinnan prosesseja tai suunnitelmia käytössä. Käyttäjäorganisaatioita edustavat terveydenhuollon organisaatioiden haastateltavat kertoivat, ettei niillä ole lääketieteellisille laitteille omia riskienhallinnan prosesseja ja suunnitelmia. Lääketieteelliset laitteet nähtiin kuuluvaksi terveydenhuollon organisaation omaan riskienhallintaan eikä tarvetta omille prosesseille nähty järkeväksi toteuttaa. Organisaatioiden haastatteluista nousi kuitenkin tarve selkeyttää ja kehittää organisaation riskienhallintaa ja sen prosesseja lääketieteellisten laitteiden osalta. Erityisesti riskienhallinnan vastuut olivat epäselviä haastateltaville ja heidän työskentelemissä tiimeissä ja yksiköissä. Vastuiden epäselvyyden yhtenä syynä nähtiin yksiköiden välinen läpinäkymättömyys, vuoropuhelun puute sekä lääketieteellisten laitteiden nouseva kehityskulku, jota ennen laitteisiin ei kohdistunut digitalisaation tuomia haasteita esimerkiksi kyberhyökkäysten muodossa.

Digitaalisen kehityksen myötä fyysiset tietoverkkoon liitettävät lääketieteelliset tulisi ottaa käyttäjäorganisaatioissa huomioon kokonaisvaltaisessa riskienhallinnassa. Riskienhallintaan ei ole yhtä oikeaa tapaa toteuttaa, mutta käyttäjäorganisaatioiden tulisi kiinnittää huomiota systemaattiseen tekemiseen ja jatkuvuuden takaamiseen (IMDRF 2019). Terveysthuollon käyttäjäorganisaatioiden fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin liittyvät riskienhallinnan vastuut tulisi määritellä yhdessä tärkeimpien yksiköiden, useimmiten tietohallinnon, lääkintätekniikan ja klinisen työn osaston, kanssa.

Lisäksi nämä laitteet on otettava huomioon organisaation riskienhallinnassa ja huolehtia, että organisaatiossa on määritelty suunnitelmat ja parhaat käytännöt laitteisiin kohdistuvien suurimpien uhkien ja riskien toteutumisten varalta.

Riskien vaikutukset – Fyysiset tietoverkkoon liitettävät laitteet ovat terveydenhuollon organisaatioissa kyberfyysisessä ympäristössä. Kyberfyysisessä ympäristössä laitteisiin kohdistuu sekä digitaalisessa, että fyysisessä ympäristössä esiintyviä riskejä ja uhkia. Fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin kohdistuu yhä kehittyneempiä kyberhyökkäyksiä ja muita kybermaailman riskejä liitettävyytensä kautta. Fyysisessä ympäristössä näihin laitteisiin kohdistuu erityisesti toimitilojen ja ihmisten toiminnan kautta riskejä ja uhkia.

Toteutuneita kyberturvallisuusriskejä haastatelluista organisaatioista oli tapahtunut pääasiassa laitteiden varastusten ja häviämisten muodossa. Pääasiassa varastuksen kohteena olivat olleet pienet lääketieteelliset laitteet ja vain harvoja fyysisiä tietoverkkoon liitettäviä lääketieteellisiä laitteita oli hävinnyt haastatelluista organisaatioista. Yhdessä organisaatiossa oli tapahtunut lääketieteellisiin laitteisiin kohdistunut kyberhyökkäys, joka onnistui vaikuttamaan lääketieteellisten laitteiden käyttöön merkittävästi. Saastuneet laitteet oli huollettava tai ostettava uudet. Saastuneiden laitteiden korjaaminen ei välttämättä aina ole mahdollista, sillä ohjelmistot saattavat vaurioitua niin pahasti, ettei niitä pystytä korjaamaan.

Organisaatioissa toteutuneiden riskien määrän vähäisyyttä voi selittää se, että lääketieteelliset laitteet ovat kyberhyökkääjien kohteena suhteellisen uusia. Niihin kohdistettujen hyökkäysten kehittyessä tulee mahdollisista riskeistä olla kuitenkin tietoinen ja hyökkäysteekniikoiden kehittymistä seurata. Laitteiden haavoittuvuudet tulee paikata mahdollisimman nopeasti, jotta niitä ei pystytä hyödyntämään. Käyttäjäorganisaatiot olivat myös hyvin tietoisia tietoverkkojen turvallisuudesta ja kehittämisestä osana lääketieteellisten laitteiden suojausta. Fyysisen ympäristön riskeihin käyttäjäorganisaatiot ovat tottuneet ja niiltä osataan suojautua kokonaisvaltaisesti. Fyysinen ympäristö ja siellä tehtävät suojaukset ja varotoimet ovat tärkeä osa laitteiden riskienhallintaa, sillä laitevalmistajat hallinnoivat vahvasti itse laitteiden turvallisuutta. Toisaalta fyysisen ympäristön suojauksessa havaittiin myös puutteita ja paikkoja, jossa turvallisuuskeinoja tulisi parantaa erityisesti ihmisiin liittyvässä toiminnassa esim. huoltotapahtumissa, laitteen käytössä ja toimitiloissa toimimisessa. Fyysistä turvallisuutta tulisi toteuttaa kaikille laitteille ja komponenteille, vaikka se olisikin haastavaa toteuttaa käytännössä (Enisa 2016).

Lääketieteellisten laitteiden liitettävyyksien kehittyessä ja kyberrikollisten jatkuvasti etsiessä uusia keinoja tunkeutua terveydenhuollon organisaatioihin, voi lääketieteellisiin

laitteisiin kohdistua monenlaisia riskejä. Erilaiset riskit voivat johtaa erilaisiin haittoihin ja negatiivisiin vaikutuksiin. Fyysisessä ja digitaalisessa maailmassa on molemmissa riskejä ja uhkia, jotka voivat toteutuessaan aiheuttaa muun muassa maineelle, taloudelle ja potilashoidon turvallisuudelle haittaa. Luvussa 3.5.6 tuotiin esille erityisesti taloudelliset vaikutukset laitevarkauksien ja häviämisten osalta, sekä potilashoidon vaikutukset viivästyminä sekä mahdollisina tietojen menetyksinä (Enisa 2016).

Haastatteluista nousivat esiin erityisesti brändihaitat, potilasturvallisuuden vaarantuminen sekä taloudelliset ja laitteisiin kohdistuneet vaikutukset. Erityisesti potilasturvallisuuteen liittyvät vaikutukset koettiin haitallisimmiksi, jotka vaikuttavat organisaatioihin myös taloudellisesti ja negatiivisesti maineelle. Potilasturvallisuuteen liittyviksi riskeiksi nostettiin potilashoidon viivästyminen, virheellinen potilashoito ja potilastietojen väärentymiset ja päätyminen ulkopuolisten käsiin, jotka kaikki ovat vakavia riskejä toteutuessaan. Toisena isona teemana haastateltavat nostivat laitteiden riskit liittyen laitteiden toimimattomuuteen, virheelliseen toimintaan ja tietojen eheyden ja saatavuuden vaarantumiseen. Kaikki nämä laitteisiin liittyvät riskit vaikuttavat organisaatioihin myös taloudellisesti ja potilashoidollisesti.

Potilashoitoon liittyvät uhkat esiintyvät erityisesti digitaalisessa ympäristössä ja muodossa (Norri-Sederholm et al. 2019). Nämä uhkat liittyvät potilastietojen elektroniseen muotoon, jotka mahdollistavat potilastietojen mahdollisen myymisen, hallussapidon ja väärentämisen sekä virheellisen potilashoidon. Haastatteluissa ja kirjallisuudessa potilashoitoon ja -turvallisuuteen liittyviä vaikutuksia pidettiin merkityksellisimpinä ja vaarallisimpina mahdollisina seurauksina, sillä tällöin ihmisten terveys ja henki sekä henkilötietojen turvallisuus vaarantuvat. Potilasturvallisuuden lisäksi aineistoissa nousi esille laiteturvallisuus, joka liittyy vahvasti sekä taloudellisiin vaikutuksiin, että potilasturvallisuuteen. Kaikkiin lääketieteellisten laitteiden toteutuneisiin riskeihin liittyy myös vaikutus käyttäjäorganisaation maineeseen ja brändiin, joita ei voida sivuuttaa minkään riskien vaikutusten osalta.

Riskeiltä ja uhilta suojautuminen – Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden käytössä riskeiltä ja uhilta suojautuminen on tärkeää kyberturvallisuuden näkökulmasta. Laitteet voivat altistua manipuloinnille ja niihin voi kohdistua luvattomia pääsyjä, jolloin laitteita tulee suojata tunnistetuilta riskeiltä ja uhilta (eHealth Suisse 2020). Laitteita tulisi suojata niin, ettei niissä kulkevia tai sisältämiä tietoja eikä itse laite joutuisi ulkopuolisen haltuun (Pöyhönen et al. 2019). Lääketieteellisten laitteiden poikkeamien ja riskien realisoitumisten selvitystyö voi kestää kauan ja laitteiden selvitystyö voi vaikuttaa negatiivisesti potilashoitoon, mikäli selvitystyön ajaksi organisaatioon ei

saada uutta laitetta käyttöön. Laitteiden käyttökatkot voivat aiheuttaa viivästyksiä ja siten tuottaa ongelmia potilashoidon ja -turvallisuuden toteutumisessa (Tapx Labs 2015).

Laitteiden suojaamiseksi laitevalmistajien tulee kiinnittää huomiota riskeihin ja uhkiin jo suunnitteluvaiheessa (eHealth Suisse 2020). Laitteiden turvallisuusvalintoihin käyttäjäorganisaatiot pystyvät vaikuttamaan valitsemalla markkinoiden turvallisemman laitteen, mutta itse turvallisuuskomponentteihin ja -valintoihin käyttäjäorganisaatiot eivät pysty vaikuttamaan. Haastatteluaineistossa erityisesti tietoverkon suojaaminen, kolmansien osapuolien hallinta, hankinnat, organisaation sisäiset prosessit ja ihmisen toiminta nousivat esille riskeiltä ja uhilta suojautumisessa. Tietoverkon suojausta ja turvallisuutta pidettiin erityisen tärkeänä osa-alueena riskeiltä suojautumisessa, sillä fyysiset tietoverkkoon liitettävät lääketieteelliset laitteet ovat yhteydessä tietoverkkoihin. Tietoverkkojen kautta voidaan kohdistaa erilaisia kyber- ja palvelunestohyökkäyksiä, joten verkkojen suojaus ja jatkuva valvonta sekä kehittäminen on merkityksellistä. Tietoverkkojen suojaaminen liittyi myös osittain kolmansien osapuolien toimintaan, jolla on merkittävä vaikutus terveydenhuollon organisaatioiden sekä lääketieteellisten laitteiden turvallisuuteen. Terveydenhuollon organisaatiot olivat riippuvaisia joidenkin palveluiden osalta kolmansista osapuolista, jolloin vuorovaikutus, yhteistyö kehityksessä ja osaaminen kolmansien osapuolien kanssa on merkityksellisessä roolissa.

Haastateltavat tunnistivat riskeiltä ja uhilta suojautumisen erityisen tärkeäksi myös hankintojen osalta. Laitevalmistajilla on määritelty vahvat vastuut laitteiden hallinnointiin, huoltoihin, päivityksiin sekä kehitysvaiheessa valittujen turvallisuusominaisuuksien osalta (Tapx Labs 2015). Käyttäjäorganisaatioilla on mahdollisuus vaikuttaa laitteiden turvallisuuteen hankintaprosessissa, jossa organisaatiot määrittelevät laitevaatimukset, tietosuojaj- ja tietoturvaliitteen sekä valitsevat laitevalmistajan tai -toimittajan, jolta laite tilataan. Hankintojen ja laitteiden kehittämiseksi tulisi valmistajien kanssa tehdä jatkuvaa yhteistyötä ja markkinakatsauksia laitteiden kehittymisen näkökulmasta. Organisaation hankintaprosessit yhdessä muiden lääketieteellisiin laitteisiin liittyvien prosessien, kuten riskienhallinnan prosessin ja sen suunnitelmien, nostettiin haastatteluissa esille riskeiltä suojautumiseksi. Prosessien ja suunnitelmien puuttuminen lääketieteellisten laitteiden osalta ovat iso haaste mahdollisen riskin tai uhan toteutuessa. Prosesseissa ja suunnitelmissa tulisi määritellä vastuut ja toimenpiteet mahdollisen riskin toteutuessa, jotta tilannetta pystyttäisiin lähtä hoitamaan mahdollisimman nopeasti oikeilla tavoilla päämäärätietoisesti.

Riskeiltä ja uhilta suojautumista hidastaa ja haasteena nähdään terveydenhuollon käyttäjäorganisaatioissa laitteiden suuri käyttöaste (Tapx Labs 2015). Suuri käyttöaste voi johtaa siihen, ettei laitteiden vikaantumista ilmoiteta ja niiden korjaamista ja päivitys- ja

huoltotapahtumia viivytetään, jotta laitteita voitaisiin käyttää potilashoidossa. Vikailmoitusten ilmoittamattomuus voi johtua ihmisten laitekoulutusten puutteista sekä tietämättömyydestä. Ilmoittamatta jättämien vikailmoitusten lisäksi myös pitkät korjausajat voivat haastaa potilasturvallisuuden toteutumisen, mikäli organisaatiot eivät saa korvaavia laitteita.

Riskeiltä ja uhilta suojautuminen ennakoivasti on merkityksellistä potilasturvallisuuden ja -hoidon takaamiseksi. Merkityksellisemmät tavat käyttäjäorganisaatioilla suojautua riskeiltä ovat erityisesti hankintojen yhteydessä tehtävät vaatimukset, tietoturvaliitteet, yhteistyö laitevalmistajien kanssa sekä turvallisten laitteiden hankkiminen. Hankittavat laitteet määrittävät hyvin pitkälti tietoverkon suojaamiseen liittyviä vaatimuksia ja koulutuksia, joiden kautta käyttäjäorganisaatiot pystyvät vaikuttamaan laitteiden turvallisuuteen hankinnan jälkeen. Toisena merkittävänä riskeiltä suojaavana tekijänä on tietoverkkojen suojaaminen, jolla käyttäjäorganisaatio pystyy vaikuttamaan konkreettisesti fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden turvallisuuteen.

Alateema	Kirjallisuus	Kirjallisuus ja haastattelut	Haastattelut
Riskit			
Ihmisten toiminta	Huolimattomuus työssä, salasanaikäytännöt ja salasanojen hallitsematon jakelu, sosiaalinen manipulointi, viestintä, USB- ja muistitikojen käyttö, asetusten luvaton muuttaminen	Laitevarkaudet ja laitteiden häviäminen, käyttäjä- ja potilasturvallisuutta vaarantava käyttö	
Kyberhyökkäykset	Kalasteluviestit	Kiristys- ja haittaohjelmat, troijalaiset, palvelunestohyökkäykset	Madot
Tietoverkko-liikenne, viestintä ja järjestelmät	Väärennetyt koodit, väärentäminen ja jäljittely, toistaminen, tietokantainjektiot, testaamattomat ohjelmat, verkko- ja laiteviestinnän häiriöt, avoimet ja käyttämättömät viestintäportit laitteissa, asetusten uudelleenohjelmointi, tietoturvaaukot ja haavoittuvuudet	Verkon kaatuminen, huonot suojaamistavat ja käytännöt. Iuston pääsy tietoverkkoihin	

Työasemat, laitteet ja käyttöoikeudet	Käyttöoikeuksien eskalointi, päivitysten ja korjauksien tekemättömyys tai myöhässä toimittaminen	Työasemien heikko suojaaminen ja turvallisuus	
Fyysinen turvallisuus	Laitteiden tuhoaminen, sähkömagneettinen häirintä	Toimitilat	Sähkönjakelujärjestelmät
Riskien vaikutukset ja toteutumiset			
Brändihaitat			Mainehaitta
Potilasturvallisuus		Tietojen eheyden ja saatavuuden vaarantuminen, potilashoidon viivästyminen, virheellinen potilas hoito, potilastietojen väärentäminen, myyminen ja hallussapito	
Taloudelliset vaikutukset			Uusien laitteiden hankkiminen, saastuneiden korjaaminen, potilaiden menettäminen kilpailija-organisaatioille
Laitteisiin kohdistuvat vaikutukset		Laitteiden toimimattomuus, virheellinen toiminta	
Uhilta ja riskeiltä suojautuminen			
Tietoverkon suojaaminen		Verkon tekniset suojaukset, yhteistyö verkon toimittajien kanssa	Työkalujen ja ohjelmien sekä analytiikan käyttö, ISO-standardoitu verkko
Kolmannet osapuolet	Riskien arviointi, riskienhallinnan tehokkuuden valvominen, laitevalmistajien ohjekirjat	Yhteistyö kolmansien osapuolien kanssa, laitevalmistajien riskienhallinnalliset toimet, laitevalmistajien päivitykset ja korjaukset	
Hankinnat		Hankintaprosessin kehittäminen, yhteistyö hankintojen yhteydessä, organisaation sisäinen yhteistyö ja vuorovaikutus	Vastuullisen laitetoimittajan valinta, vaatimustilaston ylläpito, tietoturvaliitteen ylläpito
Ihmisten toiminta	Kyberturvatietoisuuden ja käyttäytymisen tukeminen	Tietoturvakoulutukset	

Taulukko 19. Vertailu kirjallisuudessa ja haastatteluissa mainituista kyberturvallisuusriskienhallinnasta, riskeistä sekä niiltä suojautumisesta.

6.2 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden arviointi, valvonta ja hallinta

Laitteiden turvallisuuden arviointi ja validointi – Lääkinnällisiin laitteisiin kuuluvia fyysisiä tietoverkkoon liitettäviä lääketieteellisiä laitteita sekä niiden turvallisuutta pyritään huomioimaan lääkintälaitteasetuksella liittyen laitteiden turvallisuusasetuksiin. Laitteiden turvallisuuden kehittämisellä ja edistämällä voidaan estää kyberturvallisuuteen liittyviä riskejä tietoverkkoon liitettävien lääketieteellisten laitteiden käytössä (Deloitte Center for Health Solutions 2013). Laitteiden turvallisuuden kehittämisessä sekä arvioinnissa on huomioitava erityisesti turvallisuusriskit, jotka liittyvät laitteiden joutumiseen ulkopuolisten käsiin sekä laitteisiin liittyvän datan päätyminen ulkopuolisille (Pöyhönen et al. 2019).

Laitteiden turvallisuuden arviointia ja validointia tapahtuu pääasiallisesti hankintaprosessissa. Hankintaprosessissa turvallisuuden arviointia tapahtuu laitteiden tarpeisiin, turvallisuuteen ja teknisiin ominaisuuksiin liittyen. Tietoverkkoon liitettävien laitteiden turvallisuuden arviointiin voidaan käyttää myös teknisen tietoturvan erityisasiantuntijoita ja palveluntarjoajia apuna. Asiantuntijoiden arvioinneilla voidaan sanallisesti ja pisteyttämällä arvioida riskien suuruutta, jonka arvosta riippuen laitteille voidaan toteuttaa erityistoimenpiteitä. Haastattelujen perusteella tallaisista arvioinneista puhuttiin yhden organisaation osalta, jossa arviointien tekeminen koettiin hyväksi turvallisuuden arviointitavaksi osana hankintaprosessia.

Erilaisilla prosessiin sisällytettävillä arvioinneilla voidaan luokitella lääketieteellisiä laitteita ja niiden ominaisuuksia sekä tarpeita, ja toimivat siksi hyvinä arviointitapoina terveydenhuollon organisaatioissa hankintojen yhteydessä. Organisaatioiden olisi hyvä tehdä arviointia valitsemallaan tyyllillä, jota käytetään esimerkiksi muiden riskien luokitteluun. Hankintojen yhteydessä laitevalmistajaan kohdistetaan tiettyjä vaatimuksia laitteiden omien vaatimusten lisäksi. Laitevalmistajalta voidaan vaatia esimerkiksi sertifikaatteja ja lausuntoja, jotka tukevat laitevalmistajien kyvykkyyksiä kehittää ja valmistaa turvallisia laitteita.

Käyttöönoton yhteydessä lääketieteellisten laitteiden turvallisuutta arvioidaan pääsääntöisesti laitetestausten avulla. Organisaatioista riippuen käyttöönoton yhteydessä tapahtuvien testauksien määrässä, laadussa ja tyypeissä on eroavaisuuksia. Käyttöönoton jälkeen käyttövaiheessa tehtäviä turvallisuuden validointeja tai arviointeja ei haastateltavissa organisaatioissa tehty juurikaan. Turvallisuuden arviointi keskittyy laitevalmistajien

tekemiin yleisiin haavoittuvuusilmoituksiin sekä mahdollisiin laitteiden päivityksiin ja huoltoihin.

Laitteiden ympäristöön tehtäviä arviointeja terveydenhuollon organisaatiot voivat kuitenkin toteuttaa ja tehdä ilman laitevalmistajien määräytyksiä, ja monet haastateltavat organisaatiot kertoivat tehneensä palveluntarjoajien avustuksella erilaisia verkkoon liittyviä arviointeja ja testauksia. Verkon turvallisuuden arviointi ja validointi on yksi terveydenhuollon organisaatioiden tärkeimmistä keinoista arvioida laitteiden käytön turvallisuutta, sillä vastuu ja roolitus tietoverkkojen osalta on selkeä. Tietoverkkojen ulko- ja sisäverkkojen skannauksilla, penetraatiotestauksilla sekä testiverkkojen rakentamisella organisaatiot ovat pystyneet varmistamaan lääketieteellisten laitteiden yhteyksien turvallisuutta. Verkkojen testaamista suoritettiin erilaisin tavoin ja syklein riippuen organisaatiosta – organisaatiot suorittivat testaamista käyttöänon aikana, mutta myös jonkin verran käytön aikana.

Käyttäjäorganisaatioiden hankintaprosessissa suoritettavien tietoturva-arviointien tapoja on syytä kehittää ja katselmoida säännöllisesti uusien mahdollisten vaatimusten näkökulmasta. Tietoturva-arviointien tapoja ja seurauksia tulee samassa yhteydessä huomioida. Käyttäjäorganisaatioiden avuksi on luotu lääketieteellisille laitteille lista tietoturva- ja tietosuojavaatimuksista, joita käyttäjäorganisaatiot voivat käyttää pohjana omille vaatimuksille. Lista on tuotettu yhdessä Tampereen yliopiston ja Tampereen teknillisen korkeakoulun Kyber-terveys-hankkeeseen ja Huoltovarmuuskeskuksen COREQ-VE teollisuusautomaation tietoturvahankkeeseen perustuen (Kyberturvallisuuskeskus 2022; Soten hankintojen tietoturva- ja tietosuojavaatimukset). Monet haastateltavat organisaatiot olivat käyttäneet listaa jollakin tavalla omien vaatimuslistojen luomiseen tai tehneet yhteistyötä Kyberturvallisuuskeskuksen kanssa muuten. Tällaisten vaatimuslistojen ja yhteistyömuotojen avulla käyttäjäorganisaatiot voivat luoda hyvien käytäntöjen pohjalle perustuvia vaatimuksia laitevalmistajalle ja tukea turvallisten laitteiden hankkimista. Vaatimuslistojen luomisen lisäksi listoja tulisi päivittää vuosikellon mukaisesti.

Käyttöäonotossa organisaatioiden tulee varmistua riittävästä turvallisuuden arviointitoimista esimerkiksi testauksien avulla. Organisaatioiden tulisi tehdä verkon skannauksia ja testauksia säännöllisesti ja systemaattisesti, jotta organisaatioiden verkkoturvallisuus olisi hyvällä tasolla lääketieteellisten laitteiden yhteyksien osalta. Säännöllisyyden tulisi perustua esimerkiksi vuosikellon mukaiseen toimintaan ja linkittää osaksi muita arviointeja ja testauksia. Käyttövaiheen tietoturva-arviointeja voisi olla syytä tehdä erityisesti tietoverkkoyhteyksien näkökulmasta esimerkiksi tietoverkkojen skannauksien säännöllisi-

sillä jatkamisilla. Käyttövaiheessa laitteiden tietoturvatestaamista voi haastaa laitevalmistajien määräykset, jolloin niistä olisi syytä käydä keskusteluja laitevalmistajien kanssa tulevaisuusnäkökulmasta.

Haavoittuvuuksien hallinta – Laitevalmistajilla on velvollisuus sisällyttää haavoittuvuuksien tunnistamista riskienhallintaan (AAMI TIR57:2016). Laitevalmistajien tekemillä haavoittuvuuksiin liittyvillä parhailla käytännöillä, tietojen jakamisella ja suunnittelulla on merkityksellinen rooli lääketieteellisten laitteiden turvallisuuden edistämässä (IMDRF 2019). Haastateltavat organisaatiot kertoivat laitevalmistajien vastuista haavoittuvuuksien informoimisesta laitteiden käyttäjäorganisaatioille. Haavoittuvuuksien tiedottamisen lisäksi laitevalmistajien ja -toimittajien vastuulla on luoda haavoittuvuuksien paikkaamiseksi ohjeet käyttäjäorganisaatiolle tai laitevalmistajat päivittävät itse haavoittuvuuksiin liittyvät laitteet esimerkiksi etäyhteyden avulla. Ohjelmistoihin itsessään ei tehdä juurikaan päivityksiä laitteiden käyttövaiheessa.

Laitevalmistajien lisäksi myös käyttäjäorganisaatiot tekevät haavoittuvuuksien hallintaa käyttövaiheessa. Käyttäjäorganisaatiot toteuttavat omaa haavoittuvuuksien hallintaa tietoturvan toimintana ja päivittävät omien syklien mukaisesti verkkoja ja esimerkiksi Microsoftin palveluiden päivityksiä. Lisäksi organisaatiot ovat pystyneet laitevalmistajien määritysten mahdollistamissa raameissa asentaa tietoturvaohjelmia ja -komponentteja esimerkiksi laitteisiin liitettyihin työasemiin.

Käyttäjäorganisaatioille yleistä on palveluntoimittajien käyttäminen tietoturvapalveluihin, joiden toimittajasopimukseen voidaan sisällyttää myös haavoittuvuuksien hallinnan vastuuta ja rooleja. Terveystieteiden organisaatioilla tietoturvapalvelukeskuksen (SOC) palveluihin sisältyy haavoittuvuuksien hallintaa ja koordinoitua. Palveluiden sisällöt vaihtelivat organisaatioiden välillä riippuen solmitusta sopimuksesta ja siihen kirjoitetuista vastuiden määrittelyistä. Tietoturvapalvelukeskuksen palvelut kattavat ison osan käyttäjäorganisaatioiden haavoittuvuuksien hallintaa, jolloin palveluiden laatuun ja määrään sekä niihin liittyvään yhteistyöhön panostaminen on merkityksellistä haavoittuvuuksien hallitsemiseksi. Haavoittuvuuksien hallinnoimiseksi palveluntarjoajalla ja käyttäjäorganisaatiolla on hyvä olla säännöllisiä palavereita sekä selkeät kommunikoimis- ja toimintatavat eri tasoille haavoittuvuuksille ja löydöksille.

Haavoittuvuuksien hallitsemiseksi laitevalmistajien, käyttäjäorganisaatioiden ja mahdollisten kolmansien osapuolien, kuten tietoverkkojen palveluntarjoajat, tulee tehdä yhteistyötä (Norri-Sederholm et al. 2019). Tilannekuvaa ja -tietoisuutta voidaan organisaatiossa parantaa terveydenhuollon organisaatioiden välisellä yhteistyöllä. Organisaatiot kertoivat yhteistyötä tehtävän vahvasti palveluntarjoajien kanssa sekä satunnaisemmin

muiden terveydenhuollon organisaatioiden ja muiden kolmansien osapuolien kanssa, kuten esimerkiksi Kyberturvallisuuskeskuksen kanssa. Sosiaali- ja terveysalalla yhteistyötä on pyritty lisäämään viimeisten vuosien aikana verkostomaiseksi toiminnaksi ja esimerkiksi Kyberturvallisuuskeskus fasilitoi muutamia verkostoja, joihin terveydenhuollon organisaatioissa työskentelevät asiantuntijat voivat hakeutua (Kyberturvallisuuskeskus 2023).

Terveydenhuollon organisaatioiden on kannattavaa etsiä ja hakeutua verkostoihin sekä luoda yhteistyökumppanuussuhteita laitevalmistajien ja palveluntarjoajien lisäksi myös muiden terveydenhuollon organisaatioiden kanssa, jotta tieto haavoittuvuuksista ja mahdollisista uhista voisi kulkeutua kansallisia ja kansainvälisiä verkostoja pitkin saavuttaen käyttäjäorganisaatiot mahdollisimman nopeasti. Haastateltavat organisaatiot kokivat yhteistyön hyödylliseksi ja pääsääntöisesti kokivat sen lisäämisen ja kehittämisen kannattavaksi. Yhteistyöstä hyötyvät kaikki osapuolet, kun kaikki jakavat saamiaan tietoja, jolloin myös haavoittuvuuksien paikkauksiin ja korjauksiin voidaan reagoida nopeasti jopa ennen laitevalmistajien toimia.

Pääsynhallinta ja -valvonta – Tietoverkkoon liitettävät fyysiset lääketieteelliset laitteet ovat riskialttiita manipuloinnille ja luvattomille pääsyyille. Riski luvattomiin pääsyihin on kohonnut näillä laitteilla tietoverkkoon liitettävyytensä vuoksi, minkä takia tietojen suojaaminen tulee taata vahvoilla turvallisuuskeinoilla ja -ratkaisuilla. (eHealth Suisse 2020) Pääasiassa laitteiden pääsynhallinta tapahtuu laitteisiin tai niiden työasemiin kirjautumalla, jolloin käyttäjät kirjautuvat tunnuksella laitteeseen. Potilashoidon käytön lisäksi pääsynhallintaa ja -valvontaa tulee toteuttaa laitevalmistajien huolto- ja päivitystapahtumissa, jolloin laitevalmistajat ottavat etäyhteyden kautta yhteyttä laitteeseen päästäkseen tekemään huoltoa tai päivitystä. Terveydenhuollon organisaatioiden tavat hallita laitevalmistajien ja palveluntarjoajien pääsyä laitteisiin olivat erilaisia ja laite- ja organisaatiokohtaisesti. Organisaatiot kertoivat laitteisiin muodostettavien etäyhteyksien erilaisista muodostumistavoista. Jotkut organisaatiot ja laitteet hyväksyivät kerran hyväksytyä etäyhteyden muodostamisen tulevaisuudessa ja jotkut puolestaan vaativat jokaisella etäyhteyden muodostamiskerralla tehtävän erillisen hyväksymisen.

Lääketieteellisten laitteiden pääsynhallinnallisiin ja -valvonnan ominaisuuksiin sekä ratkaisuihin pystytään vaikuttamaan parhaiten laitteiden suunnittelu- ja kehitysvaiheessa. Suunnitteluvaiheessa laitevalmistajien vastuulla on määritellä riittävät pääsynhallinnalliset ratkaisut ja suojaukset sekä liittää ne osaksi laitteiden kokonaisriskienhallintaa (eHealth Suisse 2020). Laitteisiin on sovellettava käytettäväksi hyviä kyberturvallisuuskäytäntöjä liittyen verkkoliikenteen pääsynvalvontaan, käyttövaltuus- ja kulunvalvonta-

toimenpiteisiin ja korjausten, päivitysten ja huoltojen toteuttamiseksi (IMDRF 2019). Laittevalmistajien tulisi suunnitella ja valmistaa laitteisiin mahdollisimman tietoturvallisia kirjautumiskäytäntöjä käyttämällä korkeimpia mahdollisia kirjautumistapoja. Laitteisiin tulisi mahdollistaa kirjautuminen henkilökohtaisilla tunnuksilla ja priorisoida niiden käyttöä yli yhteiskäyttötunnusten tai tunnuksittomien kirjautumisten. Henkilökohtaisten tunnusten käytön etuna on myös lokitietojen hallinnoiminen ja oikeellisuus.

Pääsynhallinnassa on otettava huomioon myös fyysinen pääsynhallinta laitteiden osalta toimintaympäristössä (IMDRF 2019). Fyysisen ympäristön pääsynhallinnassa on pyrittävä toteuttamaan pääsynhallintaa niin, etteivät ulkopuoliset pystyisi pääsemään laitteiden kanssa tekemisiin ollenkaan ilman terveydenhuollon ammattilaisia ja hoitotarvetta. Terveydenhuollon organisaatiot toteuttivat fyysistä pääsynhallintaa kulunhallinnan avulla sekä sijoittamalla laitteet niin, etteivät ulkopuoliset pääsisi niihin käsiksi. Hyvällä kulunvalvonnalla ja laitteiden sijoittamisilla voidaan myös ehkäistä laitevarkauksia ja -häviöitä. Kulunvalvonnan toteuttamisen lisäksi henkilökuntaa tulee kouluttaa säännöllisesti fyysisen ympäristön turvallisuuskäytännöistä, jotta kulunvalvonta toteutuisi. Henkilökunnan yleisen, pakollisen tietoturvakoulutuksen lisäksi henkilökuntaa tulisi muistuttaa ja informoida turvallisuuskäytännöistä myös laitekoulutuksissa ja systemaattisesti.

Pääsynhallinnan ja -valvonnan kehittämiseksi on tehtävä yhteistyötä ja jatkuvaa kehitystyötä oman organisaation sisällä muun muassa riski- ja tietoturva-arviointien avulla sekä laitevalmistajien kanssa. Arviointien perusteella voidaan tehdä pääsynhallintaan liittyviä toimia kriittisyyden kautta. Terveydenhuollon organisaatioiden tulisi suosia laitehankinnoissaan uudempiä ja tietoturvallisesti kehittyneempiä lääketieteellisiä laitteita, joiden pääsynhallinnalliset ominaisuudet ovat kehittyneempiä ja tietoturvallisia käytäntöjä tukevia. Pääsynhallinnan ja -valvonnan turvallisuuteen voivat vaikuttaa esimerkiksi laitteiden päivityksien laiminlyöminen ja puutteellisuus (Piggin 2017). Haavoittuvuuksien hallinnan ominaisuuksia tulee sisällyttää myös laitehankintojen vaatimukseen ja luoda riskejä vähentäviä toimia, mikäli laitevaatimuksista joudutaan osittain luopumaan, mikäli markkinoilla olevien laitteiden ominaisuudet eivät täsmää käyttäjäorganisaatioiden vaatimukseen. Esimerkiksi mikäli laitteissa käytetään yhteiskäyttötunnuksia, tulisi henkilökuntaa kouluttaa tunnuksien käyttämisestä ja säilyttämisestä mahdollisimman tietoturvallisesti.

Turvallisuuspoikkeamien hallinta ja havainnointi – Terveydenhuollon organisaatiot tekevät turvallisuuspoikkeamien hallintaa ja havainnointia omassa toimiympäristössään. Tyypillisesti terveydenhuollon organisaatiot tekemä turvallisuuspoikkeamien havainnointi tapahtuu yhdessä palveluntarjoajien kanssa, sillä harvalla organisaatiolla on sisäisiä resursseja ja oikeanlaista osaamista toteuttaa turvallisuuspoikkeamien hallitsemi-

sesta kokoaikaisesti 24/7-toimena. Ulkopuolisten palveluntarjoajien kautta turvallisuuspoikkeamien hallintaa saadaan palveluna ja terveydenhuollon organisaatioilla on käytössä ohjelmistoja ja näkyvyys palveluntarjoajien kautta poikkeamatapahtumiin. Turvallisuuspoikkeamien hallintaan liittyen organisaatioilla on säännöllisiä kokouksia poikkeamien läpikäyntiin.

Tärkeässä osassa turvallisuuspoikkeamien havainnointia ja hallinnointia on myös käyttäjien tekemät ja ilmoittamat poikkeamahuomiot. Poikkeaman tai epätavallisen tapahtuman huomioiminen ja tunnistaminen lääketieteelliseen laitteeseen liittyen tulee ilmoittaa organisaation käytäntöjen mukaisesti eteenpäin oikealle taholle. Nopea poikkeaman tunnistaminen ja hallinnointi tukee mahdollisen kyberturvallisuuspoikkeaman, kuten esimerkiksi kyberhyökkäyksen tai vikatilän, selvitystä ja riskien torjumista (Enisa 2016). Laitteiden kanssa työskentelevän henkilökunnan sekä potilaiden kouluttaminen ja informoiminen laitteiden normaalin toiminnan ja mahdollisten poikkeamien tunnistamisesta sekä niiden ilmoitusprosessista on merkityksellinen osa fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden turvallisuuspoikkeamien hallintaa. Erityisesti laitteita käyttävä henkilökunta on vastuussa ilmoittaa havaitsemistaan poikkeamista, vaikka huomioiden ilmoittaminen toisikin lisätyötä ja hidastaisi potilashoidon toteutumista. Poikkeamatilanteiden eskaloituessa esimerkiksi mahdollisen kyberhyökkäyksen myötä potilasturvallisuus on vaarassa esimerkiksi potilastietojen päätyemisessä ulkopuolisten käsiin tai laitteiden saastuminen. Poikkeamien toteutuessa riskit ovat suuria lääketieteellisten laitteiden kanssa, jonka takia poikkeamatilanteet tulee ottaa vakavasti ja laitteiden käyttäjien tulee olla tietoisia laitteiden normaalista toimimisesta sekä mahdollisten vika- ja poikkeamatilanteiden tunnistamisesta.

Organisaatioissa tietoliikenteiden hallinnointi ja havainnointi on usein hoidettu terveydenhuollon organisaatioissa selkeänä kokonaisuutena palveluntarjoajien avulla, mutta ihmisten kautta tapahtuva poikkeamien tunnistus vaatii terveydenhuollon organisaatioiden sisäistä kouluttamista. Terveydenhuollossa ihmisen toimintaan kohdistuu erilaisia kyberuhkia yleisesti alasta riippumatta sekä terveydenhuollon toimialaan erityisesti kohdistuen (Norri-Sederholm et al. 2019). Ihmisten toimintaan kohdistuvia riskejä ja uhkia voidaan parhaiten vähentää kouluttamalla henkilökuntaa oikeanlaisesta käyttäytymisestä sekä tiedottaa mahdollisista kyberriskeistä. Haastattelujen perusteella organisaatioiden painopiste on tietoverkkojen tunnistuksessa ja konkreettisesti potilastyössä laitteiden poikkeamatoimintaa katsotaan läpi sormien kliinisen työn toteuttamiseksi. Koulutuksen määrästä ja sisällöstä myös lääketieteellisten laitteiden osalta tulisi varmistua, jotta hen-

kilökunta osaisi tunnistaa poikkeamat ja tehdä koulutusta säännöllisesti. Erityisesti lääkintätekniikan, tietoturvan tai tietohallinnon ja klinisen työn osaajien tulisi yhdessä luoda ja määritellä koulutussisältöjä myös kyberturvallisuuden näkökulman kattamiseksi.

Haastatteluissa organisaatiot olivat selkeästi sitä mieltä, että lääketieteellisten laitteiden turvallisuuspoikkeamien hallinnointi ja havainnointi tulee olla osana terveydenhuollon organisaatioiden muitakin tietoturvapoikkeamien havainnointia. Lääketieteellisten laitteiden poikkeamissa käytetään pääsääntöisesti muidenkin tietoturvapoikkeamien tapaan samoja prosesseja ja yleisiä käytäntöjä. Näitä prosesseja on kuitenkin hyvä tarkastella lääketieteellisten laitteiden näkökulmasta ja siitä, tukevatko ne laitteiden poikkeamailmoituksia. Lääketieteellisten laitteiden poikkeamiin liittyen on kuitenkin hyvä määritellä, minkälaiset poikkeamat kulusivat mihinkin kriittisyysluokkaan ja minkälaiset poikkeamat voisivat käynnistää MIM-prosessin eli laajavaikutteisen häiriön prosessin.

Toimintamallit kyberuhan tai -haavoittuvuuden realisoituessa – Laitteiden turvallisuudesta huolehtimisen lisäksi lääketieteellisille laitteille tulee määritellä toimintamallit potentiaalisten kyberuhkien tai -haavoittuvuuksien realisoitumisten varalle. Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden riskienhallinnassa tulee ottaa huomioon laitteiden mahdolliset riskien realisoitumiset sekä luoda ja määritellä suunnitelmat ja tarvittavat toimenpiteet niiden varalta. Toimintamalleja ei kuitenkaan tulisi erottaa organisaatioiden muista riskienhallinnallisista toimista ja suunnitelmista, vaan kytkeä ne muihin organisaation toipumisen, jatkuvuuden ja varautumisen suunnitelmiin.

Organisaation toimintamallit uhkien ja riskien toteutumisessa tulee määritellä tarvittavalla tasolla ja tavalla. Uhkien ja haavoittuvuuksien realisoitumisia varten organisaation tulee luoda varautumissuunnitelma, jossa vastuut ja roolit ovat selkeästi määriteltyjä. Määrittelyjen lisäksi vastuista tulee kommunikoida selkeästi vastaavien henkilöiden kanssa sekä mahdollisuuksien mukaan harjoitella uhkien realisoitumisia vastuuhenkilöiden kesken. Suunnitelmissa tulisi ottaa erityisesti huomioon teknisistä ratkaisuista ja suojauksista huolimatta jäljelle jääviä riskejä, jotka voivat olla todennäköisimmiksi tunnistettuja laitteisiin liittyviä riskejä. Riskien huomiointia tulisi käydä läpi ja päivittää säännöllisesti ja ottaa osaksi organisaation yhtenäisiä suunnitelmia, toimintatapoja ja prosesseja (Pöyhönen et al. 2019).

Toimintamallien ja suunnitelmien harjoitusten avulla vastuiden toteutumista ja määriteltyjä toimintatapoja voidaan kokeilla luodussa ympäristössä turvallisesti. Harjoituksen jälkeen suunnitelmiin voidaan tehdä kehitystoimenpiteitä ja muuttaa rooleja ja vastuita tarpeen mukaan. Haastatteluiden perusteella joitakin harjoituksia oli tehty organisaatioiden sisäisesti, mutta harjoitukset eivät olleet suoraan liittyneet lääketieteellisiin laitteisiin.

Lääketieteellisiin laitteisiin kohdistetut harjoitukset voisivat toimia hyvänä harjoituksen kohteena, sillä harjoituksen avulla voitaisiin määritellä ja päivittää laitteisiin liittyvät vastuut ja roolit lääkintätekniikan, tietoturvan, tietohallinnon, kliinisen työn ja muiden mahdollisten tahojen, kuten palveluntarjoajien kanssa. Harjoituksen avulla myös arkipäiväinen työskentely ja läpinäkyvyys tiimien välillä voisi lisääntyä ja myös muut lääketieteellisiin laitteisiin liittyviä vastuita esimerkiksi koulutusten ja tietoturvapoikkeamien osalta voitaisiin kehittää.

Kirjallisuudessa kehoitetaan suunnitelmien ja toimintamallien olemassaoloon, mutta niiden toteuttamiseen ei ole yhtä tiettyä tapaa toimia. Organisaatioiden tulisi huolehtia suunnitelmien olemassaolosta sekä niiden päivittämisestä, jotta suunnitelmat olisivat käytettäviä poikkeaman sattuessa. Suunnitelmien luomisessa on tärkeää tehdä yhteistyötä organisaation eri yksiköiden ja tiimien välillä, jotta tilanteen eskalointi ja vastuut olisivat mahdollisimman selkeitä tilanteen sattuessa.

Alateema	Kirjallisuus	Kirjallisuus ja haastattelut	Haastattelut
Turvallisuuden arviointi ja validointi			
Laitteen elinkaaren aikainen arviointi		Turvallisuusarviointi, hankintojen työryhmän osallistaminen, erikois-asiiantuntijoiden käyttö, verkon skannaukset ja testaukset, kriittisten järjestelmien testaus, laitteiden testaus	Ympäristön turvallinen rakentaminen
Laitetoimittajat		Standardien mukainen	Laitteiden vaatimukset ja turvallisuustiedot, sertifikaatit
Palveluntoimittajat ja kolmannet osapuolet	IT-riskien arvioinnit, turvallisuustarkastukset	Yhteistyön, läpinäkyvyyden ja vuotovaikutuksen lisääminen, yhteistyö kehitystyössä	Toimittajien auditointi ja validointi
Haavoittuvuuksien hallinta			
Laitetoimittajan vastuut		Laitetoimittajien päivitykset, turvallisuustiedotteet	
Verkon valvonta		Verkon valvonta, haavoittuvuuksien hallinta	
Työasemat ja tietoturvakomponentit		Työasemien päivitykset, tietoturvakomponentit	

Palveluntoimittajien ja kolmansien osapuolien palvelut	Viranomaisten raportit ja tilannekuvat	Haavoittuvuuksien hallinnan yhteistyö, kehitystyö yhteistyössä, kolmansien osapuolien tiedotteet ja dokumentit, asiantuntijaverkoston yhteistyö ja vuorovaikutus	
Tietoturvapoikkeamien hallinta			
Tietoturvapoikkeamat		Tietoturvapoikkeamien prosessi, ulkopuolisten palveluntarjoajien käyttö tietoturvapoikkeamien hallinnassa	Jatkuva verkkovalvonta, MIM-prosessi
Pääsynhallinta ja -valvonta			
Fyysinen turvallisuus		Tilojen kulun- ja pääsynhallinta, huoltotapahtumien valvonta ja hallinto	Kulkukortit, laitteiden turvallinen sijoittaminen toimitiloissa
Ihmisten toiminta	Hyvien kirjautumiskäytännöistä ohjeistaminen	Käyttäjien koulutus	
Käyttäjätunnukset		Pääsynhallinnan vaatimusten luominen, tietoturva-arviointien käyttäminen kriittisyyden arvioimiseksi, vahvojen ja turvallisten kirjautumiskeinojen käyttö	
Etäyhteydet ja verkon valvonta		Verkon tietoturvan ja teknisten kontrollien vahvistaminen	Luotettavat etäyhteydet laitetoimittajilta, etäyhteyksien tunnistus yhteyden muodostuksessa, suljettujen verkkojen käyttö laitteiden yhteydessä

Taulukko 20. Vertailu kirjallisuudessa ja haastatteluissa mainituista kyberturvallisuuden liittyvästä arvioinnista ja hallinnoinnista lääketieteellisissä laitteissa.

6.3 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden hankinnat ja niissä tehtävä yhteistyö

Yhteistyö laitevalmistajien kanssa – Terveystieteiden organisaatioiden on suositeltavaa olla vuorovaikutuksessa ja luoda yhteistyön paikkoja laitevalmistajien kanssa. Laitevalmistajien kanssa tehdyn yhteistyön avulla uhkilta ja riskeiltä voidaan suojautua eri tavoilla ja tasoilla kokonaisvaltaisemmin (Norri-Sederholm et al. 2019). Eri sidosryhmien

yhteistyön avulla voidaan vähentää riskejä ja niiden realisoitumisia (Pöyhönen et al. 2019).

Laitevalmistajien kanssa tehtävä yhteistyö käyttäjäorganisaatioiden kanssa liittyy pääasiallisesti hankintoihin sekä laitteiden huoltoihin ja päivityksiin. Yksi tärkeä yhteistyömuoto laitevalmistajien kanssa on esimerkiksi erilaisten riskien tunnistaminen, arviointi ja hallinnointi (Pöyhönen et al. 2019). Laitevalmistajilla on velvollisuus sisällyttää haavoittuvuuksien tunnistamista riskienhallintaan (AAMI TIR57:2016). Laitevalmistajien luomilla haavoittuvuuksiin liittyvillä parhailla käytännöillä, tietojen jakamisella ja suunnitellulla on merkityksellinen rooli lääketieteellisten laitteiden turvallisuuden edistämässä (IMDRF 2019). Laitevalmistajien kanssa tulisi olla tiiviisti yhteistyössä jo ennen laitteiden hankintaa ja hankintatarpeita, sillä siten käyttäjäorganisaatioilla voi olla mahdollisuus vaikuttaa myös riskien hallitsemiseen liittyvien ominaisuuksien valintoihin ja laitteiden kehitykseen. Yhteistyön avulla voisi olla mahdollista luoda tietoturvallisempia lääketieteellisiä laitteita, joiden turvallisuusratkaisut tukisivat sekä kliinisen työn suorittamista ja hyvien käytäntöjen mukaisen tietoturvan toteutumista. Laitevalmistajien kanssa käyty hankintojen ulkopuolinen yhteistyö ei todellisuudessa ole terveydenhuollon organisaatioilla säännöllistä, vaan sitä toteutettiin ennemminkin satunnaisesti ja tarpeen tullen.

Pääsääntöisesti laitevalmistajien kanssa tehtävä yhteistyö liittyy laitehankintoihin ja laitteiden käytön ylläpitämiseen. Erityisesti laitteiden käyttöönotossa laitevalmistajia kehoitetaan olemaan yhteydessä käyttäjäorganisaatioihin, jotta käyttöönotto ja laitteiden konfigurointi onnistuisi mahdollisimman hyvin (IMDRF 2019). Kaikki terveydenhuollon organisaatiot tekevät yhteistyötä laitevalmistajien kanssa hankintojen yhteydessä, sillä laitteet hankitaan laitevalmistajilta. Laitehankintojen yhteydessä tehdään usein myös yhteistyötä laitteisiin kohdistuvista vaatimuksista, jotka laitteita hankkivat käyttäjäorganisaatiot tekevät. Laitteisiin kohdistuvat vaatimukset määritetään useimmiten organisaation eri asiantuntijoista koostuvan työryhmän avulla. Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden osalta työryhmiin kuuluu lähes poikkeuksetta lääkintäteknikan ja tietoturvan asiantuntijoita, jotka osaavat laatia laitteisiin kohdistuvat vaatimukset.

Hankintojen jälkeen laitevalmistajien kanssa tehtävä yhteistyö perustuu laitevalmistajien vastuiden toteuttamiseen käyttövaiheessa. Käyttövaiheessa laitevalmistajalla on velvollisuus huolehtia laitteisiin liittyvien haavoittuvuuksien riskienhallinnasta sekä huoltojen ja päivityksien hallinnoimisista. Laitevalmistajat myös tuottavat ohjekirjoja ja tiedottavat ajankohtaisista lääketieteellisiin laitteisiin liittyvistä asioista ja teemoista. Käyttövaiheessa yhteistyö perustuu pääasiallisesti laitevalmistajien tuottamiin tiedotteisiin ja mahdollisiin päivityksiin ja huoltoihin. Laitevalmistajien puolelta tulevan yhteistyön lisäksi tu-

lisi myös käyttäjäorganisaatioiden olla proaktiivisesti yhteydessä laitevalmistajiin markkinapuheenvuorojen, tulevien hankintojen ja käytössä olevien laitteiden teemasta. Tietojen jakamisen avulla voidaan suojautua paremmin uusilta kyberriskeiltä ja -uhilta, joita fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin kohdistuu (Pöyhönen et al. 2019).

Kokonaisvaltaisen laitevalmistajien ja terveydenhuollon käyttäjäorganisaatioiden välisen yhteistyön laatuun ja määrään tulisi kiinnittää huomiota sekä huolehtia yhteistyön jatkuvuudesta ja kehittämisestä. Käyttäjäorganisaatioiden ja laitevalmistajien välisestä yhteistyöstä ja säännöllisesti tapahtuvasta vuorovaikutuksesta on hyötyä käyttäjäorganisaatioille esimerkiksi kehitettävien laitteiden turvallisuusominaisuuksien parantumisen ja vaatimusten kommunikoinnin näkökulmasta. Laitevalmistajat puolestaan voivat hyötyä tiiviistä yhteistyöstä esimerkiksi uusien kehitysideoiden ja -tarpeiden kommunikoinnilla ja asiakassuhteiden syventymisellä ja luottamussuhteen vahvistumisella. Yhteistyön myötä henkilöt ja vastuut molemmissa organisaatioissa tulevat tutuiksi. Jatkuvan yhteistyön ja ajankohtaisten asioiden lisäksi myös mahdollisten kiireellisten asioiden kommunikointi voi helpottua ja tehostua.

Riskien huomiointi hankinnoissa – Terveydenhuollon organisaatioille hankinnat ja hankintaprosessit toimivat parhaimpana vaikuttamisen paikkoina fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden turvallisuuden ja riskien näkökulmasta. Terveydenhuollon toimijaorganisaatioilla on vähäinen vaikutusvalta laitteiden käyttövaiheessa ohjelmistoihin, päivityksiin tai suojauksiin. Tästä syystä on erityisen tärkeää huomioida nämä asiat jo ennen laitteen hankkimista organisaatioon.

Terveydenhuollon käyttäjäorganisaatiot pystyvät parhaiten vaikuttamaan riskien huomiointiin laitteiden hankintaprosessissa, jolloin organisaatiot luovat itse laitevaatimukset hankittaville lääketieteellisille laitteille. Käyttäjäorganisaatioiden tulee luoda laitteille organisaation ja laitteiden tietoturvaluutta edistävät vaatimukset osaksi hankintaprosessia. Laitevaatimusten lisäksi organisaatiot luovat hankintojen yhteydessä tietoturvaliitteen, jossa laitevalmistajalle asetetaan tietoturvaluuteen liittyviä ehtoja. Vaatimuksilla ja tietoturvaliitteen avulla organisaatiot voivat vaatia ja varmistaa asettamiensa vaatimusten mukaisten laitteiden hankintojen toteutumista. Vaatimusten ja tietoturvaliitteiden ottaminen osaksi lääketieteellisten laitteiden hankintaprosessia on tärkeä ja merkityksellinen keino toteuttaa kyberturvallisuutta lääketieteellisissä laitteissa ja siksi hankkijaorganisaatioiden tulisi myös säännöllisesti katselmoida ja päivittää vaatimuksia sekä tietoturvaliitteen sisältöä.

Tarpeeksi korkeat ja tietoturvan parhaita käytäntöjä noudattelevat vaatimukset ovat käyttäjäorganisaatioiden parhaimpia suojauskeinoja esimerkiksi haittaohjelmien torjumisessa, sillä laitteisiin on tarkkaan määritellyt tietyt suojaukset, joita käyttäjäorganisaatiot pystyvät halutessaan toteuttamaan (Tapx Labs 2015). Tarkat rajaukset ja määrittelyt lisäsuojauksista luovat käyttäjäorganisaatioille hyvin vähäiset mahdollisuudet tehdä hankinnan jälkeen laitteita tietoturvalliseksi. Suojauskäytännöiltään heikot tai vajavaiset lääketieteelliset laitteet ovat erityisen alttiita erilaisille kyberhyökkäyksille ja tällaisille laitteille käyttäjäorganisaatiot joutuvat tekemään erityisiä turvallisuusjärjestelyitä esimerkiksi eriyttämällä omia tietoverkkoja tällaisille laitteille. Heikosti suojattujen lääketieteellisten laitteiden suojaaminen työllistää käyttäjäorganisaatioita sekä niiden käyttämien palveluntarjoajia, mikä on otettava huomioon myös hankinnoissa osana jatkotoimenpiteitä ja käyttöönottoa.

Riskien huomiointia hankinnoissa voidaan toteuttaa eri sidosryhmiä ja asiantuntijoita osallistuttamalla hankintaprosesseihin. Hankintoihin voidaan osallistuttaa asiantuntijoita käyttäjäorganisaation eri yksiköistä sekä esimerkiksi palveluntuottajien ja muiden terveydenhuollon käyttäjäorganisaatioiden asiantuntijoita potentiaalisten palveluiden tuottokyvykkyyden sekä markkinapuheenvuorosta. Asiantuntijoiden ja sidosryhmien sitouttaminen laitehankintojen työryhmiin on tärkeä keino luoda vuoropuhelua ja ymmärtää kliinisen käytön tarpeita sekä laitteiden turvallisuuden ja hallinnoinnin näkökulmaa. Kyber- ja tietoturvallisuuden sisällyttäminen työryhmiin on merkityksellistä potilas- ja käyttäjäturvallisuudenkin näkökulmasta, jolloin laitteiden turvallisuutta on katsottava hankinnoissa sekä fyysisen, että kyberturvallisen ympäristön näkökulmista. Monipuolisten asiantuntijoiden ja osaamisalueiden sisällyttämisellä hankintoihin käyttäjäorganisaatioiden hankinnoilla on paremmat mahdollisuudet onnistua käytön ja käytön tukemisen puolesta.

Alateema	Kirjallisuus	Kirjallisuus ja haastattelut	Haastattelut
Laitevalmistajien kanssa tehtävä yhteistyö ja kyberturvallisuuden huomiointi hankinnoissa			
Organisaation sisäiset toimintatavat		Tietoturvavaatimusten laatiminen, palveluntarjoajien, organisaation sisäinen yhteistyö, laitevaatimusten läpikäynti	Tietoturva- ja tietosuojaliite, markkinakatsaukset laitevaatimusten luomiseksi
Yhteistyö kolmansien osapuolien kanssa	Toiminta- ja varautumissuunnitelmien tuottaminen, laitevalmistajien ohjekirjojen ja ohjeiden	Asiantuntijoiden osallistuttaminen organisaatiossa osana hankintojen prosessia, laitetoimittajien ja muiden kolmansien osapuolien kanssa tehtävä yhteistyö, organisaation reagoiminen erityisvaatimus-	Tietoturva- ja tietosuojaliite, markkinakatsaukset laitevaatimusten luomiseksi

	luominen, tiedon- vaihto	ten tai -suojausten toteuttamiseksi laitteille, jotka eivät täytyä vaatimuksia, yhteistyö laitteiden kehittämiseksi ja hankintaprosesseissa	
--	-----------------------------	---	--

Taulukko 21. Vertailu kirjallisuudessa ja haastatteluissa mainituista kyberturvallisuuden liittyvien lääketieteellisten laitteiden hankinnoista.

6.4 Tietoverkkoon liitettävien fyysisten lääketieteellisten laitteiden vastuut ja seuranta

Lääketieteellisten laitteiden turvallisuuteen liittyvät vastuut – Lääketieteellisten laitteiden turvallisuus on vahvasti laitevalmistajien vastuulla ja hallinnoimaa. Laitevalmistajat suunnittelevat ja toteuttavat laitteiden turvallisuusominaisuudet. Lisäksi ne hallinnoivat laitteiden käyttöä esimerkiksi päivitysten ja huoltojen osalta. Koska laitevalmistajilla on laitteiden turvallisuuteen liittyen merkittäviä vastuita ja laitteita käytetään terveydenhoidon alalla, laitevalmistajat määrittelevät pitkälti minkälaisia lisäsuojauksia käyttäjäorganisaatioilla on mahdollisuus niihin tehdä. Laitteisiin ei voida usein asentaa mitään tietoturvaohjelmia ja mikäli asennus on mahdollista, niin asentaminen onnistuu vain laitevalmistajan hyväksymään ohjelmaan (Vartiainen 2017).

Laitevalmistajien rooli laitteiden riskienhallinnassa on merkittävä, sillä riskienhallinnan suunnittelu ja osittain myös toteuttaminen tulisi tapahtua mahdollisimman varhaisessa vaiheessa jo laitteiden suunnitteluvaiheessa. Laitevalmistajilla on velvollisuus huomioida potilasriskit ja osoittaa niiden olevan hallittavissa (ISO 14971:2019). Laitevalmistajien tulisi riskienhallinnallisesta näkökulmasta huolehtia kokonaisvaltaisesta riskien tunnistuksesta ja niiden hallintakeinojen suunnittelusta laitteiden. Laitteen riskienhallintaprosessissa tulee ottaa huomioon kyberturvallisuusriskit, jotka vaikuttavat laitteen turvallisuuteen, suorituskykyyn, negatiivisesti kliiniseen leikkaukseen tai tuloksiin virheellisesti. (AAMI TIR57:2016) Suunnitteluvaiheessa laitevalmistajilla on vastuu huolehtia riskienhallinnan huomioinnista laitteiden liitettävyyden, identiteetin ja pääsynhallinnan, tietojen salausten ja suojaamisen sekä säilömistä elinkaaren aikana sekä muiden teknisten ominaisuuksien osalta, joiden avulla pyritään suojaamaan laitetta esimerkiksi palvelinsuojauksen ja verkkoviestinnän kautta. (eHealth Suisse 2020)

Käyttäjäorganisaatiolla on erityisesti vastuita fyysisen turvallisuuden ja turvallisten tietoverkkojen ja yhteyksien muodostamisessa. Lisäksi käyttäjäorganisaatiot huolehtivat työasemien suojaamisesta. Fyysiset tietoverkkoon liitettävät lääketieteelliset laitteet ovat tyypillisesti liitettynä työasemiin, jolloin niiden suojaaminen on käyttäjäorganisaatioiden

vastuulla. Fyysisessä turvallisuudessa käyttäjäorganisaatioiden on huolehdittava toimitiloista ja laitteiden sijoittamisesta turvallisiin fyysisiin paikkoihin. Tilaturvallisuudessa tärkeintä on huolehtia, etteivät laitteet ole ulkopuolisten henkilöiden saavutettavissa esimerkiksi kokonaisvaltaisen kulunvalvonnan ja ihmisten koulutuksen avulla. Lisäksi käyttäjäorganisaatioiden tulee pystyä huolehtimaan sähkönjakelujärjestelmissä.

Käyttövaiheessa laitevalmistajan riskienhallinnallinen vastuu siirtyy suureksi osaksi käyttäjäorganisaatiolla, jotka ottavat lääketieteelliset laitteet osaksi omaa riskienhallintaansa toimintaympäristössään. Laitteen riskienhallinnassa osavastuu pysyy silti laitevalmistajilla, sillä laitevalmistajat huolehtivat laitteiden päivityksistä ja huolloista, sekä yleisten haavoittuvuuksien informoimisesta. Varsinainen laitteiden käytön vastuu siirtyy kuitenkin osaksi käyttäjäorganisaatioiden toimintaa ja sitä kautta myös organisaation riskienhallintaa, jossa tulisi huomioida laitteiden käyttöturvallisuus ja käytön aikaiset riskit (IMDRF 2019).

Haastateltavat tunnistivat laitevalmistajien vastuut turvallisten laitteiden valmistuksessa ja käyttövaiheessa riskienhallinnan ja uhilta suojautumisessa. Haastatellut organisaatiot olivat vahvasti sitä mieltä, että suuri turvallisuuteen liittyvät vastuut kuuluvat pääasiassa laitevalmistajille läpi laitteiden koko elinkaaren. Laitevalmistajat pystyvät vaikuttamaan riskeiltä suojautumiseen ja riskienhallinnan keinoihin vaikuttamaan laitteiden ominaisuuksien suunnittelussa ja valitsemisessa. Lisäksi laitevalmistajien rooli jatkuu laitteiden myös käyttövaiheessa, sillä laitevalmistajat vaikuttavat vahvasti siihen, mitä käytön aikaisia suojauksia laitteissa on ja minkälaisia lisäkomponentteja ja -ohjelmia käyttäjäorganisaatiot voivat laitteisiin asentaa.

Kirjallisuudessa vastuut lääketieteellisistä laitteista nähtiin kuuluvaksi käyttövaiheessa terveydenhuollon organisaatioille, joiden tulee varmistaa laitteiden käyttöturvallisuus ja huolehtia käytön aikaisista riskeistä (IMDRF 2019). Terveydenhuollon organisaatiot olivat tästä osittain eri mieltä, sillä organisaatiot kokivat heidän mahdollisuutensa vaikuttaa laitteiden turvallisuuteen olevan suhteellisen rajatut. Terveydenhuollon organisaatiot kuitenkin tunnistivat heidän vastuunsa liittyvän käyttövaiheen turvallisuuteen esimerkiksi fyysisen turvallisuuden ja turvallisten verkkojen ja yhteyksien osalta. Selkeiden vastuualueiden lisäksi haastatteluisissa esille tuotiin epäselvyys tiedottamisen ja ihmisten koulutuksen vastuista sekä kyberturvallisuuden merkityksestä koulutuksissa ja tiedotuksissa.

Vastaava taho	Suunnittelu ja valmistus	Käyttöönotto	Käyttövaihe
---------------	--------------------------	--------------	-------------

Laitevalmistaja	Laitteiden suojauskeinojen ja -ominaisuuksien suunnittelu ja valinnat	Laitteiden käyttöön-oton tukeminen.	Huoltojen hallinnointi ja toteutus, päivityksien toimittaminen, haavoittuvuuksista ja muista mahdollisista asioista tiedottaminen.
Käyttäjääorganisaatio	Ei vastuita, mahdollisuus vuorovaikutukseen laitevalmistajien kanssa.	Laitteiden testaus, laiterestikierin täyttämisen ja käyttöön-oton suorittaminen.	Työasemien ja verkkojen suojaus sekä rakentaminen, mahdolliset laitteiden lisäsuojaukset.

Taulukko 22. Laitevalmistajan ja käyttäjäorganisaatioiden vastuut lääketieteellisistä laitteista laitteiden elinkaaren aikana.

Vastuut hoitohenkilökunnan ja potilaiden informoisesta kyber- ja tietosuojariskeistä – Päävastuussa kyberturvallisuuden ja tietosuojan riskien informoisesta ja tiedottamisesta hoitohenkilökunnalle ja potilaille ovat käyttäjäorganisaatiot. Vastuu tiedottamisesta kuuluu käyttäjäorganisaatiolle, sillä kohderyhmänä ovat potilaat ja hoitohenkilökunta kliinisestä työstä. Laitevalmistajien vastuulla on tiedottaa käyttäjäorganisaatioita esimerkiksi laitteisiin liittyvistä haavoittuvuuksista, jotka käyttäjäorganisaatioiden on päivitettävä mahdollisimman nopeasti (IMDRF 2019). Tieto haavoittuvuuksista ja muista mahdollisista laitteisiin liittyvistä tiedoista kulkee laitevalmistajalta ensin laitteista vastuussa oleville henkilöille, jotka usein työskentelevät lääkintätekniikan yksikössä.

Haastatteluissa terveydenhuollon organisaatiot toivat kuitenkin esille, ettei hoitohenkilökunnalle tai potilaille tiedoteta juurikaan kyberturvallisuuteen liittyvistä asioista. Haastattavat eivät olleet tietoisia potilaiden ja hoitohenkilökunnan kyberturvallisuuteen liittyvistä kysymyksistä, mutta tietosuojaan liittyviä kysymyksiä oli kysytty joitakin. Potentiaaliset tiedotettavat asiat koskevat enemmän tietosuoja ja kyberturvallisuuden informoinnista ei osattu sanoa juurikaan. Lääketieteellisten laitteiden käyttöön liittyvät tiedotukset potilaille ja hoitohenkilökunnalle nähtiin haastatteluissa kuuluvan kliinisen työn osastoille, joissa lääketieteellisiä laitteita konkreettisesti käytetään. Haastatteluissa esille nousi, ettei tietohallinnolla ja lääkintätekniikalla ole näkyvyyttä juurikaan potilaiden ja hoitohenkilökunnan toimimiseen, jolloin kliinisen työn suorittajille jää suuri vastuu mahdollisten tapahtumien tiedottamisesta ja huomioimisesta. Lääketieteellisten laitteiden kliinisen käytön kouluttajien tulisi koulutustilaisuuksissa tuoda esille tietosuojaan ja kyberturvallisuuteen liittyviä asioita, kuten riskejä, huomioita ja hyviä turvallisia toimintatapoja.

Lääketieteellisten laitteiden kyberturvallisuuteen ja tietosuojaan liittyvistä tiedotuksista sekä niiden vastuut tulisi määritellä käyttäjäorganisaatioissa. Kyberturvallisuusaspekteja

tulisi ottaa huomioon jo laitekoulutuksissa, jotta laitteita käyttävät ihmiset osaisivat toimia kyberturvallisesti. Kyberturvallisuuden liittyvien teemojen nostaminen osaksi koulutukseen tukee käyttäjien osaamista. Samalla koulutuksissa voidaan tuoda esille, miten mahdolliset kyberturvallisuus- ja tietosuojariskeistä voidaan ilmoittaa, jotta tiedotukset saavuttavat käyttäjät. Lisäksi on kannattavaa hyödyntää kaikkia laitevalmistajien tietoja sekä huolehtia, että nämä tiedotukset välitetään sopivassa muodossa eteenpäin kliiniseen työhön, jossa laitteita käytetään osana potilashoitoa.

Lääketieteellisten laitteiden listaukset ja seuranta – Riskienhallinnallisesta näkökulmasta käyttäjäorganisaatioiden listaukset ja rekisterit lääketieteellisistä laitteista ovat tärkeitä ja tarvittavia. Haastatteluissa fyysiset tietoverkkoon liitettävät lääketieteelliset laitteet olivat osana lääkintälaitteiden listauksia. Haastatteluista nousi esille organisaatioiden erilaiset tavat toteuttaa lääketieteellisten laitteiden rekisteriä oman organisaation lääketieteellisistä laitteista. Laitelistaukset tehdään osana laitteiden käyttöönottoa.

Yksi haastateltavista organisaatioista nosti edustamansa terveydenhuollon organisaation hyvän linjauksen ja toteutuksen kokonaisvaltaisen lääketieteellisten laitteiden rekisterin ylläpitämiseksi. Tässä organisaatiossa laiterekisterin kehittämiseen ja ylläpitoon oli kiinnitetty erityisesti huomiota ja kehitetty laiterekisteristä ajankohtaisen ja päivitetyn tiedon keskitetty paikka lääketieteellisiin laitteisiin liittyen. Laiterekisterin kehityksen lopputuloksena on laiterekisteri, johon on sisällytetty myös fyysisistä tietoverkkoon liitettävistä lääketieteellisistä laitteista päivitetty tiedot mukaan lukien teknisistä tiedoista, kuten yhteyksistä ja porteista. Tarkkojen keskitettyjen tietojen avulla on mahdollista kiireellisessäkin tilanteessa, esimerkiksi kyberhyökkäyksen realisoituessa lääketieteellisiin laitteisiin, saada selville laitteiden yhteydet ja tekemään jatkotoimenpiteitä.

Tällaisten kattavien laitelistausten kehittäminen on riskienhallinnan näkökulmasta erinomainen tapa tietojen säilömisen ja saatavuuden, mutta myös riskien mahdollisten toteutumisten ja niistä seuraavien toimenpiteiden näkökulmasta. Laiterekisterit tulee ottaa osaksi ja keskipisteeksi laitteiden riskienhallintaa sekä laitteiden seuranta ja valvomista. Laiterekisterien päivittäminen vaatii kuitenkin jatkuvaa ylläpitämistä ja päivittämistä, sekä työntekijöiden sitoutumista laiterekisterin huolelliseen käyttämiseen.

7. JOHTOPÄÄTÖKSET

Viimeisessä luvussa tutkimusta käydään läpi tutkimuksen tulokset kokonaisuudessaan. Lisäksi luvussa arvioidaan, miten tutkimus onnistui, mitä merkitystä sillä on ja minkälaisia mahdollisia jatkotutkimusaiheita ja -tarpeita tutkimus on synnyttänyt. Ensimmäisessä alaluvussa eli yhteenvedossa tutkimuksen havainnoista muodostetaan päätelmiä. Tutkimuksen toisessa, arvioinnin alaluvussa käydään läpi ja arvioidaan tutkimuksesta saatuja tuloksia ja miten tulokset vastaavat pää- ja alatutkimuskysymyksiin. Kolmannessa alaluvussa, jatkotutkimuskohteissa arvioidaan tutkimuksen mahdollisia jatkotutkimuskohteita ja -tarpeita.

7.1 Yhteenveto

Tämän tutkimuksen tarkoituksena oli selvittää ja tutkia fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuuden nykytilaa kansallisissa terveydenhuollon organisaatioissa. Päättökysymyksenä oli selvittää fyysisten tietoverkkoon liitettyjen lääketieteellisten laitteiden kyberriskien ja -uhkien huomiointi terveydenhuollon organisaatioissa kyberturvallisuuden hallitsemiseksi ja hallinnoimiseksi. Tutkimuksen avulla pyrittiin tekemään laaja ja kokonaisvaltainen katsaus kansallisten terveydenhuollon organisaatioiden kyberturvallisuuskäytäntöihin ja -tapoihin liittyen fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin. Kyberturvallisuuskäytäntöjen ja -tapojen selvittämiseksi lääketieteellisten laitteiden kyberturvallisuusteemat jaettiin neljään isoon kokonaisuuteen - kyberturvallisuuden riskeihin ja riskienhallintaan, hallintaan, arviointiin ja valvontaan, yhteistyöhön ja hankintoihin sekä vastuisiin ja seurantaan. Kyberturvallisuusteemojen avulla tutkimuksessa syvennyttiin haastateltavien organisaatioiden kyberturvallisuuden osa-alueiden tekemiseen ja hallinnointiin. Tutkimus toteutettiin kattavalla teoreettisella katsauksella kyberturvallisuuteen terveydenhuollossa ja lääketieteellisten laitteiden kyberturvallisuuden kautta. Empiirinen osuus tutkimuksesta tehtiin puolistrukturoiduilla haastatteluilla, jotka toteutettiin kolmen organisaation viiden eri asiantuntijoiden kanssa. Johtopäätösten tarkoituksena on nostaa esille tärkeimmät tutkimuksesta tehdyt havainnot.

Tutkimuksessa käytettiin päätutkimukseen vastaamisen apuna kolmea alatutkimuskysymystä. Ensimmäisen alatutkimuskysymyksen avulla on tarkoituksena selvittää, *minkälaisia kyberuhkia ja -riskejä tietoverkkoon liitettyihin fyysisiin lääketieteellisiin laitteisiin kohdistuu ja miten niitä on pyritty tunnistamaan*. Tämän alatutkimuskysymyksen avulla tutkimuksessa selvitetään lääketieteellisiin laitteisiin liittyviä kyberturvallisuusriskejä

sekä miten organisaatiot ovat huolehtineet riskeistä muun muassa riskienhallinnan keinoin. Lääketieteellisiin laitteisiin on alkanut kohdistumaan yhä enemmän kyberturvallisuushkia ja -riskejä, joista osa on ollut jopa suoraan lääketieteellisiin laitteisiin tarkoituksellisesti kohdistettuja. Potentiaalisten ja toteutuneiden kyberturvallisuusriskien ja -uhkien selvittäminen oli merkityksellistä tunnistettujen riskien huomioimiseksi organisaation riskienhallinnan suunnitelmissa ja käytänteissä. Riskienhallintaan liittyvät kysymykset auttoivat selvittämään organisaation hallinnollisia keinoja organisaatiotason riskienhallinnan osana.

Terveydenhuollon organisaatiot tunnistivat tietoverkkoon liitettäviin lääketieteellisiin laitteisiin kohdistuvia kyberturvallisuusriskejä. Tunnistetut riskit olivat teorian alalukujen 3.4 ja 3.5 kanssa samankaltaisia riskejä, joista kuitenkin haastatteluissa korostuivat erityisesti ihmisen toimintaan ja tietoverkkoliikenteen sekä työasemien kyberturvallisuusriskit. Vaikka tunnistettuja ja potentiaalisia riskejä tunnistettiin lääketieteellisiin laitteisiin liittyviksi, eivät riskit kuitenkaan olleet juurikaan realisoituneet tai vain osittain realisoitunut organisaatioissa lääketieteellisten laitteiden osalta. Realisoituneet riskit liittyivät pääasiassa laitteiden häviämisiin sekä kyberhyökkäyksiin, joita oli tapahtunut kohdistettuna lääketieteellisiin laitteisiin ja yleisesti terveydenhuollon organisaatioiden laitteisiin ja järjestelmiin.

Potentiaalisimmat käyttäjäorganisaatioita koskevat riskit liittyivät pääsääntöisesti tietoverkon kautta tapahtuvia kyberhyökkäyksiä ja luvaton liikehdintää verkoissa. Näitä riskejä hallittiin erityisesti ulkopuolisen palveluntarjoajan kanssa, joiden avulla terveydenhuollon organisaatiot huolehtivat jatkuvasta tietoliikenteen turvaamisesta. Myös työasemiin liittyvät riskit tunnistettiin merkityksellisiksi ja terveydenhuollon organisaatioiden päävastuulla olevaksi huolehtia työasemien haavoittuvuuksien hallinnasta ja päivityksistä, joilla lääketieteellisten laitteiden kyberturvallisuusriskeihin voitiin myös vaikuttaa. Ihmisen toimintaan liittyvät riskit koskivat pääasiassa laitteiden käytössä tapahtuvia, huolimattomuudesta ja tietämättömyydestä johtuvia tapahtumia ja asioita. Ihmisiin liittyvien riskien vähentämiseksi lääketieteellisten laitteiden kyberturvallisuudesta tulisi kouluttaa ihmisiä enemmän ja kohdennetusti kyberturvallisuuden teemoihin liittyen. Ihmisen toimimiseen pystytään parhaiten puuttumaan, mikäli toiminta tapahtuu tietämättömyydestä, jolloin kouluttamalla ihmisiä oikeanlaisesta kyberturvakäyttäytymisestä ja -toiminnasta voidaan lääketieteellisten laitteiden käyttäjiä saada toimimaan turvallisemmin. Ihmisiin liittyvät riskit vaikuttavat vahvasti myös fyysisen turvallisuuden toteutumiseen, jonka turvallisuuskäytäntöihin liittyvät ihmisten käyttäytyminen ja käytäntöjen toteuttaminen.

Riskien hallitsemiseksi terveydenhuollon organisaatiot toteuttavat tyypillisesti organisaatiotason riskienhallintaa, johon lääketieteellisten laitteiden riskienhallinta kuuluu osaksi.

Terveydenhuollon organisaatioiden riskienhallintaan ei ole tiettyä oikeaa tapaa toteuttaa, mutta laitteiden käytön aikaista riskienhallintaa tulee määritellä ja toteuttaa käyttäjäorganisaatioissa yhteistyössä laitevalmistajien kanssa, joiden vastuu käytön aikaiseen riskienhallintaan on valmistusvaiheenkin jälkeen olemassa (AAMI TIR57:2016). Terveydenhuollon organisaatioiden riskienhallinnan haasteina nähtiin vastuiden jakaminen, riskienhallinnan suunnitelmien luominen sekä toiminnan läpinäkymättömyys kliinisen työn ja tietohallinnon sekä lääkintätekniiikan yksiköiden välillä.

Riskienhallinnan ja siihen liittyvien suunnitelmien lisäksi riskeiltä ja uhilta suojaautumisessa terveydenhuollon käyttäjäorganisaatioiden on huomioitava tietoverkon suojaaminen, ihmisten kouluttaminen ja sisäisten prosessien ja suunnitelmien määrittely ja hyödyntäminen riskeiltä suojaautumisessa. Lisäksi organisaatiot voivat selvittää mahdollisten lisäkomponenttien ja tietoturvaohjelmien lataamisen mahdollisuuksia laitevalmistajalta ja luoda muutenkin yhteistyökeinoja ja -tapoja laitevalmistajien ja muiden kolmansien osapuolien kanssa yhteistyön tekemiseksi esimerkiksi hankintaprosessien kyberturvallisuuden kehittämiseksi.

Kyberturvallisuusriskejä voidaan tunnistaa myös laitteiden turvallisuuden arvioinnilla. Laitteiden turvallisuuteen ja sitä edistäviin ominaisuuksiin pystytään vaikuttamaan parhaiten laitteiden suunnitteluvaiheessa. Näin ollen laitevalmistajilla on merkityksellinen rooli laitteiden elinkaaren aikana turvallisuuden edistämiseksi. Laitteiden turvallisuutta voidaan arvioida hankintojen yhteydessä vaatimuslistauksilla, käytössä käyttöönoton testauksissa ja yhteyksien avauksissa ja käytön aikana sekä laitteiden ympäristön erilaisilla testauksilla.

Toisessa alatutkimuskysymyksessä selvitettiin, *minkälaista kyberturvallisuuteen liittyvää yhteistyötä tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden osalta toteutetaan hankintojen yhteydessä terveydenhuollon organisaatioissa*. Tämän alatutkimuskysymyksen tarkoituksena oli määrittää terveydenhuollon organisaatioiden yhteistyömuotoja ja -tapoja erityisesti hankintaprosessin yhteydessä. Hankintaprosessit ja laitehankinnat ovat merkityksellisiä vaikuttamisen paikkoja terveydenhuollon organisaatioille, jotka päättävät laitehankinnoistaan. Isoissa terveydenhuollon organisaatioissa tietoverkkoon liitettäviä laitteita on usein monia satoja, jolloin hankintoja on tehtävä ja hankintasopimuksia ylläpidettävä.

Terveydenhuollon organisaatioiden tekemä yhteistyö keskittyi erityisesti laitevalmistajien, palveluntarjoajien sekä mahdollisten muiden kolmansien osapuolien kanssa tehtävään yhteistyöhön. Laitevalmistajien kanssa yhteistyötä tehdään erityisesti laitteiden

hankintaprosessissa, jossa laitevalmistajille asetetaan käyttäjäorganisaation laitekohtaiset vaatimukset. Laitevaatimusten lisäksi tutkimuksessa tunnistettiin, että laitevalmistajien kanssa tehdyllä tiiviillä yhteistyöllä ennen hankintoja, hankintaprosessin aikana ja hankintavaiheen jälkeen laitteiden käytön aikana on hyötyä sekä laitevalmistajille, että laitteiden käyttäjäorganisaatiolle. Laitteiden suunnitteluvaiheessa käyttäjäorganisaatiot voivat ilmaista klinisen käytön kyberturvallisuuden tarpeista ja ennen hankintoja käydä yleisesti keskustelua tarpeista ja niiden huomioimisesta. Käyttövaiheessa tiivis yhteistyö edesauttaa tiedon kulkemista ja mahdollisten poikkeamien, haavoittuvuuksien ja huoltojen toteutumista selkeiden roolitusten ja vastuiden avulla. Tutkimuksessa nousi esille tarve kehittää ja luoda vahvempaa yhteistyötä laitevalmistajien kanssa erityisesti ennen hankintoja kuin käytön aikana.

Yhteistyön kehittämisen lisäksi kyberturvallisuusriskien huomiointi hankinnoissa tulisi olla merkittävässä roolissa, sillä käyttäjäorganisaatioilla on parhaat mahdollisuudet vaikuttaa laitteiden kyberturvallisuuteen laitteiden hankinnan yhteydessä. Laitteiden hankinnan jälkeen käyttäjäorganisaatioilla vaikutusvalta on rajoitettua, sillä laitevalmistajien vastuisiin kuuluu vahvasti laitteiden käytön aikainen kyberturvallisuus huoltojen, päivitysten, laitteistojen haavoittuvuuksien korjaamisten osalta. Käyttäjäorganisaatioiden tulisi näin ollen säännöllisesti hankintaprosessissa kehittää, katselmoida ja päivittää laitevaatimuksia, jotta hankitut laitteet täyttävät halutut kyberturvallisuusominaisuudet riskien vähentämiseksi. Lisäksi organisaatioiden tulisi kehittää toimenpidelistausta, jonka avulla käyttäjäorganisaatio voi huomioida ja hallita kyberturvallisuusriskiä, mikäli laitevalmistajat eivät pysty vastaamaan kaikkiin käyttäjäorganisaation vaatimuksiin. Kaikissa laitteiden elinkaarivaiheissa olisi syytä hyödyntää kolmansien osapuolien yhteistyömuotoja.

Kolmannessa alatutkimuskysymyksen avulla oli tarkoituksena saada selville, *miten tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuutta hallitaan ja miten vastuut kyberturvallisuudesta on jaettu*. Organisaatioissa kyberturvallisuutta hallitaan erityisesti tietoverkkojen ja -liikenteen havainnoinnilla ja turvallisten yhteyksien luomisella, huolehtimalla pääsynhallinnasta, havainnoimalla turvallisuuspoikkeamia sekä tekemällä suunnitelmia kyberturvallisuuden poikkeamien realisoitumiselle. Haavoittuvuuksien hallinnassa käyttäjäorganisaatiot hyödyntävät palveluntoimittajien palveluita ja tekevät erityisesti verkon valvontaa kyberturvallisuuden edistämiseksi. Tietoturva- poikkeamien hallinnassa jatkuvalla verkon valvonnalla on suuri rooli poikkeamien havainnoimiseksi yhdessä muiden palveluntarjoajien tuottamien valvonta- ja havainnointipalveluiden kanssa. Pääsynhallinnan ja -valvonnan keinoilla voidaan huolehtia lääketieteellisten laitteiden kyberturvallisuudesta erityisesti fyysisen turvallisuuden, ihmisen toiminnan, käyttäjätunnusten, etäyhteyksien, verkon valvonnan ja huoltotapahtumien yhteydessä.

Käyttäjörganisaatioiden päävastuulla pääsynvalvonnasta ovat erityisesti fyysisen turvallisuuden ja kulunhallinnan käytännöt, verkon valvonta sekä ihmisten toimintaan liittyvät käytännöt. Toimintamallien, prosessien ja suunnitelmien määrittely ja päivittäminen ovat isossa roolissa organisaation kyberturvallisuuteen liittyvää varautumista ja hallinnoimista. Toimintamalleista tulisi luoda selkeitä prosessimaisia malleja, suunnitelmia ja käytäntöjä, jotka sisältävät vastuut ja roolitukset. Toimintamallien toteutumiseksi organisaation tulisi tehdä yhteistyötä organisaation sisäisesti eri tiimien ja yksiköiden välillä, sekä kolmansien osapuolien kanssa.

Turvallisuuteen liittyvät vastuut puolestaan jakaantuvat pääasiassa laitevalmistajille, käyttäjörganisaatioille sekä palveluntarjoajille. Kyberturvallisuuden vastuista iso ja merkityksellinen rooli kuuluu laitteiden käyttövaiheessakin laitevalmistajille, jotka hallinnoivat laitteiden huoltoja ja päivityksiä sekä määrittävät laitteiden mahdolliset lisäkomponenttien asennukset ja kommunikoivat haavoittuvuuksista. Laitevalmistajien vastuiden lisäksi käyttäjörganisaatiot ovat vastuussa lääketieteellisten laitteiden käyttöympäristön turvallisuudesta. Käyttäjörganisaatioiden tulee rakentaa turvalliset yhteydet ja verkot, joissa toteutetaan palveluntarjoajien kanssa tarvittavia tietoturvapalveluita. Lisäksi käyttäjörganisaation tulee luoda fyysisen ympäristön osalta turvallinen käyttöympäristö laitteille ja kouluttaa ihmisiä laitteiden turvalliseen käyttöön.

Alatutkimuskysymyksillä syvennettiin päätutkimuskysymystä perehtymällä kyberturvallisuuden teemoihin tarkemmin. Alatutkimuskysymysten avulla päätutkimuskysymykseen pystyttiin vastaamaan kattavammin ja kokonaisvaltaisemmin riskeistä, hallinnasta, yhteistyöstä ja vastuista lääketieteellisten laitteiden näkökulmasta. Alatutkimuskysymysten tarkoituksena oli pohjustaa ja vastata tarkemmin tutkimuksen päätutkimuskysymyksen, *miten tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberriskit ja -uhkat ovat otettu huomioon terveydenhuollon organisaatioissa kyberturvallisuuden hallitsemiseksi ja hallinnoimiseksi*. Tutkimuksessa selvisi, että kyberturvallisuuden huomiointi terveydenhuollon organisaatioissa ja lääketieteellisten laitteiden käytössä on merkityksellistä ja se koetaan tärkeäksi, mutta laitevalmistajan vahvojen vastuiden takia käyttäjörganisaatioiden mahdollisuudet turvallisuuden edistämässä ovat rajatut.

Tutkimuksen perusteella voidaan todeta, että terveydenhuollon käyttäjörganisaatioissa kyberturvallisuus on otettu huomioon pakollisten vastuiden ja toimintojen osalta, mutta organisaatioiden vastuiden roolituksesta ja toteuttamisesta tulisi tehdä yksiselitteisempää ja läpinäkyvämpää. Terveydenhuollon organisaatioissa lääketieteellisten laitteiden riskejä hallitaan ja hallinnoidaan riskienhallinnan, tietoliikenteen ja -yhteyksien turvallisuudesta huolehtimalla, valitsemalla turvallisia ja luotettavia palveluntarjoajia, hankinta-

prosessissa vaatimusten mukaisilla laitehankinnoilla sekä organisaation sisäisillä prosessilla ja suunnitelmilla. Lisäksi organisaatiot huolehtivat jossakin määrin ihmisten koulutuksesta, mutta erityisesti kyberturvallisuuteen lääketieteellisten laitteiden osalta tulisi kiinnittää huomiota ja korostaa oikeanlaista toimintaa. Organisaation yleisten fyysiseen turvallisuuteen liittyvät käytännöt ja niistä kouluttaminen voidaan nähdä tukevan lääketieteellisten laitteiden turvallisuutta, sillä osa laitteiden turvallisuudesta liittyy esimerkiksi toimitilaturvallisuuteen ja laitteen fyysiseen sijaintiin ja sijoittumiseen käyttäjäorganisaatiossa.

Terveydenhuollon käyttäjäorganisaatioiden näkökulmasta lääketieteellisten laitteiden kyberturvallisuuteen voi olla haasteellista vaikuttaa, sillä laitevalmistajat hallinnoivat laitteisiin liittyvää turvallisuutta lainsäädännön kautta tulevien vastuiden takia. Käyttäjäorganisaatiot pystyvät kuitenkin vaikuttamaan lääketieteellisten laitteiden toimintaympäristön turvallisuuteen sekä käyttäjien kouluttamiseen. Lisäksi yhteistyöllä tarkasti valittuihin palveluntarjoajiin ja laitevaatimuksiin vastaaviin laitevalmistajiin voidaan kyberturvallisuutta ottaa paremmin huomioon ja luoda yhteistyössä turvallisempia ja parhaita käytäntöjä noudattavia ratkaisuja.

7.2 Tutkimuksen arviointi

Tämän tutkimuksen tarkoituksena oli selvittää ja tutkia fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuuden nykytilaa kansallisissa terveydenhuollon organisaatioissa. Tutkimuksessa selvitettiin terveydenhuollon organisaatioissa lääketieteellisten laitteiden kyberturvallisuutta syventymällä eri osa-alueisiin ja teemoihin. Kyberturvallisuuden teemoista keskityttiin riskeihin ja riskienhallintaan, hallintaan, arviointiin ja valvontaan, yhteistyöhön ja hankintoihin sekä vastuisiin ja seurantaan. Kaikkia kyberturvallisuuden tutkimusteemoja käytiin läpi ja heijastettiin käyttäjäorganisaation näkökulmasta lääketieteellisiin laitteisiin.

Tutkimuksen metodologiaksi valittiin laadullinen tutkimus, jolla saatiin haastateltavien asiantuntijoiden ymmärrystä, merkitystä ja ulottuvuutta tutkimukseen (Fossey et al. 2002). Laadullisen tutkimuksen haasteena voidaan kuitenkin nähdä tutkijan subjektiivisuus ja puolueellisuus, jotka voivat vaikuttaa tutkimuksen luotettavuuteen. Tutkimus perustuu tällöin empiirisen tiedon omaan tulkintaan tutkijan osalta (Leung 2015). Tutkimuksen luotettavuuden lisäksi tutkimuksen validiteetti eli tutkimukseen käytettyjen työkalujen, prosessien ja tietojen oikeanmukaisuus tutkimukseen voi kärsiä tutkijan omista empiirisistä tulkinnoista. Tutkimuksen validiteettia voidaan arvioida myös tutkimusongelman ja tulosten yhdenmukaisuudesta. (Fossey et al. 2002). Tämä tarkoittaa, että tutkimusanalyysissä tulokset voivat varioida riippuen tutkijasta ja hänen tavastaan katsoa

tutkimusvastauksia ja -tuloksia. Tutkimuksessa haastatteluista kerättyä aineistoa on analysoitu kokonaisvaltaisesti teoreettisen taustan kulkiessa mukana analysoinnin tukena. Teorian kuljettaminen analysoinnin mukana voi vähentää tutkijan omien mielipiteiden ja ajatusten vaikuttamista tutkimuksen analysointiin ja näin tukea tutkimustulosten objektiivisuutta ja luotettavuutta.

Tutkimuksen pää- ja alatutkimuskysymyksiin vastaamiseksi käytettiin haastateltavien vastauksia oman edustamansa organisaation tavoista ja käytännöistä kyberturvallisuudesta lääketieteellisissä laitteissa. Haastateltavien vastausten avulla saatiin luotua kansallisten terveydenhuollon organisaatioiden käytänteistä hyvä kokonaiskuva. Haastatteluiden avulla saatiin esille mielipiteitä ja toimintatapoja, jotka olivat merkityksellisiä kvalitatiiviselle tutkimukselle. Tutkimuksen puolistrukturoidut haastattelut toimivat tutkimuksessa tuoden haastateltaville vapauden kertoa kysymyksen aiheesta oman organisaation tapojen mukaisesti. Puolistrukturoitujen haastattelujen etuna voidaan nähdä haastatteluiden luoma mahdollisuus haastateltaville kertoa omista ajatuksista ja näkökulmista vapaamuotoisesti ja syvällisesti (Leung 2015).

Yinin (2014) mukaan rakenteellisen validiteetin avulla voidaan valita tutkimuskohteen mukaisesti tutkimusmenetelmään sopiva haastatteluiden toteutus. Tässä tutkimuksessa rakenteellista validiteettia pyrittiin huomioimaan monipuolisilla haastatteluiden kohdeorganisaatioilla ja -asiantuntijoilla, jotka on valittu huolellisesti ja asiantuntijoiden tietämykseen perustuen. Tutkimuksessa haastateltiin kolmesta organisaatiosta yhteensä viittä eri asiantuntijaa. Alun perin haastateltavia pyrittiin saamaan tutkimukseen viidestä organisaatiosta ja noin kaksi asiantuntijaa yhtä organisaatiota kohden. Kaksi organisaatiota jäättyi pois pitkien tutkimuslupaprosessien ja vapaaehtoisten henkilöiden löytämättömyyden vuoksi, jonka takia alkuperäinen haastateltavien määrä väheni. Haastateltavat valittiin pääsääntöisesti organisaatiosta tutkimuskoordinaattorien ja vastaavien henkilöiden tekemänä, jotta haastatteluihin saatiin valittua asiantuntijat, joiden työnkuvaan liittyvät kyberturvallisuus ja lääketieteelliset laitteet.

Tutkimustulosten toistettavuudesta voidaan määrittää kvalitatiivisen tutkimuksen luotettavuutta (Leung 2015). Toistettavuutta kuvaa reliabiliteetti, josta on huolehdittu aineistojen objektiivisella keräämisellä ja käytöllä (Yin 2014). Huolella valittujen asiantuntijoiden kautta haastatteluaineistoista saatiin sisällöllisesti kattavia ja näin myös tutkimuksen luotettavuutta voi pitää vahvana. Tutkimuksen luotettavuuden voidaan nähdä olevan suhteellisen todenmukainen ja hyvä vähäisestä haastateltavien määrästä huolimatta, sillä haastateltavat valittiin työnkuvan ja -osaamisalueiden mukaan jokaisesta organisaatiosta. Näin ollen haastatteluotos voidaan nähdä tarpeeksi suurena tutkimuksen luotet-

tavuuden osoittamiseksi ja toimialan kokemusten kokonaiskuvan luomiseksi. Haastattelutoksen pienuuden vuoksi tutkimuksen luotettavuutta pyrittiin edistämään läpinäkyvällä haastattelujen raportoinnilla ja analysoinnilla.

Tutkimuksessa otettiin huomioon myös näkökulmien eettisyys, joka on tärkeä ja merkityksellinen osa tutkimuksen tekemistä. Eettisyyden huomiointi oli tutkimuksessa erityisen merkityksellisessä asemassa, sillä tutkimus toteutettiin terveydenhuollon toimialalla toimivista organisaatioista, joiden toimimista rajoittavat omat potilas- ja henkilötietoihin liittyvät rajoitukset ja huomiot. Tässä laadullisessa tutkimuksessa eettisyyden huomiointi korostui erityisesti suostumuksessa ja luotettavuudessa. Suostumuksella tarkoitetaan tutkittavien ja haastateltavien henkilöiden tiedottamista tarpeeksi tarkasti ja kattavasti tutkimuksen tiedoista ja tarkoituksista. Suostumuksen yhteydessä on kerrottava myös mahdollisimman tarkasti mihin ja miten tietoja käytetään. (Fossey et al. 2022) Tutkimustyössä eettisyys on huomioitu erityisen tarkasti niin, ettei tutkimuksesta käy selville haastatellut organisaatiot tai haastateltavat. Lisäksi tutkimusaineistoista poistettiin kaikki organisaatioon ja haastateltaviin liittyvät tiedot haastatteluaineiston keräämisen ja analysoinnin jälkeen luottamuksellisuuden toteuttamiseksi.

Tutkimuksen pää- ja alatutkimuskysymyksiin vastataan käyttämällä tieteellisten julkaisujen, artikkelien, tutkimusraporttien ja muiden teoriaa tukevien julkaisujen teoreettista sisältöä sekä empirian osalta haastatteluaineistoja. Tutkimuksen teoriasta koostuvien aineistojen käyttö oli kokonaisvaltaista ja laajaa suhteutettuna aiheen ajankohtaisuuteen ja uutuuteen tieteellisissä julkaisuissa. Tietoverkkoon liitettävien fyysisten laitteiden julkaisujen ja artikkelien lisäksi tutkimusta täydennettiin terveydenhuollon toimialan sekä kyberturvallisuuden teoreettisella lähestymistavalla, joka loi tietoverkkoon liitettävien laitteiden kyberturvallisuuden tutkimiselle selittävän perustan ja lähtökohdan syvemmälle tutkimukselle. Toimialaraporttien avulla terveydenhuollon toimialan ja kyberturvallisuuden yhteenliittymistä saatiin kattava katsaus tutkimukselle. Tieteellisten julkaisujen sekä toimiryhmien ja -elinten ja organisaatioiden raporttien avulla kyberturvallisuutta voitiin tarkastella tietoverkkoon liitettävien lääketieteellisten laitteiden näkökulmasta jo tehtyjen tutkimusten ja raporttien avulla. Uutisten avulla pystyttiin tutkimukseen tuomaan ajankohtaisia nostoja esimerkiksi kyberturvallisuusriskeistä, jotka olivat toteutuneita terveydenhuollon organisaatioissa.

Tutkimuksen tarkoituksena oli toimia nykytilakatsauksena terveydenhuollon organisaatioissa tapahtuvaan kyberturvallisuuteen lääketieteellisissä tietoverkkoon liitettävissä fyysisissä laitteissa. Pää tutkimuskysymyksen avulla oli tavoitteena selvittää, miten kyberturvallisuus on otettu huomioon fyysisissä tietoverkkoon liitettävissä lääketieteellisissä laitteissa ja kuinka näiden laitteiden kyberriskejä ja -uhkia hallitaan ja hallinnoidaan

terveydenhuollon organisaatioissa. Päättökäytännön vastattiin tutkimuksessa laajalti selvittämällä kyberturvallisuuden eri osa-alueisiin liittyviä käytäntöjä ja tapoja, sillä nykytilakatsauksen toivottiin kattavaa kokonaiskuvaa laitteiden kyberturvallisuuden huomiointista. Tutkimuksessa olisi voinut käsitellä tarkemmin haastateltavien ajatuksista kehityksen tarpeista ja mahdollisista haasteista. Tämän tutkimuksen kysymykset viittasivat pääasiassa tämänhetkisen tekemisen muotoihin ja oli haastateltavan omista vastaustavoista riippuvaista, kertoiko haastateltava nykytilan lisäksi myös kehitystarpeista ja -toiveista. Mahdollisessa jatkotutkimuksessa kehitystarpeita voisi tutkia enemmän sekä kohdistaa nykytilakatsauksen tekemistä myös terveydenhuollon käyttäjäorganisaatioiden lisäksi muihin lääketieteellisiin laitteisiin liittyviin organisaatioihin ja tahoihin laajemmän kokonaiskuvan luomiseksi.

Haasteita tutkimuksen tekemiselle tuotti aiheen ajankohtaisuus, jonka vuoksi tieteellisiä julkaisuja ja artikkeleita ei ollut saatavissa rajoitettua määrää enempää. Kyberturvallisuudesta terveydenhuollosta on tehty tieteellisiä julkaisuja, mutta erityisesti kyberturvallisuuden ja lääkinnällisten laitteiden tai niiden tietoverkkoon liitettävyyden yhteydestä ei julkaisuja löytynyt yhtä lailla. Tämän vuoksi tieteellisiä julkaisujen määrä tutkimuksessa oli vähäisempi. Tieteellisten julkaisujen sijasta tutkimukseen käytettiin kuitenkin erilaisia tieteellisiä toimiala- ja laiteraportteja tietoverkkoon liitettävistä laitteista. Näiden toimialaraporttien avulla saatiin tutkimukseen tuotua nykytilaan liittyvää ajankohtaisuutta, joka oli tärkeä kyberturvallisuuden nykytilakatsauksen tekemiseksi tietoverkkoon liitettävien lääketieteellisten laitteiden tarkastelussa. Hyvin osuvien tieteellisten julkaisujen ja toimialaraporttien yhteisestä aineistosta saatiin luotua tarpeeksi tieteellinen kirjallisuuskatsaus.

Tutkimuksen kirjallisuusosuuden ja empirian arvioinnissa voidaan hyödyntää erityisesti ulkoista validiteettia. Ulkoisen validiteetin avulla voidaan selvittää tutkimustulosten yleistämistä ilmiöihin, tapahtumiin ja organisaatioihin. (Yin 2014) Ulkoisen validiteetin näkökulmasta tutkimuksen kirjallisuus- ja empiriaosuuksien avulla voidaan yhteisesti arvioida tutkimuksen kuvaavan kansallisella tasolla kyberturvallisuutta lääketieteellisten laitteiden osalta kokonaisvaltaisesti. Kirjallisuuden ja hyvin valittujen haastattelukohteiden avulla voidaan muodostaa nykytila kyberturvallisuuden suhteen kansallisissa terveydenhuollon organisaatioissa. Sisäisen validiteetin, eli miten tutkimuksen avulla voidaan luoda syyseuraus-suhteita, voidaan nähdä toteutuvan kohtuullisesti (Yin 2014). Aineiston avulla voidaan selittää kyberturvallisuuteen liittyviä tapahtumia lääketieteellisissä laitteissa sekä miten kyberturvallisuutta voitaisiin kehittää laitteiden toiminnassa.

Tieteellisten julkaisujen vähäisyyttä perustelee ajankohtaisen teeman ja sen takia vähäisten tutkimusartikkelien määrän lisäksi terminologiaan liittyvät haasteet fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden osalta, sillä monet tieteelliset julkaisut

liittyivät lääkinnällisiin laitteisiin, joihin kuuluvat myös muun muassa tämän tutkimuksen ulkopuolelle jääneet ohjelmistot. Suhteellisen vähäisestä tähän tutkimukseen suoraan linkittyvistä tutkimuksien ja tieteellisten julkaisujen määrästä huolimatta kirjallisuuskatseaus pystyttiin rakentamaan terveydenhuollon kyberturvallisuuteen ensin tutustuen ja sen jälkeen lääketieteellisiin laitteisiin ja kyberturvallisuuteen. Kirjallisuus ja haastatteluaineistot tukivat suurimmaksi osin toisiaan, mutta haastatteluaineistoista nousi myös terveydenhuollon organisaatioista esiin monesti haastatteluista mainittuja osa-alueita tai asioita, jotka eivät korostuneet teoriassa. Erityisesti yhteistyössä kolmansien osapuolien kuten laitevalmistajien, palveluntarjoajien ja valtiollisten osapuolien kanssa esille tuli lääketieteellisiin laitteisiin liittyvien vastuiden ja toimintatapojen toteutuksista asioita, jotka eivät korostuneet tieteellisissä julkaisuissa ja raporteissa. Tämä voi johtua myös siitä, että käyttäjäorganisaatioiden keinot ja tavat vaihtelevat näissä tilanteissa, jolloin organisaatioiden tapoja toteuttaa esimerkiksi riskienhallintaa ei ole tutkittu tarkemmin.

Tutkimuksen arvo voidaan nähdä muodostuvan neljän eri teeman tunnistetuista käytännöistä ja tavoista fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuudesta. Käytänteitä tunnistettiin riskien hallitsemisesta ja riskienhallinnan toteuttamisesta, hallinnasta ja havainnoinnista, hankinnoista ja yhteistyöstä sekä vastuista ja seurannasta. Tunnistettujen käytäntöjen ja tapojen avulla voidaan toimialan kyberturvallisuustapoja kehittää kohti kyberturvallisuuden parhaimpia käytäntöjä sekä teknisissä ratkaisuuksissa, että hallinnollisissa tavoissa. Erityisesti ihmisten toiminnan huomiointiin ja kouluttamiseen tulisi kiinnittää huomiota käyttäjien ja potilaiden turvallisuuden parantamiseksi. Organisaatioiden kyberturvallisuuden kokonaiskuvaa tulisi huomioida lääketieteellisten laitteiden riskienhallinnan prosessien ja käytänteiden määrittämisessä ja luomisessa.

7.3 Opinnäytetyöprosessin ja oman oppimisen arviointi

Diplomityöprosessini käynnistyi vuoden 2021 syksyllä tutkimusaiheiden kartoituksella ja selvittämällä toimeksiantajaryityksessä. Vuoden 2021 joulukuussa aloitin tutkimussuunnitelman luonnostelun ja aiheeseen liittyvän selvitystyön. Diplomityöprosessi osoittautui tutkimussuunnitelman laatimisen jälkeen haasteellisemmäksi kuin mitä minä tai toimeksiantajakaan ajattelimme, sillä terveydenhuollon organisaatioiden kanssa keskusteltua esille tuli tarve hakea erillisiä tutkimuslupia haastateltavista organisaatioista. Haastattelulupien hakemisessa ja aiheesta tuntevien haastateltavien löytämisessä kesti kokonaisuudessaan 10 kuukautta. Aihe oli kuitenkin mielenkiintoinen ja ajankohtainen myös omaan työhön, jolloin aikaa vievistä ja prosessia pitkittävästä haasteista huolimatta prosessi tuntui mielekkäältä.

Diplomityöhön johtanut prosessi on haastanut itseäni monella tavalla, mutta samalla tutkimus oli myös opettavainen ja omaan tämänhetkiseen työkuvaan ajankohtainen. Teorian, taustojen ja tieteellisten julkaisujen tutkimisen kautta sain luotua kokonaisvaltaista käsitystä lääketieteellisistä ja erityisesti rajaamistani fyysisistä tietoverkkoon liitettävistä lääketieteellisistä laitteista. Vaikka aiheesta ei tutkimuksia ollut aikaisemmin tehty runsaasti, löytyi kuitenkin toimialasta, lääketieteellisistä laitteista ja kyberturvallisuudesta teoriataustaa tarpeeksi tutkimuksen tekemiseen. Haastattelut olivat erityisen antoisia, sillä niiden kautta lääketieteellisten laitteisiin liittyvistä kyberturvallisuusasioista sai parhaimman ja ajankohtaisimman käsityksen ja näkemyksen käytössä. Oppimista on tapahtunut teoria ja haastatteluiden lisäksi myös tutkimuksen analysointivaiheessa, jolloin teemoja on täytynyt käsitellä ja pohtia analyttisesti.

Tutkimusprosessin antoisin vaihe oli tulosten kirjoittaminen ja tutkimuskysymyksiin vastausten löytäminen. Tutkimus vastaa tutkimuskysymyksiin ja tuloksissa annetaan vastaukset tutkimusongelmaan. Tutkimustulokset voivat parhaimmassa tapauksessa toimia terveydenhuollon organisaatioille apuna oman toiminnan kehittämiseksi ja kehitystarpeiden luomiselle. Lisäksi tuloksia voidaan käyttää kokonaisvaltaisena katsauksena terveydenhuollon kyberturvallisuuteen fyysisissä tietoverkkoon liitettävissä lääketieteellisissä laitteissa.

7.4 Tutkimuksen merkitys ja jatkotutkimuskohteet

Fyysiset tietoverkkoon liitettävät lääketieteelliset laitteet ovat suhteellisen uusia terveydenhuollon alalla ja niiden kyberturvallisuusominaisuuksia on kehitettävä laitteiden muun kehittämisen rinnalla. Kyberrikolliset käyttävät lääketieteellisten laitteiden kyberturvallisuusuhkia ja -haavoittuvuuksia hyödyksi yhä enenevässä määrin lääketieteellisten laitteiden tietoverkkoon liitettävyyden kautta. Potentiaalisten riskien kasvaessa myös realisoituneet riskit tietoverkkoon liitettävissä fyysisissä lääketieteellisissä laitteissa ovat lisääntyneet. Riskien vähentämiseksi ja laitteiden turvallisen käytön edistämiseksi laitevalmistajien tulee kehittää kyberturvallisuusominaisuuksia yhdessä käyttäjäorganisaatioiden kanssa. Lisäksi terveydenhuollon käyttäjäorganisaatioiden tulee huomioida lääketieteellisiin laitteisiin kohdistuvat riskit ja luoda käyttöympäristöstä turvallinen laitteille tarvittavilla menettelyillä ja keinoilla.

Fyysisten tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuuden nykytilatutkimuksella saatiin selvitettyä kansallisen tason terveydenhuollon käyttäjäorganisaatioiden näkökulmasta tämänhetkisiä laitteisiin liittyviä kyberturvallisuusteemoja. Kyberturvallisuuden nykytilan selvityksessä saatiin selville kyberturvallisuuden näkökulmasta riskeistä ja riskienhallinnan toimista, arvioinneista ja hallinnasta, yhteistyötavoista

ja hankintaprosesseista sekä vastuista ja seurannasta. Lääketieteellisten laitteiden kyberturvallisuudesta on tehty aikaisempia tutkimuksia, jotka ovat keskittyneet kaikkiin lääkekäyttöön liittyviin laitteisiin ja niiden riskeihin. Lisäksi lääketieteellisiin laitteisiin kohdistuneista toteutuneista uhista ja riskeistä on uutisoitu valtakunnan median tasolla kansallisesti ja kansainvälisestikin.

Tämän tutkimuksen etuna voidaan nähdä tutkimuskohteen rajauksen selkeästi tiettyyn joukkoon lääkekäyttöön liittyviä laitteita eli fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin, jotka käytännössä erottavat lääkekäyttöön liittyvien laitteiden joukosta ohjelmistot ja laitteet, joilla ei ole ominaisuutta kytkeytyä tietoverkkoihin. Tutkimus käsittelee kyberturvallisuutta kokonaisvaltaisesti ottaen huomioon riskienhallinnan, hallinnan ja valvonnan keinot, erilaiset yhteistyömuodot ja hankintaprosessin sekä vastuut ja seurannan. Tutkimuksen merkittävyys syntyy näin ollen tutkimuksen nykytilakartoituksen laajuudesta ja tutkimuksen rajatusta kohteista fyysisiin tietoverkkoon liitettäviin lääketieteellisiin laitteisiin. Tietoverkkoon liitettävien lääketieteellisten laitteiden kyberturvallisuudesta ja niiden riskienhallinnallisista keinoista käyttäjäorganisaatioiden näkökulmasta ei ole tehty vielä tutkimuksia, jolloin kartoitettava tutkimus kansallisten terveydenhuollon organisaatioiden tavoista on tärkeää kehityskohteiden ja parhaiden käytäntöjen määrittelemiseksi. Lisäarvoa ja merkityksellisyttä tutkimukseen tuovat neljä tunnistettua pääaluetta, joihin kyberturvallisuuden teemat lääketieteellisiin laitteisiin on voitu jakaa ja määritellä.

Tutkimuksen myötä terveydenhuollon organisaatiot ja tutkimuksen toimeksiantaja voivat hyötyä tutkimuksesta käytännön arvon myötä. Tutkimuksen vahvuutena voidaan nähdä suuri käytännön arvo organisaatioille, vaikka tutkimuksesta tieteelliset tulokset jäivät vähäiseksi nykytilakartoituksessa. Tutkimuksen avulla kansalliset terveydenhuollon organisaatiot voivat verrata omia toimintatapoja kyberturvallisuuden suhteen lääketieteellisten laitteiden käytössä. Lisäksi terveydenhuollon organisaatiot voivat tunnistaa kehityskohtia ja -tarpeita omassa toiminnassaan kyberturvallisuuden edistämiseksi. Terveydenhuollon organisaatioille tutkimuksesta on käytännön arvoa omien toimintatapojen vertailussa toisiin organisaatioihin sekä mahdolliseen kehitystyöhön, johon voidaan saada lähtökohtia tutkimuksesta. Tutkimuksen tulosten avulla organisaatiot voivat parantaa kyberturvallisuuden huomiointia sekä lääketieteellisten laitteiden, kuin yleisesti organisaatioiden kyberturvallisuuden kypsyyden osalta.

Terveydenhuollon organisaatioiden saaman hyödyn lisäksi tutkimuksen merkityksellisyys syntyy toimeksiantajayrityksen saamasta käytännön arvosta. Tutkimuksen avulla toimeksiantaja voi kasvattaa markkinatietoisuutta terveydenhuollon organisaatioista ja niiden kyberturvallisuudesta. Tutkimuksesta saatuja tuloksia voidaan käyttää sekä ylei-

sesti kyberturvallisuuden, että erityisesti lääketieteellisten laitteiden toiminnan selvittämiseksi. Toimeksiantaja voi käyttää tutkimustuloksista saamiaan tietoja paremman toimialatietoisuuden kasvattamiseen ja siten pyrkiä tarjoamaan terveydenhuollon organisaatioille kyberturvallisuuspalveluita. Tutkimuksen avulla toimeksiantaja voi tarjota kohdistetusti kyberturvallisuuspalveluita tutkimuksessa tunnistettuihin kyberturvallisuuden osa-alueisiin, joille on erityisesti tunnistettu tutkimuksessa kehityksen tarvetta. Lisäksi toimeksiantaja saa tutkimuksen avulla kokonaiskuvan lääketieteellisten laitteiden kyberturvallisuuteen liittyvistä yhteistyökumppaneista ja -osapuolista, joiden kanssa voi luoda yhteistyötä ja mahdollisesti tarjota palveluita.

Tutkimuksen jatkotutkimuskohteiksi olisi merkityksellistä ottaa tutkittavaksi laitevalmistajien näkökulma fyysisten tietoverkkoon liitettävistä lääketieteellisistä laitteista, sillä tässä tutkimuksessa on käsitelty kyberturvallisuuden nykytilaa terveydenhuollon käyttäjäorganisaatioiden näkökulmasta. Laitevalmistajien näkökulmasta tehdyssä tutkimuksessa laitevalmistajien kyberturvallisuuteen liittyvistä suunnittelu- ja valmistusprosesseista, riskienhallinnasta ja käyttövaiheen vastuista voitaisiin saada tutkimustuloksia. Näistä tuloksista voitaisiin luoda kehitysehdotuksia ja -tarpeita kyberturvallisuuden parhaiden käytäntöjen toteuttamiseksi. Laitevalmistajien näkökulmasta tehdyn tutkimisen yhdistäminen tähän terveydenhuollon käyttäjäorganisaatioiden kattavaan tutkimukseen voi luoda merkityksellisen kokonaiskuvan lääketieteellisten laitteiden kyberturvallisuuteen ja alalla tarvittaviin kehitysmuotoihin. Laitevalmistajien näkökulmien lisäksi tutkimusta voisi jatkaa syventymällä tutkimuksen alakysymyksiin tarkemmin ja jatkaa näin nykytilakartoitusta määrittämällä ja selvittämällä yhteisiä hyviä käytäntöjä esimerkiksi riskienhallinnan toteuttamiseen lääketieteellisten laitteiden osalta.

LÄHTEET

- [1] AAMI TIR57:2016. (2016). Principles For Medical Device Security - Risk Management. Technical Information Report.
- [2] Andress, J. (2019). Foundations of information security: a straightforward introduction. No Starch Press. Saatavilla: <https://lccn.loc.gov/2019024099> (viitattu 20.12.2022).
- [3] Andreasson, A., Koivisto, J., Ylipartanen, A. (2013). Tietosuojavastaavan käsikirja. Helsinki: Hakapaino.
- [4] Aram, S., Shirvani, R. A., Pasero, E. & Chouikha, M. F. (2016). Implantable Medical Devices; Networking Security Survey. J. Internet Serv. Inf. Secur., vol. 6, no. 3, pp. 40–60.
- [5] Brewster, T. (2017). Medical Devices Hit By Ransomware For The First Time in Us Hospitals. Forbes. Saatavilla: <https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/?sh=60ab88f9425c> (viitattu 11.1.2023).
- [6] Clarke R, Youngstein T. (2017). Cyberattack on Britain's National Health Service – A wakeup call for modern medicine. New England Journal of Medicine 377(5). DOI:10.1056/NEJMp1706754.
- [7] Csulak, E., Meadows, T., Corman, J., DeCesare, G., Fernando, A., Finn, D., Jarrett, M., Laybourn, L., McNeil, M., McWhorte, D., Mellinger, R., Monson, J., Radadoos, R., Rice, T., Sardanopoli, V., Suarez, R., Stine, K., Sublett, C., Thompson, L., Ting, D. & Trotter, F. (2017). Report on improving cybersecurity in the health care industry. Health care industry cybersecurity task force report. Saatavilla: <https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf> (viitattu 28.11.2022).
- [8] Deloitte Centre of Health Solutions. (2018). Medtech and the Internet of Medical - Things How connected medical devices are transforming health care. Saatavilla: <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf> (viitattu 2.5.2023).
- [9] Dhillon, B.S. (2009) Life Cycle Costing for Engineers. ISBN 9781138072022. 1st edition.
- [10] eHealth Suisse. (2020). Guide for app developers, manufacturers and distributors. Swiss Competence and Coordination Centre of the Confederation and the Cantons. OID: 2.16.756.5.30.1.127.1.3.5.1.1 Saatavilla: https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2018/E/180731_Leitfaden_fuer_App_Entwickler_def_EN.pdf (viitattu 20.10.2022).
- [11] Enisa. (2016). Cyber security and resilience for Smart Hospitals. European Union Agency For Network And Information Security. Saatavilla: <https://www.enisa.europa.eu/publications/cybersecurity-and-resilience-for-smart-hospitals> (viitattu 10.12.2022).

- [12] Euroopan parlamentin ja neuvoston asetus (EU). (2017). Euroopan unionin virallinen lehti. 2017/745. Saatavilla: <https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32017R0745&from=FI> (viitattu 3.1.2023).
- [13] Eriksson & Koistinen. (2005). Monenlainen tapaustutkimus. Kuluttajatutkimuskeskus. Julkaisuja 4:2005.
- [14] Fimea. (2022). Lääkinnälliset laitteet. Kansalaisen lääketieto. Saatavilla: https://www.fimea.fi/kansalaisen_laaketieto/tuotetietoa-terveysteknologiasta (viitattu 30.12.2022).
- [15] Fossey, E., Harvey, C., McDermott, F. & Davidson, L. (2022). Understanding and evaluating qualitative research. *Australian and New Zealand Journal of Psychiatry*, Vol. 36, 717–732.
- [16] Grimes, S. T. (2016). Part 1 of 3: Best Practices for Medical Device Cybersecurity Management. CE-IT Collaboration Town Hall Series 23–24. Saatavilla: <https://docplayer.net/35473652-Part-1-of-3-best-practices-for-medical-device-cybersecurity-management.html> (6.2.2023).
- [17] Gubrium, J.F., Holstein, J.A., Marvasti, A.B. & McKinney, K.D. (2012). *The SAGE Handbook of Interview Research: The Complexity of the Craft*. 2nd ed. Thousand Oaks: Sage Publications Inc.
- [18] Hadnagy, C., Fincher, M., Dreeke, R. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails*.
- [19] Hafiz, M., P. Adamczyk ja R.E. Johnson. (2007). "Organizing security patterns". *Software, IEEE* 24 (4): 52–60.
- [20] Health care and cybersecurity: Increasing threats require increased capabilities. (2015). KPMG. Saatavilla: <https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-caresurvey-kpmg-2015.pdf> (viitattu 20.10.2023).
- [21] Hirsjärvi, S. & Hurme, H. (2011). *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö*.
- [22] IMDRF. (2019). Principles and Practices for Medical Device Cybersecurity. Medical Device Cybersecurity Working Group. Saatavilla: <https://www.imdrf.org/sites/default/files/2021-09/imdrf-cons-ppmdc.pdf> (viitattu 28.12.2022).
- [23] ISO 14971:2019. Medical devices — Application of risk management to medical devices.
- [24] Jauhiainen, M. & Värri, A. (2017). Lääkintätekniikan prosessien järjestäminen sairaanhoitopiirin tietohallinnossa. Tampereen teknillinen yliopisto. Saatavilla: <http://urn.fi/URN:NBN:fi:tyy-201708291841>.
- [25] Järviö, J. (2012). *Kunnossapito: tuotanto-omaisuuden hoitaminen*. 5. p. Helsinki: KPMedia.
- [26] Keränen, T. (2017). WannaCry haittaohjelma löytyi TYKS:sta. *Lääkärilehti*. Saatavilla: <https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/> (viitattu 8.1.2023).

- [27] Khandelwal, S. (2016). World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices. The Hacker News. Saatavilla: <http://thehackernews.com/2016/09/ddos-attack-iot.html> (viitattu 26.12.2022).
- [28] Korhonen, V. (2009). Tapauksena tapaustutkimus. Aikuiskasvatus. (Online). 29 (1), 66-67.
- [29] Kortesoja, M. (2022). Tapaus Vastaamo: Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista. Tutkimus & Kriittikki, 2(1), 9–32.
- [30] Kullas, J. (2022). Hakkerit iskivät sairaalaan – lähes 270 000 potilaan tiedot varastettiin. Mikrobitti. Saatavilla: <https://www.mikrobitti.fi/uutiset/hakkerit-iskivat-sairaalaan-lahes-270-000-potilaan-tiedot-varastettiin/c00cc89c-db1f-4571-8457-700d41aa5460> (viitattu 11.1.2023)
- [31] Kyberturvallisuuskeskus. (2016). Terveystietosuojan kyberuhkia. Viestintävirasto. Saatavilla: [Terveystietosuojan_kyberuhkia.pdf](http://www.viestinta.fi/attachments/kyberuhkia.pdf) (kyberturvallisuuskeskus.fi) (viitattu 15.1.2023)
- [32] Kyberturvallisuuskeskus. (2019). Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset. Saatavilla: <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja> (viitattu 10.4.2023)
- [33] L 24.6.2010/629. Laki terveydenhuollon laitteista ja tarvikkeista. Valtion säädöstietopankki Finlex, ajantasainen lainsäädäntö. Saatavilla: <http://www.finlex.fi/fi/laki/ajantasa/2010/20100629> (viitattu 10.1.2023)
- [34] Laki terveydenhuollon laitteista ja tarvikkeista 629/2010.
- [35] Lehto, M., Pöyhönen, J. & Lehto, M. (2019). Kyberturvallisuus sosiaali- ja terveydenhuollossa. Loppuraportti Vol.2. Jyväskylän yliopisto. Saatavilla: <http://urn.fi/URN:ISBN:978-951-39-7711-5>.
- [36] Lehto, M. (2015). Phenomena in the Cyber World. In: Lehto, M., Neittaanmäki, P. (eds) Cyber Security: Analytics, Technology and Automation. Intelligent Systems, Control and Automation: Science and Engineering, vol 78. Springer, Cham. Saatavilla: https://doi.org/10.1007/978-3-319-18302-2_1
- [37] Lehto M. Kybermaailman ilmiöitä ja määrittelyjä. (2017). v 8.0. 1.9.2017. Informaatioteknologian tiedekunta, Jyväskylän yliopisto.
- [38] Lehto, M. & Lehto M. (2017). Kyberturvallisuus sairaalajärjestelmissä: Osa 1. 14.8.2017. Informaatioteknologian tiedekunta. Jyväskylän yliopisto.
- [39] LeRouge, C., Mantzana, V., Wilson E. (2017). Healthcare information systems research, revelations, and visions. Verkkojulkaisu. Saatavilla: <https://www.tandfonline.com/doi/full/10.1057/palgrave.ejis.3000712>. (viitattu 1.12.2022)
- [40] Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. Journal of family medicine and primary care, Vol. 4, No. 3, 324–324.
- [41] Libicki Martin C. (2007). Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007, s. 236-240.

- [42] Lääkintälaitedirektiivi 93/42/ETY.
- [43] Mikkonen, H. (2009). *Kuntoon perustuva kunnossapito: käsikirja*. 1.p. Kerava: Savion Kirjapaino Oy.
- [44] Norri-Sederholm, T., Laitinen, T., Lehto, M., & Kari, M. J. (2019). Health care and cyber threats. *Finnish Journal of EHealth and EWelfare*, 11(1-2), 86–99. Saatavilla: <https://doi.org/10.23996/fjhw.74183>
- [45] OYS:n nimissä tietojen kalastelua - sairaala ei koskaan kysy potilaiden verkkopankkitunnuksia. (2020). Pohjois-Pohjanmaan hyvinvointialue Pohde. Saatavilla: <https://www.sttinfo.fi/tiedote/oysn-nimissa-tietojen-kalastelua---sairaala-ei-koskaan-kysy-potilaiden-verkkopankkitunnuksia?publisherId=69817636&releaseId=69880809> (viitattu 22.12.2022).
- [46] Patton, M.Q. (2005). *Qualitative Research*. Qualitative Research. Sage, Thousand Oaks, CA.
- [47] Pennanen, T. (2022). Omakannan nimissä liikkuu huijausviestejä. *Lääkärilehti* 29.3.2022. Saatavilla: <https://www.laakarilehti.fi/terveydenhuolto/omakannan-nimissa-liikkuu-huijausviesteja/> (viitattu 20.12.2022).
- [48] Piggini R. (2017). *Cybersecurity of medical devices: Addressing patient safety and the security of patient health information*. BSI. Saatavilla: https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf (viitattu 13.1.2023)
- [49] Pulliainen, M. (2020). Varoitus: kyberhyökkäyksistä sairaaloihin tulossa globaali trendi, kasvu Euroopassa ”hälyttävää”. *Tekniikka ja talous*. Saatavilla: <https://www.tekniikkatalous.fi/uutiset/tt/f3d302d3-8fff-43ee-80f8-cda61a1eaf34> (viitattu 12.1.2023)
- [50] Rabionet, S. E. (2011). *How I Learned to Design and Conduct Semi-structured Interviews: An Ongoing and Continuous Journey*. *The Qualitative Report*, Vol. 16, No. 2, 563– 566.
- [51] Rakitin, S. R. (2009). *Networked Medical Devices: Essential Collaboration for Improved Safety*. *Management & Technology*. *Biomed Instrum Technol* (2009) 43 (4): 332–338.
- [52] Rautio, M. (2017). Kelan Kanta-palvelut vaikeuksissa – syynä jälleen palvelunestohyökkäys. *Yle Uutiset* 3.6.2017. Saatavilla: <https://yle.fi/uutiset/3-9647957> (viitattu 12.1.2023).
- [53] Remenyi D, Wilson R. *Glossary of Cyber Warfare, Cyber Crime, Cyber security*. ACPI, UK; 2018.
- [54] Ruusuvuori, I. & Tiittula, L, M. (2017). Tutkimushaastattelu ja vuorovaikutus. In M. Hyvärinen, P. Nikander, & Ruusuvuori (Eds.), *Tutkimushaastattelun käsikirja* (pp. 46-83). Vastapaino.
- [55] Saunders, M., Lewis, P. & Thornhill, A. (2016) *Research methods for Business Students*, 7th edition. Pearson.
- [56] Saunders, M., Lewis, P. & Thornhill, A. (2019) *Research methods for Business Students*, 8th edition. Pearson.

- [57] Seale, K., McDonald, J., Glisson, W., Pardue, H. & Jacobs, M. (2018). MedDevRisk: Risk Analysis Methodology for Networked Medical Devices. Proceedings of the 51st Hawaii International Conference on System Sciences. Saatavilla: <http://hdl.handle.net/10125/50302> (viitattu 2.5.2023)
- [58] Soininen, M. (2016). Kyberhyökkäykset lisääntyvät terveydenhuollossa. Potilaan lääkirilehti 5.6.2016. Saatavilla: <http://www.potilaanlaakarilehti.fi/uutiset/kyberhyokkaykset-lisaantyyvat-terveyden-huollossa/> (viitattu 29.1.2023).
- [59] Sosiaali- ja terveysministeriö. (2019). Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019.:14. ISBN PDF: 978-952-00-4085-7. Saatavilla: <http://urn.fi/URN:ISBN:978-952-00-4085-7>
- [60] Symantec. (2018). New orangeworm attack group targets the health care sector in the US, Europe and Asia. Symantec Blogs 23.4.2018. Saatavilla: <https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia> (viitattu 20.1.2023).
- [61] Tham, I., Au-Yong, R., May Linn, T. & Pazos, R. (2018). SingHealth cyber attack: How it unfolded. The Straits Times. Saatavilla: <https://graphics.straitstimes.com/STI/STIMEDIA/Interactives/2018/07/sg-cyber-breach/index.html> (viitattu 20.2.2023)
- [62] The Deloitte Center for Health Solutions. (2013). Issue Brief: Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives. Saatavilla: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/uslhsc-networked-medical-device.pdf> (viitattu 20.2.2023).
- [63] Traficom. (2021). Tietoturvan vuosi 2021. Kyberturvallisuuskeskuksen vuosikatsaus. Traficom julkaisuja 3/2022. Saatavilla: <https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Tietoturvan-vuosi-2021.pdf> (viitattu 28.2.2023).
- [64] Trapx Labs. (2015). Anatomy of an Attack. Medjack Medical Device Hijack. TrapX Labs - A Division of TrapX Security, Inc. Saatavilla: https://securityledger.com/wpcontent/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf (viitattu 28.1.2023).
- [65] Turvallisuuskomitea; 2013. Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös, 22.1.2013. Saatavilla: <https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf> (viitattu 26.12.2022).
- [66] Turvallisuuskomitea. (2018). Kyberturvallisuuden sanasto. Sanastokeskus TSK ry. Saatavilla: https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf (viitattu 3.1.2023).
- [67] Uusitalo, K. (2020). Terveystalon verkkoajanvarauksesta kalasteltu henkilötietoja – järjestelmän haavoittuvuus oli tiedossa jo etukäteen. Yle Uutiset 3.2.2020. Saatavilla: <https://yle.fi/a/3-11189706> (viitattu 22.12.2022).
- [68] Vaarama, V. (2019). Verkkohyökkäys voi lamaannuttaa sairaalan – esimerkkejä löytyy jo Suomestakin. Yle Uutiset 11.2.2019. Saatavilla: <https://yle.fi/a/3-10640642> (viitattu 26.12.2022).

- [69] Vartiainen J. (2017). Lääkintälaitteen turvallinen liittäminen sairaalan tietoverkkoon. Opinnäytetyö. Lahden ammattikorkeakoulu, tekniikan ala. Saatavilla: <http://urn.fi/URN:NBN:fi:amk-2017060212042>
- [70] Williams, P. & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical devices*. Vol.8, p.305-316. Saatavilla: <https://doi.org/10.2147/MDER.S50048>
- [71] Zhang, Y., Qui, M., Chun-Wei, T., Hassan, M. M. & Alamri, A. (2017). Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. *IEEE Systems Journal*, 1 (88–95).
- [72] Yaqoob, T., Abbas, H. & Atiqzaman, M. (2019). Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices. *IEEE Communications surveys and tutorials*. Vol.21 (4), p.3723-3768.
- [73] Yin, R. K. (2014). *Case Study Research: Design and Methods*. 5th edition. Los Angeles: SAGE.

LIITE 1: TUTKIMUSTIEDOTTEEN POHJA HAASTATELTAVILLE TERVEYDENHUOLLON ORGANISAATIOILLE

TIEDOTE TUTKIMUKSESTA

Tutkimus – Tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuus terveydenhuollossa

Pyydämme teitä osallistumaan tähän tutkimukseen, jossa tutkitaan lääketieteellisten laitteiden kyberturvallisuuden nykytilaa terveydenhuollossa eli minkälaisia kyberriskejä ja -uhkia lääketieteellisiin laitteisiin kohdistuu ja miten näitä hallitaan, seurataan ja kuinka vastuunjako on toteutettu. Tämä tiedote kuvaa tutkimusta ja Teidän mahdollista osuuttanne siinä. Porehdytjänne rauhassa tähän tiedotteeseen teille järjestetään mahdollisuus esittää kysymyksiä tutkimuksesta. Jos päätätte osallistua tutkimukseen, teiltä pyydetään suostumus tutkimukseen osallistumisesta.

Tutkimuksen tarkoitus

Tämän tutkimuksen tarkoituksena on selvittää, miten kyberturvallisuus on otettu huomioon riskien, uhkien ja haavoittuvuuksien osalta ja kuinka kyberturvallisuuden vastuut on jaettu ja kyberturvallisuutta seurataan, hallitaan ja raportoidaan tietoverkkoon liitetyissä fyysisissä lääketieteellisissä laitteissa. Tietoverkkoon liitetyllä fyysisellä lääketieteellisellä laitteella tarkoitetaan esimerkiksi lääkinnällistä instrumenttia, laitetta tai välinettä, jolla on ominaisuus ottaa yhteys tietoverkkoon. Tampereen yliopistollisen sairaalan erityisvastuualueen alueellinen eettinen toimikunta on arvioinut tutkimussuunnitelman ja antanut siitä puoltavan lausunnon.

Tutkimuksen toteuttaja

Tämän tutkimuksen toteuttavat Deloitte Oy toimeksiantajana ja Tampereen yliopisto opinnäytetyön ohjaavana toteuttajaorganisaationa.

Tutkimuksen kulku

Tutkimus suoritetaan puolistrukturoituina haastatteluina. Haastattelussa käsitellään aluksi lyhyesti haastateltavien henkilöjen taustatietoja (nimi ja työhistoria). Tämän jälkeen siirrytään käsittelemään organisaation lääketieteellisiä laitteita ja niiden kyberturvallisuutta sekä kyberriskien vastuiden jakautumiseen, hallintaan ja seurantaan liittyviä asioita.

Yhden haastattelun kesto on noin 60-90 minuuttia ja toteutetaan etäyhteydellä. Haastatteluihin pyritään löytämään yhdestä kolmeen henkilöä, joita haastatellaan joko yksilö- tai ryhmähaastattelulla. Haastatteluja on tarkoitus pitää yksi haastattelu yhtä haastateltavaa kohden, mutta mikäli on tarpeellista tutkimuksen kannalta, voidaan haastattelutilaisuuksia järjestää useampia.

Tutkimukseen liittyvät hyödyt sekä mahdolliset riskit ja haitat

Tutkimuksesta saatuja tietoja voidaan käyttää hyväksi terveydenhuoltoalan käyttämien lääketieteellisten laitteiden kyberturvallisuuden nykytilan arvioimiseen kyberturvallisuusriskien, -uhkien ja -haavoittuvuuksien hallinnan, seurannan, raportoinnin ja vastuiden jakamisen suhteen.

On mahdollista, ettei tutkimukseen osallistumisesta ole Teille tai edustamallenne organisaatiolle välitöntä hyötyä. Tutkimuksen avulla pyritään selvittämään, miten kyberturvallisuus on otettu huomioon riskien, uhkien ja haavoittuvuuksien osalta ja kuinka kyberturvallisuuden vastuut on jaettu ja kyberturvallisuutta seurataan, hallitaan ja raportoidaan tietoverkkoon liitettyissä fyysisissä lääketieteellisissä laitteissa terveydenhuollossa.

Henkilötietojen käsittely ja tietojen luottamuksellisuus

Henkilötietojanne käsitellään tässä tiedotteessa kuvattua tieteellistä tutkimusta varten. Henkilötietojen käsittelyn perusteena on Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 (yleinen tietosuoja-asetus) artiklan 6(1)(e) mukaisesti:

- yleisen edun mukainen tieteellinen tutkimus (henkilötiedot yleisen tietosuoja-asetuksen artikla 6.1.e)

Tutkimuksessa rekisteriin tallennetaan vain tutkimuksen tarkoituksen kannalta välttämättömiä henkilötietojanne. Teistä kerättyjä tietoja ja tutkimustuloksia käsitellään luottamuksellisesti henkilötietojen käsittelyä koskevan lainsäädännön edellyttämällä tavalla. Tutkimuksen aikana henkilötietoja kerätään vain niiltä osin, kuin on tarpeellista tutkimuksen kannalta. Tutkimuksen kannalta tarpeellisia henkilötietoja ovat tutkimukseen osallistuvan nimi ja työhistoria. Haastatteluihin osallistuvat henkilöt ja heidän edustamat organisaatiot jäävät vain tutkimuksen toteuttamiseen osallistuvien henkilöi-

den tietoon. Lopulliset tutkimustulokset raportoidaan opinnäytetyön yhteydessä siten, että vastaajan henkilöllisyyttä tai hänen edustamaa organisaatiota ei voida tunnistaa, ja aineisto anonymisoidaan. Yksittäisen tutkittavan tunnistaminen ei ole mahdollista tutkimustulosten julkaisuista tai selvityksistä.

Tutkimuksessa teistä ja organisaatiosta kerätään seuraavia tietoja seuraavista lähteistä:

Haastattelut

Vapaaehtoisuus

Osallistuminen tähän tutkimukseen on täysin vapaaehtoista. Voitte kieltäytyä osallistumisesta tai peruuttaa suostumuksenne syytä ilmoittamatta milloin tahansa ilman siitä koituvaa haittaa Teille.

Voitte myös peruuttaa antamanne suostumuksen milloin tahansa tutkimuksen aikana ilman perusteluita ilmoittamalla siitä tutkimushenkilökunnalle. Suostumuksen peruuttamisesta ei koidu teille mitään haittaa. Jos päätätte peruuttaa suostumuksenne, tai osallistumisenne tutkimukseen keskeyty jostain muusta syystä, siihen mennessä kerättyjä tietojanne voidaan edelleen käyttää tässä tutkimuksessa, mikäli tutkimuksen toteuttaminen sitä vaatii.

Tutkimuksen kustannukset ja taloudelliset selvitykset

Tutkimukseen osallistumisesta ei makseta palkkiota.

Tutkijalle ja muulle henkilökunnalle ei makseta erillistä korvausta tutkimuksen tekemisestä.

Tutkimustuloksista tiedottaminen

Tutkimustulokset ovat vapaasti nähtävillä Tampereen yliopiston avoimessa julkaisuarkistossa diplomityön valmistuttua. Tutkimustulosten esittämisestä voidaan sopia tutkimuksen valmistuttua organisaation kanssa erikseen.

Lisätiedot

Voitte esittää kysymyksiä tutkimuksesta tutkijalle.

LIITE 2: TUTKITTAVAN SUOSTUMUS

Tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden kyberturvallisuus terveydenhuollossa

Minua on pyydetty osallistumaan yllämainittuun tieteelliseen tutkimukseen.

Olen lukenut ja ymmärtänyt saamani tutkimustiedotteen. Olen saanut riittävän selvityksen tutkimuksesta ja sen yhteydessä suoritettavasta henkilötietojeni (nimeni ja työhistoriani) keräämisestä, käsittelystä ja luovuttamisesta. Tutkimuksen sisältö on kerrottu minulle myös suullisesti ja olen saanut riittävän vastauksen kaikkiin tutkimusta koskeviin kysymyksiini. Tiedot antoi minulle Eerika Kauppinen.

Olen saanut riittävät tiedot oikeuksistani tutkittavana, tutkimuksen tarkoituksesta ja sen toteutuksesta sekä tutkimuksen hyödyistä ja riskeistä. Minulla on ollut riittävästi aikaa harkita osallistumistani tutkimukseen.

Ymmärrän, että tähän tutkimukseen osallistuminen on vapaaehtoista. Minulla on oikeus kieltäytyä siitä sekä peruttaa tutkimukseen antamani suostumus milloin tahansa tutkimuksen aikana ilman perusteluita ilmoittamalla siitä tutkimushenkilökunnalle.

Ymmärrän, että tietojani käsitellään luottamuksellisesti. Tutkimuksen yhteydessä henkilötietojani voidaan käyttää tieteellisessä julkaisutoiminnassa tutkimustiedotteessa kuvatulla tavalla.

Tutkimuksesta kieltäytymisestä tai suostumuksen peruuttamista ei aiheudu minulle kielteisiä seurauksia eikä se vaikuta kohteluuni tai saamaani hoitoon millään tavalla. Olen tietoinen siitä, että mikäli peruutan suostumukseni tai osallistumiseni tutkimukseen keskeytyy muusta syystä, siihen mennessä kerättyjä tietojani voidaan edelleen käsitellä tässä tutkimuksessa, mikäli tutkimuksen toteuttaminen sitä vaatii ja lainsäädäntö sallii sen tai edellyttää sitä.

Allekirjoituksellani vahvistan osallistumiseni tähän tutkimukseen ja suostun vapaaehtoisesti tutkittavaksi sekä ymmärrän, että henkilötietojani käsitellään osana tätä tutkimusta.

(Paikka) __. __ 20__

(Paikka) __. __ 20__

Suostun osallistumaan tutkimukseen:

Suostumuksen vastaanottaja:

Tutkittavan allekirjoitus

Tutkijan allekirjoitus

Nimen selvennys

Nimen selvennys

Virka/toimi

LIITE 3: HAASTATTELUKYSYMYKSET JA - RUNKO

Tutkimuksen tarkoituksena on selvittää, miten kyberturvallisuus on otettu huomioon riskien, uhkien ja haavoittuvuuksien osalta ja kuinka kyberturvallisuuden vastuut on jaettu ja kyberturvallisuutta seurataan, hallitaan ja raportoidaan tietoverkkoon kytkettyjen fyysisiä lääketieteellisten laitteiden osalta.

1. Taustatiedot

- a. Haastateltavan nimi, organisaatio ja rooli

2. Lääketieteelliset laitteet & kyberturvallisuus nykytila

Lääketieteellisenä laitteena käsitellään tässä haastattelussa tietoverkkoon kytkettyjä fyysisiä laitteita terveydenhuollossa. Fyysisellä lääketieteellisellä laitteella tarkoitetaan esimerkiksi lääkinnällistä instrumenttia, laitetta tai välinettä eli ulkopuolelle haastattelun rajauksesta jäävät esimerkiksi erilaiset ohjelmistot. Tietoverkkoon kytkettävällä lääketieteellisellä laitteella tarkoitetaan laitetta, jolla on ominaisuus, jolla pystytään ottamaan yhteys tietoverkkoon (esimerkiksi sykemittari, joka välittää potilaan syketiedot lääkärin tabletille bluetoothin avulla).

- a. Miten riskejä pyritään hallitsemaan organisaatiossa yleisesti?
 - i. Miten vastuut on järjestetty?
 - ii. Käytetäänkö viitekehyksiä? Onko olemassa formaalia prosessia tms.?
- b. Millaisia kyberriskejä ja -uhkia on tunnistettu ja miten niitä pyritään tunnistamaan tietoverkkoon kytketyissä fyysisissä lääketieteellisissä laitteissa?
 - i. Kuinka niihin on reagoitu?
 - ii. Sovelletaanko riskienhallinnassa jotain formaalia viitekehystä (esim. ISO/IEC 80001)?
 - iii. Miten tietosuojaan (potilaiden henkilötietojen käsittelyyn) liittyviä riskejä pyritään tunnistamaan? Esim. tehdäänkö uusien laite-/teknologiahankintojen yhteydessä säännönmukaisesti tietosuojaa koskeva vaikutustenarviointi?
- c. Millaisia potentiaalisia vaikutuksia edellä mainittuihin riskeihin liittyy?
- d. Millaisiin toimenpiteisiin riskien hallitsemiseksi on ryhdytty ja mitä on mahdollisesti suunnitteilla?

- e. Ovatko riskit lääketieteellisiin laitteisiin realisoituneet ja jos ovat, niin minäkalaisia seurauksia niistä on syntynyt?

3. Kyberturvallisuuden hallinta & valvonta

- a. Miten ja milloin laitteiden turvallisuutta käytännössä arvioidaan/validoidaan?
 - i. Tehdäänkö esim. tietoturvatestausta? Kuinka säännöllistä ja kattavaa testaaminen on?
 - ii. Luotetaanko laitevalmistajien antamiin tietoihin (esim. varmennuslausunnot, sertifikaatit)?
- b. Miten laitteisiin liittyviä haavoittuvuuksia hallitaan niiden elinkaaren ajan?
 - i. Esim. miten tieto laitteisiin liittyvistä haavoittuvuuksista saavuttaa organisaation ja miten tietoon reagoidaan?
 - ii. Seurataanko esim. viranomaisten tai laitevalmistajien antamia varoituksia?
- c. Miten pääsyä laitteisiin kontrolloidaan/valvontaan?
 - i. Sisältäen laitteiden huolto, vikadiagnostiikka, muut kolmansien osapuolten etäyhteydet
- d. Miten turvallisuuspoikkeamia (esim. epäilyttävä verkkoliikenne, haittaohjelmatartunnat) havainnoidaan?
 - i. Ovatko laitteet 24x7 valvonnan piirissä?
 - ii. Kuinka usein poikkeamia havaitaan? Millaisia vaikutuksia niillä on ollut? Onko potilasturvallisuus tai potilaiden tietosuojaa vaarantunut? Onko poikkeamista informoitu viranomaisia? *(Mietittävä ovatko organisaatiot valmiita vastaamaan näihin kysymyksiin.)*
- e. Onko olemassa protokollaa tai toimintamallia, joka kertoisi kuinka toimia, jos kyberuhka ja/tai haavoittuvuus huomataan tietoverkkoon kytketyissä fyysisissä lääketieteellisissä laitteissa?
- f. Miten hoitohenkilökuntaa ja potilaita on informoitu laitteisiin liittyvistä kyber- tai tietosuojariskeistä?
 - i. Tuleeko henkilökunnalta tai potilailta kysymyksiä aiheeseen liittyen?
 - ii. Miten tiedotus tapahtuu, onko säännöllistä?

4. Kyberturvallisuus & hankinta

- a. Millaista kyberturvallisuuteen liittyvää yhteistyötä laitevalmistajien kanssa harjoitetaan? Onko se riittävää/toimivaa?
- b. Miten kyberriskit on otettu huomioon hankinnoissa?
 - i. Miten kyberturvallisuus huomioidaan tarjouksia arvioitaessa?
 - ii. Miten kyberturvallisuus on sisällytetty sopimusehtoihin?
 - iii. Kuka vastuussa/miten vastuutettu organisaatiossa?

5. Kyberturvallisuus & vastuu lääketieteellisistä laitteista organisaatiossa

- a. Onko tietoverkkoon liitettyjen fyysisten lääketieteellisten laitteiden turvallisuudesta sovittu vastuita?
 - i. Kuka/ketkä vastuussa turvallisuudesta liittyen hoitoyölaiteiden turvallisuuteen (IT olemassa, mutta entä hoitotyössä käytettävät laitteet)? Onko vastuita määritelty koko laitteen elinkaaren ajaksi?
 - ii. Kuka vastuussa kehityksestä ja jatkuvuudesta?
 - iii. Onko vastuista, seurannasta ja hallinnasta ohjeistuksia ja päivitetäänkö niitä?
 - iv. Miten edellä mainittuja asioita seurataan ja raportoidaan?
- b. Onko olemassa päivitettyä listausta organisaation lääketieteellisistä laitteista?