Teemu Parviainen

KYBERTURVALLISUUDEN UHAT TERVEYDENHUOLLOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2022

TIIVISTELMÄ

Parviainen, Teemu
Kyberturvallisuuden uhat terveydenhuollossa
Jyväskylä: Jyväskylän yliopisto, 2021, 26 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Seppänen Ville

Tässä tutkielmassa tarkastellaan kyberturvallisuuden haasteita terveydenhuollossa ja pyritään löytämään ratkaisuja potilasturvallisuutta koskeviin kysymyksiin. Tutkielmassa käydään läpi kyberturvallisuuden perussananstoa ja perehdytään kyberhyökkääjien motiiveihin. Aikaisemmin terveydenhuolto on pääosin välttynyt kyberhyökkäyksien vaaroilta, mutta on viime vuosien aikana noussut yhdeksi suosituimmaksi kyberhyökkäysten kohteeksi. Kyberhyökkäysten äkillinen lisääntyminen on tehnyt haittaa myös terveydenhuollon maineelle ja luottamukselle. Potilastietojärjestelmät sisältävät paljon henkilökohtaisia tietoja, joita hyökkääjä voi hyödyntää taloudellisen tai poliittisen aseman parantamiseksi. Tutkielma osoittaa kyberturvallisuuden haavoittuvuuksien johtuvan useista tekijöistä, kuten turvallisuuteen käytetystä niukasta budjetista tai muiden alojen standarteista, joita on monitulkintaisesti sovellettu terveydenhuollossa. Tutkielmassa käy ilmi, että nopea terveydenhuollon toimintaympäristön digitalisoituminen on antanut hyökkääjille uusia mahdollisuuksia, joihin ei ole valmistauduttu tarpeeksi hyvin. Ongelmien ratkaisuun löytyy useita keinoja, kuten resurssien uudelleen kohdentaminen, terveydenhuoltoon räätälöityjen standartien kehittäminen ja vastuun jakaminen yhdessä terveydenhuollon verkostoon kuuluvien sidosryhmien kanssa.

Asiasanat: kyberturvallisuus, kyberuhka, terveydenhuolto, haavoittuvuudet

ABSTRACT

Parviainen, Teemu
Cybersecurity threats in healthcare
Jyväskylä: University of Jyväskylä, 2021, 26 pp.
Information Systems, Bachelor's Thesis
Supervisor: Seppänen, Ville

This bachelor's thesis examines the challenges of cybersecurity in healthcare and seeks to find solutions to patient security issues. The thesis reviews the basic vocabulary of cybersecurity and the motives of cyber attackers. In the past, healthcare has mostly avoided the dangers of cyber-attacks, but has now become one of the most popular targets of cyber-attacks in recent years. The sudden increase in cyber-attacks has also damaged the reputation and trust of healthcare organizations. Patient information systems contain a lot of personal information that an attacker can use to improve their financial or political position. The thesis shows that vulnerabilities in cybersecurity are due to several factors, such as the limited budget spent on security and the ambiguity of standards from other industries that have been applied in healthcare. Also, that the rapid digitalization of the healthcare operating environment has given attackers new opportunities for which healthcare was not properly prepared. There are several ways to address these issues, such as reallocating resources, developing tailor-made standards for healthcare, and sharing responsibilities with stakeholders in the healthcare network.

Keywords: cybersecurity, cyber threat, healthcare, vulnerabilities

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Monet alat ovat altistuneet kyberhyökkäyksille vuosikymmenten ajan, ja terveydenhuolto on ollut sivussa seuraajan roolissa. Tällä hetkellä tilanne on kuitenkin muuttunut ja terveydenhuollosta on tullut yksi kyberuhille eniten altistuneimmista aloista. Kyberuhat voivat toteutuessaan vaarantaa yhteiskunnalle tärkeitä toimintoja, kuten veden tai virran saannin. Onnistuneet terveydenhuoltoon kohdistuneet kyberhyökkäykset ovat olleet uutisotsikoissa ja, jopa 110 miljoonan yhdysvaltalaisen potilaan tiedot olivat vaarassa yksinään vuonna 2015 (Martin ym., 2017, s. 1). Kyberhyökkäykset ovat monikertaistuneet viimevuosien aikana ja muodostavat globaalin ongelman. Terveydenhuoltojärjestelmät ympäri maailmaa ovat huomanneet digitaalisen teknologian parantavan kliinisiä lopputuloksia, mutta useat haittaohjelmista johtuvat kyberhyökkäykset ovat aiheuttaneet kriittisen ongelman liittyen potilaiden yksityisyyteen, sekä potilasturvallisuuteen. Monien potilaiden yksityiset potilastiedot ovat vaarassa joutua vääriin käsiin.

Tutkielmassani keskityn tunnistamaan mahdollisimman kattavasti terveydenhuollon digitaalisen kehityksen ja toimintaympäristön muutosten aiheuttamia kyberhaavoittuvuuksia, sekä mahdollisia ratkaisuja potilasturvallisuuden parantamiseksi. Vaikka tutkielman näkökulma painottuu kyberturvallisuuteen, käsitellään tutkimuksen teemoja osin myös tietoturvallisuuden näkökulmasta, sillä nämä aihealueet risteävät osittain keskenään. Tutkielman tutkimuskysymyksiä on kaksi ja ne ovat:

1. Mitkä ovat tyypillisimmät terveydenhuoltoon kohdistuvat kyberuhat?
2. Miten potilastietojen turvallisuus voidaan varmistaa tulevaisuudessa?

Näihin kysymyksiin pyrin löytämään vastauksia kirjallisuuskatsauksen keinoin analysoimalla useita eri tutkimuksia ja tieteellisiä artikkeilta. Kirjallisuuskatsauksessa käytetyt lähteet ovat pääosin haettu Jykdokista, Google Scholarin ja IEEE Xplore Digital Libaryn tietokannoista. Tavoitteena on ollut, että lähteinä on käytetty vertaisarvioituja tieteellisiä artikkelita, joita on haettu pääosin hakusanoilla ”cybersecurity”, ”cyberthreats” ja ”healthcare”. Suurin osa

lähdekirjallisuudesta ovat viimeisen kymmenen vuoden ajalta, sillä kyseessä on ajankohtainen teema, josta on herännyt paljon keskustelua viime vuosien aikana.

Motivaatio tutkimukselle syntyi useista potilasturvallisuuteen liittyvistä haasteista ja aiheen teemojen ajankohtaisuudesta. Selvitystyössä kävi ilmi, että terveydenhuollon tarvitsee jatkuvasti kehittää omaa toimintaansa parantaakseen potilastietojen turvallisuutta. Yhteistyö ja vastuunjako terveydenhuollon kanssa samaan verkostoon kuuluvien kanssa osoittautui tärkeäksi turvallisuuden kehityksen kannalta. Terveydenhuollon rajalliset resurssit ja äkillinen digitalisaatiosta johtuva toimintaympäristön muutos, johon ei ole osattu reagoida ennakoivasti ovat osasyitä vallitsevaan tilanteeseen, joka vaatii toimenpiteitä terveydenhuollon organisaatioiden, mutta myös päättäjien osalta tarkennettujen standartien muodossa.

Tutkielman toisessa luvussa esitelen kyberturvallisuuden määritelmiä ja perussanastoa, jotka ovat tutkielman kannalta tärkeitä. Pyrin myös havainnollistamaan kyberturvallisuuden, tietoturvallisuuden ja teknisen turvallisuuden toimintakenttää. Samalla esittelen yleisimpiä kyberuhkia, joita kohdataan terveydenhuollossa. Kolmannessa luvussa tutustutaan digitalisaation aiheuttamiin haasteisiin terveydenhuollon toimintaympäristössä, joita ilmenee uusien teknologioiden implementoinnissa ja lääkinnällisten laitteiden käyttöönotossa. Neljännessä kappaleessa puolestaan esitellään tutkimuskirjallisuuden pohjalta löydettyjä strategisia ratkaisuja ja toimintamalleja, joiden avulla kyberuhille altistumisen riskiä pyritään pienentämään. Johtopäätösten jälkeen teen yhteenvedon tutkimuksesta, samalla pohtien jatkotutkimustarvetta.

2 KYBERTURVALLISUUDEN KÄSITTEISTÄ

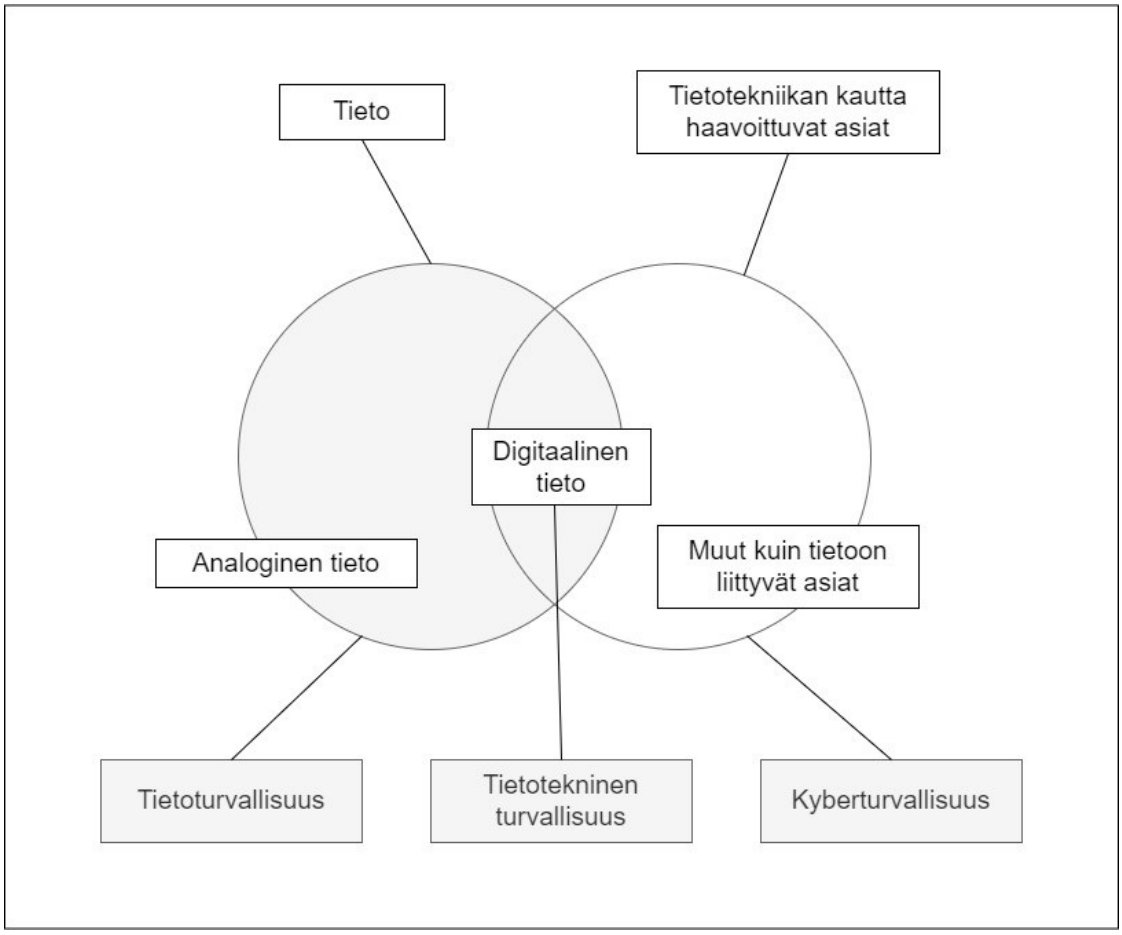
Tässä kappaleessa tutustumme kyberturvallisuuden ja siihen liittyvien käsitteiden määrittelyyn, samalla antaen esimerkkejä kyberturvallisuuden yhtymäkohdista terveydenhuoltoon. Viime vuosien aikana kyberturvallisuus on noussut laajalti käsitellyksi termiksi ja se on omaksuttu monien eri toimijoiden kesken. Kuten useiden uusien termien kanssa myös kyberturvallisuuden määritelmän kohdalla näyttää olevan hyvin vähän ymmärrystä siitä, mitä termi todella sisältää. Termin väärin käyttäminen epävirallisessa kontekstissa ei välttämättä tuota ongelmia, mutta organisaatioiden sisäisessä ja ulkoisessa toiminnassa se voi aiheuttaa paljonkin sekaannusta, jos termillä nähdään olevan moninaisia merkityksiä. (Coventry & Branley, 2018.)

2.1 Kyberturvallisuuden määrittelyä

Kyberturvallisuus on hyvin laajasti käytetty termi ja sen määritelmässä on eroavaisuuksien eri tieteenalojen välillä. Joillakin aloilla, kuten terveydenhuollossa käsite on otettu käyttöön vasta viimevuosien aikana. Monesti käsitettä nähdään käytettävä tiedotusvälineissä väärin, joka voi johtaa ristiriitoihin alan asiantuntijoiden kesken, samalla vaikuttaen myös tavallisen kansalaisen käsityksiin kyberturvallisuudesta ja sen luonteesta. Turvallisuuskomitean (2018) mukaan kyberturvallisuus tähtää tavoitetilaan, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta voidaan turvata. Kyber- ja informaatioturvallisuuden keskus (CCIS) on määritellyt kybertuvallisuuden liittyvän teknologiaan, mutta kyberturvallisuuteen sisältyy nykypäivänä myös muita osa-alueita. Kyberturvallisuuden tavoitteena on myös suojata kriittinen infrastruktuuri ja terveydenhuollossa, sillä tarkoitetaan etenkin verkko- ja tietoliikenteen, sekä veden ja sähkön toiminnan suojaaminen. Terveydenhuollon järjestäminen vaarantuu, mikäli jokin edellä mainituista osa-alueista ajautuu epäkuntoon. Kyberturvallisuutta ei kuitenkaan voida koskaan täysin taata, sillä teknologian kehit-

tyminen on jatkuvaa ja muuttuva toimintaympäristö tuo jatkuvasti esiin uusia haavoittuvuuksia. (Lehto ym., 2017, s. 44–45.)

Coventry ja Branley (2018) ovat tutkimuksissaan pyrkineet selkeyttämään kyberturvallisuuden käsitteen käyttöä ja määrittämään sen uudelleen ottamalla huomioon useiden yhteisöjen ja organisaatioiden näkemykset. Tätä kautta on pyritty helpottamaan viestintää eri toimijoiden kesken. Heidän mukaansa kyberturvallisuus on lähestymistapa ja siihen liittyvät toimet yhdessä turvallisuusriskien hallintaprosessien kanssa, jota seuraa organisaatioiden ja valtioiden tapa suojella käytettävien tietojen ja resurssien luottamuksellisuutta, eheyttä ja saatavuutta kyberavaruudessa. Kyseinen määritelmä pitää sisällään myös suuntaviivoja, käytänteitä, suojatoimenpiteiden kokoelmat, teknologiat, sekä koulutuksen, joka tarjoaa parhaan suojan kybertoimintaympäristölle ja sen käyttäjille.



KUVIO 1 Tietoturvallisuuden, tietoteknisen turvallisuuden ja kyberturvallisuuden rajapinnat. Suomennos (Simi, 2017).

Kuvio 1 kuvaa tietoturvallisuuden, tietoteknisen turvallisuuden ja kyberturvallisuuden rajapintaa, jossa osa-alueet kietoutuvat toisiinsa organisaation sisältä kuvattuna. Jotta organisaatioiden toiminta voidaan turvata, tulee kaikki edellä mainitut osa-alueet huomioida johtamisen ja riskien hallinnan näkökulmasta. (Simi, 2017.) Jokainen osa-alue pyrkii kohti turvallisuuden päämäärää,

mutta sen saavuttamiseksi käytetään poikkeavia keinoja. Tietoturvallisuuden tavoitteet yhtenevät osittain kyberturvallisuuden tavoitteiden kanssa, sillä tiedon luottamuksellisuus (confidentiality), eheys (integrity) ja tiedon, sekä palveluiden saatavuus (availability) ovat yhteisiä päämääriä. Tätä kutsutaan CIA-malliksi (Nweke, 2017). Tietoturvallisuuden käsite käsittää analogisen tiedon, kuten henkilöstön kokemuksen, toimintatavat ja tiedot, joiden avulla analogista tietoa suojataan. Tietotekninen turvallisuus, josta puhutaan nimellä IT-turvallisuus tai ICT-turvallisuus puolestaan pyrkii keskittymään tietojen, tietojärjestelmien ja tietoverkkojen tekniseen suojaamiseen. Tekniset ratkaisut, tietoturvatuotteet ja tämän lisäksi myös tekninen osaaminen, ovat välineitä turvata teknologinen ja digitaalinen tieto. (Simi, 2017.)

2.2 Kyberhyökkäykset ja kyberuhat

Internetin ja tietokoneiden rooli modernissa yhteyskunnassa on hyvin tunnistettu. Viimeaikaiset kehitykset tietoverkoissa ja kyberavaruudessa ovat roimasti edesauttaneet ihmiskuntaa ja helpottaneet ihmisten arkea. Hienojen saavutusten ja tulosten lisäksi, on uutta teknologiaa myös mahdollista väärinkäyttää henkilökohtaisen edun saavuttamiseksi. Tämän kaltainen kyberavaruuden hyväksikäyttö, jossa suojattuja tietoja käytetään luvatta, vakoillaan, poistetaan verkkoja pois käytöstä, sekä varastetaan tietoja tai rahaa, kutsutaan kyberhyökkäykseksi (Uma & Padmavathi, 2013, s. 1). Tietoturvallisuuskomitean (2018) mukaan termi kyberhyökkäys ei tarkoita ainoastaan tietoverkkohyökkäystä, sillä se viittaa laajempaan käsitteeseen, koska kyberhyökkäyksiä voidaan tehdä myös muilla tavoin. Etenkin sosiaalisen median kanavia hyödyntävät hakkeroinnit ovat yleistyneet ja kohdennetut tietojenkalasteluhyökkäykset ovat kasvaneet. Myös terveydenhuolto tarjoaa paljon tietoa tällaisille hyökkäystavoille. Tämän lisäksi hyökkäyksiin on saatavilla laaja määrä työkaluja. Näitä työkaluja usein käytetään edistyneisiin käyttäjän manipulointihyökkäyksiin. (Lehto ym., 2017, s. 20.) Seuraavassa taulukossa esitellään yleisimpiä ja tyypillisimpiä uhkia terveydenhuollossa.

TAULUKKO 1 Yleisimmät ja tyypillisimmät kyberuhat terveydenhuollossa (Martin ym., 2017, s. 1).

Tietovarkauden taloudellisen hyödyn saamiseksi.	Varastetaan henkilökohtaista dataa, kuten nimiä, osoitteita, henkilöturvatunnuksia tai taloudellisia tietoja.
Tietovarkaus vaikutuksen vuoksi.	Varastettu arkaluontoinen tieto tuodaan julki. Uhreina esimerkiksi julkisuuden henkilöt, poliitikot tai muut korkean profiilin henkilöt.
Kiristyshaittaohjelma.	Varastettu arkaluontoinen tieto tuodaan julki. Uhreina esimerkiksi julkisuuden henkilöt, poliitikot tai muut korkean profiilin henkilöt.

Datan korruptointi.	Tietojen tahallinen vioittuminen, kuten testitulosten peukalointi poliittista tai henkilökohtaista etua tavoitellen.
Palvelunestohyökkäys.	Ruuhkautetaan verkko tai järjestelmä tarpeettomilla pyynnöillä, jonka tavoitteena on kiristää, kostaa tai toimia aktivistina
Yrityssähköpostin vaarantaminen.	Luodaan väärennetty viestintäkanava taloudellisen hyödyn tavoittelemiseen petollisten maksujen ja henkilökohtaisen tiedon hankkimiseen.

Vain noin puolet terveydenhuollon organisaatioista Yhdysvalloissa kokevat kykenevänsä puolustautumaan kyberhyökkäyksiltä ja ne, jotka kohdistavat kyberhyökkäyksiä terveydenhuoltojärjestelmiin näkevät terveydenhuollon sektorin olevan helppo kohde, joka tarjoaa paljon arvokasta dataa. Terveydenhuoltojärjestelmät ovat kyberhyökkäysten uhreja usein rahallisen voiton tavoittelun takia. Kyberhyökkäysten tavoitteena on usein varastaa rahaa, tai immateriaalioikeuksia (Coventry & Branley, 2018, s. 3). Nyt kuitenkin poliittisen vaikutuksen ja sekasorron luominen ovat olleet kyberhyökkäysten tavoitteena kasvavassa määrin. Kyseessä on monikansallinen ongelma, johon myös valtiot osallistuvat. Monet hyökkäykset jäävät huomaamatta tai kokonaan raportoimatta ja vain pieni osa niistä päätyy julkiseen tietoon. Hyökkäyksen tahoa on usein hyvin haastava todistaa tai asettaa vastuuseen teoistaan. Vaikka hyökkääjälle maksetaan esimerkiksi haittaohjelman lopettamisesta, on hyökkääjää vaikea kohdentaa varsinkin, jos maksuvälineenä on Bitcoinin, Dashin, Vergen tai ZCashin kaltaiset kryptovaluutat (Millard, 2017).

2.3 Kyberuhkien aiheuttajat

ENISA:n (2011) mukaan kyberuhkia aiheuttaa monet eri tahot. Kyberuhan aiheuttaja voi löytyä organisaatio sisä- ja ulkopuolelta, mikä muodostaa laajaan joukon toimijoita. Sisäpiirin voi tämänhetkisten työntekijöiden lisäksi kuulua myös aikaisempia työntekijöitä ja nykyisiä tai entisiä palveluntarjoajia. Myös liiketoimintakumppanit, konsultit ja asiakkaat kuuluvat sisäpiiriin. Suurin osa kyberhyökkäyksistä voidaan jäljittää näihin ryhmiin. Sisäisen turvallisuuden kannalta on järkevää tiedostaa, kenellä näistä ryhmistä on hallussaan käyttöoikeuksia esimerkiksi organisaation tietojärjestelmiin. Väärinkäytösten motiiveina voi olla esimerkiksi tilanteen sopivuus, rahastustarkoitus tai kosto.

Kybervandaaleiden joukkoon kuuluu useita eri toimijoita. Hakkerilla tarkoitetaan henkilöä, joka tunkeutuu jonkun toisen tietoverkkoon tai tietojärjestelmään ja samalla käyttää luvatta tämän tietojärjestelmää, ohjelmaa tai palvelua. Haktivisti muodostuu sanoista hakkeri ja aktivismi. Haktivismin tavoitteena on hakkeroida ja levittää tietoa kohdeorganisaatiosta tai vallassa olevista ihmisistä. Näillä tiedoilla pyritään saada aikaan huomioita tai muutosta johon-

kin tiettyyn ennalta määritettyyn asiaan, kuten sananvapauteen tai internetin avoimuuteen. Yksinäiset sudet puolestaan ovat henkilöitä, jotka valmistelevat sekä toteuttavat itse väkivaltaisia tekoja ilman muiden apua. Heillä ei ole komentorakennetta tai tukiverkkoa. Kyberterroristien intresseihin kuuluvat anonyymit maksujen siirrot ja he myös ostavat heitä hyödyttäviä kyberrikoksia palveluina. Kybersotilaat puolestaan ovat usein kansallisesti motivoituneita ja sijoittuvat kyberterroristien, aktivistien ja kybervakoilun välimaastoon. (Lehto ym., 2017.)

AT&T (2015) toi esille, että USA:n hallituksen mukaan kybervakoilu on kaikista merkittävin ja kasvava uhka valtioiden turvallisuudelle, sekä menestykselle. Kybervakoilua suorittaa niin valtiot kuin yritykset. Erinäiset kybervakoiluun erikoistuneet ryhmät ovat kiinnostuneet niin liiketoimintasalaisuuksista kuin kansallisista salaisuuksista, sotilaallisesta luottamuksellisesta tiedosta, aineettomasta tiedosta ja valtioiden poliittisiin prosesseihin vaikuttamisesta. Raja valtiollisen ja teollisen vakoilun välillä on kuin veteen piirretty viiva, etenkin silloin kun suuren monikansalliset toimijat ovat mukana. Sama pätee vihamielisiin aktivistiryhmiin, kilpailijoihin sekä teollisuusvakoiluun. Kybervakoojien taidot ja keinot kehittyvät jatkuvasti ja tämä näkyy valtioiden puolustusstrategioissa. Kehitys on kohti kyberfyysisiä järjestelmiä, joka voi vahingoittaa fyysistä omaisuutta ja aiheuttaa laajoja tappioita kolmansille osapuolille (Lehto, 2021, s. 43).

3 KYBERTURVALLISUUDEN HAASTEET TERVEYDENHUOLLOSSA

IBM Security (2016) antaman tutkimuksen mukaan toimialat, jotka joutuvat eniten kyberhyökkäysten kohteiksi ovat terveystoimiala, valmistus ja tuotanto, pankki- ja rahoitustoimiala, julkishallinto sekä liikenne. Ennen terveydenhuolto seurasi kybersotaa sivussa katsojana, koska hyökkäykset eivät kohdistuneet terveydenhuollon sektoriin, mutta nykyään tilanne ei ole sama. Terveydenhuolto on noussut vuonna 2015 eniten kyberhyökkäyksille altistuneeksi toimialaksi rahoitusalan tilalle. Jopa viisi kahdeksasta suurimmasta terveydenhuollon sektoriin kohdistuvasta hyökkäyksestä sitten vuoden 2010, tapahtui vuoden 2015 ensimmäisen kuukauden aikana. Tästä seurasi yli 100 miljoonan potilastiedon vaarantuminen. Potilastiedot ovat hedelmällistä tietoa rikollisten silmissä, sillä potilastietojen avulla rikollinen voi saada selville potilaasta monia tietoja kuten luottokorttinumeroita, sähköpostiosoitteita, sairasvakuutusnumeroita, työnantajatietoja ja sairaushistoriatietoja. Monet näistä tiedoista ovat vielä vuosien päästä käyttökelpoisia ja niistä maksetaan pimeillä markkinoilla hyvä summa. Kyberrikolliset käyttävät osaa näistä tiedoista tehdäkseen tietojenkalastelu-hyökkäyksiä, petoksia ja identiteettivarkauksia.

Millardin (2017) Terveydenhuollon järjestelmiin kohdistuvat hyökkäykset eivät ainoastaan uhkaa potilaiden identiteettiä ja taloutta, mutta niillä voi olla myös vaikutuksia sairaaloiden toiminnalle, joka voi asettaa potilaan terveyden ja hyvinvoinnin alttiiksi riskeille. Esimerkiksi jotkin sairaalat, jotka ovat altistuneet haittaohjelmille ovat joutuneet viivästyttämään hoitosuunnitelmia ja jopa uudelleenohjaamaan saapuvia ambulansseja, koska pääsy yksikön tietojärjestelmiin oli evätty. Toiminnallisten ja rahallisten seurausten lisäksi kyberhyökkäyksillä on pitkäaikaisia haitallisia vaikutuksia sairaaloiden ja muiden terveydenhuollon yksiköiden maineeseen, sekä palveluihin (Reagin ym., 2018).

Maailmanlaajuinen WannaCry kiristyshaittaohjelma levisi vuoden 2017 toukokuussa voimakkaasta ja kosketti yli 200 000 järjestelmää yli 150 maassa. Vaikka hyökkäys ei kohdistunut ainoastaan terveydenhuoltoon, vaikutti se suorasti Yhdistyneen kuningaskunnan alueella sijaitsevan 50 sairaalan toimintaan. Tämän lisäksi monen muun laitoksen tietojärjestelmät suljettiin ennalta-

ehkäisevästi. Tämä aiheutti huomattavasti häiriötä hoidon toimittamiseen, samalla vaarantaen potilasturvallisuuden. Kyseinen kiristyshaittaohjelma salaa uhrin tiedot, estää pääsyn niihin ja uhkaa julkaista tai poistaa tiedot, jos lunnaita ei makseta. Ainoa keino päästä käsiksi tartunnan saaneeseen tietokoneeseen ja sen tietoihin on maksaa hyökkääjän vaatimat lunnaat tai pyyhkiä järjestelmät tiedot ja käyttää varmuuskopioituja tietoja. (Martin ym., 2017).

3.1 Uusien teknologioiden implementointi terveydenhuollossa

Krusen (2017) mukaan kyberhyökkäykset ovat selvästi kasvava uhka terveydenhuollon toimialalla ja siltä puuttuu systemaattinen valmistautuminen kyberuhkia vastaan. Tämä johtuu osittain siitä, että terveydenhuolto on kohdannut uusia haasteita jatkuvasti muuttuvassa teknologisessa toimintaympäristössä. Uusia teknologioita implementoidaan nopeammin kuin turvallisia järjestelmiä voidaan tehdä tai päivittää puolustaakseen niitä. Terveydenhuollon teknologian käyttöönotto on työläs prosessi, joka vaatii paljon suunnittelua ja implementaatioihin kuluu aikaa. Monet terveydenhuollon organisaatiot investoivat paljon intregroitumiseen, mutta unohtavat samalla panostaa ohjelmistojen päivityksiin (Coventry & Branley, 2018). Kyberrikolliset etsivät jatkuvasti uusia katvealueita terveydenhuollon järjestelmistä, joten järjestelmien pysyminen ajan tasalla on tärkeää turvallisuuden kannalta.

Myös lääkinnällisten laitteiden aiheuttamat uhat voivat vaarantaa sairaaloiden IT-verkkojen ja laitteiden eheyden. Lääkinnälliset laitteet ja tietojärjestelmät sisältävät paljon potilaiden henkilökohtaisia ja lääkinnällisiä tietoja, sekä maksutietoja. Lääkinnälliset laitteet, joita ennen käytettiin irtonaisina muista järjestelmistä, ovat alkaneet muodostamaan yhteyden internettiin ja siten integroitumaan sairaaloiden IT järjestelmien kanssa, jonka johdosta ne eivät enää ole immuuneja kyberhyökkäyksille. (Kruse ym., 2017.) Tällä hetkellä lääkinnällisten laitteiden valmistajat implementoivat ja laajentavat verkkoon liitettyjä lääkintälaitteita, mutta eivät pysty ylläpitämään vauhtia mahdollisten verkkointegraation aiheuttamien kyberturvallisuusuhkien kiertämiseksi.

Ongelmia voi myös muodostua kun käyttöjärjestelmän päivitys on asennettava. Päivityksen tekemisestä on onnistuttava viestimään selkeästi kaikille tahoille, jotka työskentelevät päivitystä koskevien lääkinnällisten laitteiden toiminta-alueella. Nopean muutoksen ympäristössä lääkinnällisten laitteiden toiminnallisuuden varmistaminen voi olla haasteellista ja tapauksia laitteiden toimintakunnon heikkenimestä on ilmennyt. Ongelmat laitteissa tai laitteistossa on jopa aiheuttanut hoidon viivästymisen tai keskeytymisen. (Coronado & Wong, 2014).

Terveydenhuollon organisaatiot joutuvat jatkuvasti tasapainotella turvallisuuden, asiakaskokemuksen sekä käytännöllisyyden välillä. Etenkin Yhdysvalloissa hallitus on päättänyt lisätä teknologiaa terveydenhuollon instituutioissa, sekä laajentaa sähköisesti tapahtuvaa tiedonvaihtoa (Rowe,

2016). Tämä lisää terveydenhuollon yksiköiden riippuvaisuutta internettiin, joka on osaltaan vaikuttanut siihen, että terveydenhuollon organisaatiot Yhdysvalloissa haluavat toimia hallituksen ohjeiden mukaan ja satsaavat noin 95 prosenttia IT-budjeteistaan uuden teknologia implementointiin ja käyttöönottoon, kun alle viisi prosenttia budjetista käytetään turvallisuuteen (Kruse ym., 2017).

Teknologinen kehitys ja uudet poliittiset aloitteet ovat laajentaneet terveydenhuollon altistumista kyberhyökkäyksille dramaattisesti. Vaikka kyberhyökkäyksille altistuminen ja niiden tiheys ovat muuttuneet, on hyökkääjien motiivit pysyneet samana. Tutkimukset viittaavat siihen, että lääketieteellinen data ja informaatio ovat noin 20-50 kertaa arvokkaampia kyberrikollisille kuin henkilökohtaiset taloudelliset tiedot. (Rowe, 2016.)

3.2 Lääkinnälliset laitteet

Viimeaikainen tekninen kehitys on johtanut muutoksiin terveydenhuollon toiminnassa, jolla on nyt enemmän kapasiteettia ja kykyä parantaa potilaiden hoitoa. Hyvä esimerkki tästä on lääkinnällisten laitteiden ja muiden kliinisten järjestelmien yhteenliitettävyyden lisääntyminen. Tämä yhteenliitettävyys jättää lääkinnälliset laitteet alttiiksi tietoturvaloukkauksille ja samalla muut samaan verkkoon kytketyt tietojärjestelmät ovat haavoittuvaisia eri tyyppisille haittaohjelmille (Abraham ym., 2019). Nämä haavoittuvuudet herättävät huolta lääkinnällisten laitteiden vaikutuksista suoraan kliiniseen hoitoon, sekä potilasturvallisuuteen. Lääketieteellisten laitteiden, verkkojen, ohjelmistojen ja käyttöjärjestelmien integrointi tuo mukanaan monimuotoisia haasteita niin johtamisessa kuin turvallisuudessa. Näitä haasteita yhdessä kutsutaan kyberturvallisuuden haavoittuvuuksiksi. (Williams & Woodward, 2015, s.305.)

3.2.1 Lääkinnällisten laitteiden määritelmiä

Lääkinnällisten laitteiden määritelmä on muovautunut viimevuosikymmenten kuluessa usean kertaan yhdistämättömistä laitteista, langattomasti uudelleen ohjelmoitaviin laitteisiin, joista viimeisimpinä ovat ohjelmistot ja sovellukset. Tämän takia on hyvä määritellä mitä lääkinnällisellä laitteella tarkoitetaan verkottuneessa mobiilimaailmassa. Williams & Woodward (2015) määritelevät lääkinnällisen laiteen olevan instrumentti, laite työväline, kone, apuväline, implantti, IVD-laite tai muu vastaava esine mukaan lukien komponentti tai lisävaruste, jota on tarkoitettu käytettäväksi sairauden tai muiden tilojen diagnosoinnissa tai sairauksien parantamisessa, lieventämisessä, hoidossa tai ehkäisyssä. Yhdysvaltain elintarvike- ja lääkeviraston (2019) mukaan lääkinnällisten laitteiden määritelmää tulisi laajentaa huomioiden mobiililaitteilla käytettävät terveys- ja hyvinvointisovellukset. Lisäksi lääketieteellisiin laitteisiin upotettujen ohjelmistojen myötä ohjelmisto

lääketieteellisenä laitteena (Software as Medical Device, SaMD) on jo nykypäivää. Tämän takia hyvin kehitettyä ja validoitua ohjelmistoa, joka vaikuttaa merkittävästi ja positiivisesti potilaan hoitoon, voidaan pitää lääkinnällisenä laitteena. (IMDRF, 2014, s. 7-9.)

3.2.2 Lääkinnällisten laitteiden haavoittuvuudet ja seuraukset

Razaque (2019) tuo esille, että langattomien verkkoyhteyksien lisääntynyt käyttö ja lääkinnällisten laitteiden liittäminen internettiin, sekä halu käyttää niillä kerättyjä tietoja muissa terveydenhuollon järjestelmissä on altistanut lääkinnälliset laitteet avoimemmiksi kyberuhille. Verkkoon liittämisen takia vastuu laitteen toimivuudesta, tietojen eheydestä, luottamuksellisuudesta ja potilaan yksityisyydestä on nyt valmistajien, terveydenhuollon palveluntarjoajien ja potilaiden vastuulla Monet lääkinnällisiin laitteisiin kohdistuvat haasteet johtuvat osin hallinnollisista syistä ja terveydenhuollon organisaatioiden valmistautumisen puutteesta. Nopeat muutokset terveydenhuollon digitaalisessa toimintakentässä on osin lisännyt turvallisuusriskien tiedostamattomuutta..

Lääkinnällisten laitteiden luottamuksellisuus saattaa vaarantua, jos luvattomat toimijat pääsevät niihin käsiksi. Tämä johtuu usein huonojen kulunvalvontatoimenpiteiden vuoksi. Tästä voi seurata terveydenhuollon organisaatiolle huonoa mainetta määräysten noudattamatta jättämisen takia, joka puolestaan voi johtaa oikeudenkäyntiin ja sitä kautta taloudellisiin seurauksiin oikeudenkäyntikulujen muodossa. Datan ja informaation eheyteen voidaan vaikuttaa negatiivisesti laitteiden huonolla konfiguraatiolla, tietojen turmeltumisen johdosta tai tietojen luvattomasta käsittelystä. Seurauksina voi olla potilasturvallisuuden vaarantuminen mahdollisten virheellisten kliinisten tutkimustulosten takia. Lisäksi hyökkäyksen kohteena olevan laitteen käyttäminen ei ole potilaan turvallisuuden kannalta järkevää. Datan saatavuus voi vaarantua, jos pääsy tietoihin tai laitteeseen on rajoitettu. Tällä voi olla vaikutus potilasturvallisuuteen, koska potilaan hoitoon tarvittaviin tietoihin ei ole pääsyä, joka voi vaikuttaa tuleviin kliinisiin päätöksiin. On myös mahdollista, että potilasturvallisuus vaarantuu, jos puuttuvaa informaatiota ei huomata. (Williams & Woodward, 2015.)

3.3 Verkot ja langattomat haavoittuvuudet

Williamsin ja Woodwardin (2015) mukaan Verkkoa pitkin suoritetut hyökkäykset tähtäävät löytämään verkkoon liitettyjen laitteiden tai tietokoneiden haavoittuvuuksia. Kolme yleisintä hyökkäysten kohdetta ovat verkkopalvelimet, tietokannat ja sovellusohjelmistot. Verkkopalveluiden käyttö lääkinnällisten laitteiden yhteydessä on yleistä, koska se tarjoaa lääkinnällisille laitteille graafisen käyttöliittymän, jonka avulla laitetta on helpompi käyttää. Tämänkaltaisen käyttöliittymän hyödyntämisen huonona puolena on se, että verkkopalveluissa on usein monia haavoittuvuuksia, joita hyökkääjä voi hyödyntää. Nykypäivänä

monia ilmaisia hyökkäystyökaluja on ladattavissa, joiden avulla verkkopalveluiden haavoittuvuudet voidaan selvittää ja hyökkääjä voi saatujen tietojen avulla muodostaa ja suunnitella tilanteeseen sopivan hyökkäysmetodin.

Useissa laitteissa ja järjestelmissä on jonkinlainen tietokanta tai tietovarasto, jossa kyseisen laitteen tietoja säilytetään. Monissa tietokannoissa käytetään strukturoitua kyselykieltä, kuten SQL-kieltä ja jos sitä ei ole määritetty oikealla tavalla, on kyseinen järjestelmä hyvin altis SQL-injektioille. SQL-injektiot ovat vakavia hyökkäyksiä tietokantoja kohtaan, sillä hyökkääjä voi lukea kaiken informaation, joka tietokantaan on kirjattu ja samalla muokata niitä. (Williams & Woodward, 2015, s. 309.) Suuri osa sairaaloista on siirtynyt paikallisesta tietojen tallennuksesta pilvitallennukseen, joissa potilastietoja säilötään. Niihin käytetyt yhteydet eivät kuitenkaan ole kaikista turvallisia ja esimerkiksi lääkinnällisten laitteiden lähettämä data pilvipalveluun verkon välityksellä aiheuttaa haavoittuvuuksia useille kyberuhkien muodoille. (Razaque ym., 2019)

Sovellusohjelmistoon kohdistuvat hyökkäykset voivat puolestaan tarkoittaa mitä tahansa ohjelmistoa, joka toimii laitteessa, oli se sitten kumpi tahansa edellä mainituista. Tämänkaltainen hyökkäys onnistuu todennäköisesti siellä, missä ohjelmisto ei ole käynyt läpi tiukkaa haavoittuvuustestausta, jonka avulla voidaan määrittää mahdollisia haavoittuvuuksia. Monet onnistuneet kyberhyökkäykset ovat hyödyntäneet koodin haavoittuvuuksia, joita ei ole testattu ennen käyttöönottoa oikeassa toimintaympäristössä. (Williams & Woodward, 2015, s. 309–310.)

4 KYBERTURVALLISUUDEN KEHITTÄMINEN TERVEYDENHUOLLOSSA

Millardin (2017) mukaan kyberturvallisuuden tavoitteena on suojata potilaiden henkilötietoja, sekä suojattuja terveystietoja, joita käsitellään melkein jokaisessa terveydenhuollon yksikössä, joko yhdessä tai useammassa tietojärjestelmässä. Muilla aloilla kuten rahoitusalalla kyberturvallisuuskysymyksiä on kohdattu vuosikymmenten ajan, joten resursseja on osattu kohdistaa turvallisuuteen, koska sitä on pidetty osana välttämätöntä turvallisuusstrategiaa. Terveydenhuollossa puolestaan on vaikeuksia löytää riittävästi resursseja turvallisuuteen, koska kyberturvallisuuteen liittyvät ongelmat ovat vielä suhteellisen uusia.

AT&T (2017) tuo raportissaan esille keinoja, joiden avulla, joilla organisaatiot voivat parantaa suojautumista kyberuhilta. Näitä ovat kulttuuri, suunnittelu, työkalut, kumppanuudet ja rahoitus. Kyberturvallisuuden tulisi olla osa organisaation kulttuurirakennetta, joka tulee esille koko organisaation arjessa. Liiketoimintaa suunnitellessa ja päätöksiä tehdessä kyberturvallisuuden tulisi kulkea päätösten rinnalla, jotta turvallisuusriskit voidaan minimoida. Organisaatioille tulisi olla aina ajantasaiset palvelut ja ratkaisut, jotka auttavat suojautumaan kyberhyökkäyksiltä. Organisaation johdosta lähtien tulisi olla tietoinen teknisistä termeistä, kuten uhkien hallinta, turvallisuustasot ja pilvipohjaiset hallintapalvelut, jotta johdolla olisi käsitys jopa yksittäisten laitteiden suojauksen tilasta. Näitä työkaluja voi hallita organisaation sisältä tai yhteistyössä ulkoisten toimijoiden kanssa. On useita palveluntarjoajia ja konsulttifirmoja, jotka auttavat kyseisten työkalujen kanssa.

Organisaation on myös järkevää auditoida käytössä olevaa tietoturvaratkaisua luotettavan partnerin kanssa esimerkiksi testihyökkäysten ja toimintatapojen testausten avulla. Kumppanuuksilla tarkoitetaan niiden sidosryhmien identifioimista, joiden kanssa voidaan parantaa yhteisen verkoston turvallisuutta. Näille sidosryhmille tulisi asettaa turvallisuuden suhteen yhteisiä tavoitteita. Uusia investointeja tehdessä tulisi varmistaa kyberturvallisuuteen ja tietoturvallisuuteen liittyvät tarpeet ja uusien IT-projektien yhteydessä tulisi huomioida asianmukaiset kyberturvallisuuteen liittyvät ratkaisut. Investointi päätökset

tulisi tehdä riskien, turvallisuuden, käytettävissä olevien tietolähteiden ja datan turvallisuuden pohjalta. (AT&T, 2017, s. 30.)

4.1 Häiriönsietokyky ja tietoisuus

Kybertuvallisuus ei voi koskaan olla täysin turvallisia ja terveydenhuollonjärjestelmien haavoittuvuus on todellinen uhka. Kuitenkin yksilöt ja organisaatiot voivat toiminnallaan vaikuttaa nykyisten järjestelmien turvallisuuteen. Kyberturvallisuuden tavoitteena tulisi olla järjestelmien häiriönsietokyvyn vahvistaminen. Häiriönsietokyvyn ylläpitämisellä kyetään ylläpitämään turvallisempi järjestelmä, jolloin hyökkäyksen tapahtuessa, pystytään se myös todennäköisesti torjumaan. Hyvin yksinkertainen tapa parantaa organisaation häiriönsietokykyä on ylläpitää turvattua varmuuskopioita ja kärsiä siten vähemmän mahdollisista vahingoista. Riskien lieventäminen (mitigation) on johtamisstrategia, jota käytetään potentiaalisen hyökkäyksen seurauksien minimoimiseen. Olennaisena asiana on ymmärtää hyökkäyksen aiheuttamien vahinkojen suuruus ja mitä turvallisuuden osa-aluetta hyökkäys koskee. (Williams & Woodward, 2015, s. 308.)

Työntekijöiden kouluttaminen on erityisen tärkeää, sillä Conaty-Buckin (2017) mukaan henkilöstä voi myös aiheuttaa riskin kyberuhille. Ihmiset muodostavat kyberturvallisuuden heikoimman lenkin ja terveydenhuollon organisaatioiden tulisi informoida ja kouluttaa kaikkia käyttäjiä sen vaaroista. Loppukäyttäjät eli klinikoiden laskutus-, aikatauluvastaavat, sekä potilaat ja hoitajat, jotka yhdistävät omat henkilökohtaiset laitteensa sairaalan verkkoon voivat tahattomasti tai tarkoituksella uhata terveydenhuollon kyberturvallisuutta (Argaw ym., 2020, s. 5). Terveyslaitosten tulisi arvioida ja tunnistaa tiedon puutteita, jotta käyttäjille voidaan tarjota asianmukaista ja tehokasta koulutusta. Loppukäyttäjien on tärkeä tiedostaa riskit, joita he voivat tahattomalla toiminnallaan aiheuttaa (Coronado & Wong, 2014, s. 27). Kyberturvallisuusongelmat koskettavat kaikkia, ja organisaation jäsenten kouluttaminen voi tehostaa yhteistyötä ja auttaa kohdentamaan tarvittavat resurssit kyberturvallisuuden uhkien torjumiseen. Siksi tarvitaan konkreettisia ohjeita ja valistusta siitä, mitä riskejä esimerkiksi mobiililaitteet voivat aiheuttaa yksityisyyteen, ja tiedon eheyteen tai miten irrotettavat tallennuslaitteet voivat lisätä haittaohjelmien suorittamisen riskiä. Loppukäyttäjille olisi hyvä luoda koulutusohjelmia, joissa käsitellään erilaisia toimintatapoja esimerkiksi sähköpostiviestien ja tietojenkalasteluun liittyvissä tilanteissa. Kaikkien laitteiden käyttäjien kouluttaminen perusturvatoimenpiteisiin, kuten henkilökohtaisten mobiililaitteiden ja USB-muistitikkujen käyttöön, voi myös olla suositeltavaa. (Coronado & Wong, 2014.)

4.2 Terveydenhuollon turvallisuusstandartit

Hyvän häiriönsietokyvyn lisäksi tulisi terveydenhuoltoon liittyviä yleisiä turvallisuus standardeja kehittää. Standartit ovat ainoastaan silloin hyödyllisiä, jos ne ovat asianmukaisia ja niitä noudatetaan. Tällä hetkellä terveydenhuolto sektorille ei ole erityisesti sitä varten suunniteltuja standardeja tai niitä ei ole johdonmukaisesti sovellettu. Iso-Britannian Kyberperusteiden järjestelmän (2015) mukaan hajanainen hallinto, valtava yhteenliitettävyys, laaja saatavuus, sääntelypaineen puute ja rajalliset resurssit osoittavat terveysalalle suunnattavan kyberturvallisuuden standardien ja ratkaisujen tarpeen. Standartit tarjoavat hyviä käytäntöjä, mutta niitä on sovellettava ja tulkintatavat eroavat. Vaikka on olemassa useita kansainvälisiä standardeja, jotka ovat edellytyksiä lääkinnällisten laitteiden sertifioinnille, on ongelmana niiden rajoittuneisuus vain kehitykseen ja riskiarviointiprosessin suunnitteluun. Nämä standartit eivät keskity kyberturvallisuuden edellyttämään spesifisyyteen kompleksissa terveydenhuollon ympäristössä. (Williams & Woodward, 2015, s. 312–313)

4.3 Sidosryhmät ja verkostot

Rowen tutkimuksien (2017) mukaan terveydenhuollon organisaatiot ovat hiljalleen ymmärtäneet, että turvallisuustoimien tulee kantaa oman organisaation ulkopuolelle. Tavarantoimittajat ja asiakkaat ovat terveydenhuollon organisaatioiden kanssa osa samaa verkostoa, jotka käsittelevät yhtä lailla arkaluonteista tietoa. Terveydenhuollon toimiala alkaa nyt tutkia tarkemmin turvallisuuskäytäntöjä ja toimittajien kanssa solmittuja sopimuksia varmistaakseen, että nämä suhteet eivät luo lisää haavoittuvuuksia, joita rikolliset voisivat hyödyntää. Vastuun jakaminen terveydenhuollon ja valmistajien välillä voi kuitenkin Millardin (2017) mukaan johtaa vastakkaiseen suhteeseen. Sen sijaan, että molemmat osapuolet työskentelisivät yhdessä varmistaakseen korkeammat turvallisuuskäytännöt, on mahdollista, että heistä voi tulla kilpailijoita, jotka pyrkivät välttämään vastuuta sen jakamisen sijaan. Siksi onkin tärkeää määrittää vastuualueet ja tilivelvollisuudet, jotta tulevat hyökkäykset voidaan estää tehokkaasti. Terveydenhuollon organisaatiot myöntävät, että ei ole olemassa yhtä ratkaisua, joka vastaisia heidän turvallisuushaasteisiinsa. Ajattelun muutos voi kuitenkin poikia uudenlaisia monikerroksisia ratkaisuja ja tietoturvastrategioita, jotka tarjoavat enemmän kattavaa suojelua koko terveydenhuollon verkostolle.

Vaikka terveydenhuollon organisaatioiden turvallisuusstrategia on tärkeä asia, tuo Rowen (2017) myös esille terveydenhuollon ja sen asiakkaiden välisen kommunikaation tärkeyden. Monet terveydenhuollon organisaatiot ovat ajautuneet mediassa negatiiviseen valoon useiden tietovuotojen takia. Tämä on puolestaan vaikuttanut negatiivisella tavalla potilaiden haluun jakaa omia henkilökohtaisia tietojaan kohdeorganisaation kanssa. 64 prosenttia potilaista kertoo yksityisyysongelmien olevan syy siihen, miksi ei halua jakaa tietojaan ver-

kossa ja 21 prosenttia myöntää salaavansa informaatiota hoitavalta lääkäriltä dataturvallisuus syistä. Tämä käyttäytyminen on suoraan ristiriidassa yhteistoiminnan tavoitteiden kanssa, joita sähköisillä potilasasiakirjoilla on pyritty saavuttamaan. Terveydenhuollon organisaatioiden on oltava proaktiivisia ja avoimia tavoista, joilla potilaiden henkilökohtaisia tietoja pidetään turvassa ja keskittyä rakentamaan vahvempaa luottamusta potilaidensa kanssa.

4.4 Digitaalinen terveydenhuolto

Liikenne ja viestintäministeriön (2018) mukaan digitalisaation aiheuttama kehitys on johtanut datan eksponentiaaliseen kasvuun, joka on puolestaan muodostanut tarpeen nopeammille yhteyksille. Nopeammat yhteydet ovat tarjonneet monille aloille lisätyn todellisuuden sovelluksia, kuten myös terveyspalveluissa esimerkiksi koulutuskäytössä. Digitaalinen terveydenhuollon avulla pyritään vähentämään hoitokustannuksia ja mahdollistaa hoitopalvelujen saatavuuden kaikkialle. Näihin tavoitteisiin voidaan päästä terveydenhoidon virtualisoinnin ja tietoliikenneyhteyksiä hyödyntävän etähoitamisen avulla. Tämä osoittaa sen, että terveydenhuolto on laajasti digitalisoitunut. Etälääketiede ja robotiikka on ollut laajamittaisesti käytössä jo vuosia. Nopeammat yhteydet voivat tarjota terveydenhuollolle paremmat puitteet myös turvallisuuden suhteen.

5G edustaa seuraavan sukupolven mobiiliteknologiaa ja on muuttamassa langattomien teknologioiden roolin. Nopeammat langattomat yhteydet, pienempi tiedonsiirron viive ja parempi turvallisuus on syitä, joiden takia terveydenhuolto tulee olemaan yksi keskeisimpiä 5G-teknologiaa hyödyntäviä sektoreita. (Wirén ym., 2018, s. 21.) Latifin (2017) mukaan 5G tarjoaa terveydenhuollon sektorille paljon mahdollisuuksia, mutta myös uhkia. Yksi nouseva uhka on IoT-laitteiden alttius haavoittuvuuksille. Tämän aiheuttaa niiden vähäinen laskennallinen tehokkuus, jonka takia ne eivät pysty käsittelemään monimutkaisia salausalgoritmeja. Tästä syystä siirrettävät tiedot on lähetettävä ilman mitään salausta. Myös pilvipohjaiset IoT-alustat, joita käytetään terveydenhuollon ulkoistetussa tietojen tallennuksessa, sekä ulkoisessa laskennassa luovat joukon yksityisyyttä koskevia turvallisuuskysymyksiä. 5G-verkot tulevat kohtaamaan kyberturvallisuusriskejä ja käyttäjien yksityiseen liittyviä uhkia, mutta pyrkii vastaamaan niihin vankoilla turvallisuustoimilla, joiden tarkoituksena on ratkaista eettisyyteen ja yksityisyyteen liittyvät huolenaiheet. Aikaisempiin mobiiliverkon sukupolviin nähden 5G-verkkojen on tarkoitus tarjota parempi turvallisuus ja tietosuojan taso. (Latif ym., 2017. s. 19.)

Terveydenhuollon laitosten verkon turvaaminen ja kyberturvallisuusuhkille altistumisen minimointi voidaan tehdä useiden mekanismien avulla. Esimerkiksi virtuaalisen paikallisverkon (VLAN) käyttö voi rajoittaa ulkopuolisten toimijoiden pääsyä laitteisiin. Sen toimintojen avulla voidaan rajoittaa tiedonsiirtoa pääverkon kanssa tiettyihin portteihin ja tiettyjen järjestelmien välillä. Tehokas ja päivitetty haittaohjelmien torjuntajärjestelmä voi havaita ja asettaa karanteeniin verkossa olevat uhat. Verkon suojaaminen verkon sisällä olevilta

käyttäjiltä on myös tärkeää. Se alkaa siitä, että käytössä on tiukka ja tehokas todennusprosessi, ja käyttäjille tulisi antaa vain vähimmäiskäyttöoikeus, joka tarvitaan heidän tehtäviensä suorittamiseen. (Coronado & Wong, 2014.)

4.5 Lääkinnällisten laitteiden turvallisuus

Lääkinnälliset laitteet ovat kiinteä osa lääketiedettä, joten niiden turvallisuuden tulee olla olennainen osa terveydenhuollon kyberturvallisuutta. Lääkinnällisiin laitteisiin liittyvät kyberturvallisuuden haavoittuvuudet ovat luonteeltaan samankaltaisia kuin mikä tahansa muu verkkoon liitetty järjestelmä. Lääkinnälliset laitteet eroavat muista järjestelmistä kuitenkin siten, että niiden haavoittuvuudet voivat aiheuttaa mahdollisia haittavaikutuksia potilasturvallisuudelle.

Lääketiede on siirtynyt hyödyntämään verkkoa vahvasti ja nykyisen lääkinnällisiin laitteisiin liittyvät ongelmat pakottavat käsittelemään lääkinnällisiä laitteita merkittävämpänä osana organisaatioiden turvallisuusstrategiaa. Lääketieteellisten laitteiden kehittyminen ja laajeneminen tulee varmasti aiheuttamaan haasteita kyberturvallisuuden kehittämisessä. Riski potilaiden arkaluonteisten tietojen paljastumiseen ja siihen liittyviä potilaiden yksityisyyden ongelmia ilmenee tällä hetkellä. (Williams & Woodward, 2015, s. 314.) Siksi on tärkeää upottaa kyberturvallisuussuojaus myös lääketieteellisten laitteiden suunnittelu- ja kehitysvaiheisiin, jotta laitteet saadaan pidettyä turvallisina ja mahdollisia haavoittuvuuksia voidaan vähentää. Standartit edesauttavat lääkinnällisten laitteiden kyberturvallisuustasoa ja samalla lakisääteinen valvonta kasvattaa myös laitteiden valmistajien vastuuta. Lääkinnällisten laitteiden teollisen puolen edustajat on saatava kiinnostumaan ja edistämään tietoisuutta kyberturvallisuuden ja yksityisyyden ongelmista, joita lääkinnällisten laitteiden käyttöön liittyy.

Lääkinnällisten laitteiden kyberturvallisuus on erittäin tärkeä aihe terveydenhuoltoalalla. Kun laitteet tarjoavat yhä enemmän liitettävyyttä ja integrointimahdollisuuksia, myös laitteisiin liittyvät kyberturvallisuusriskit kasvavat. Kyberturvallisuusriskien hallinta on valtava vastuu, ja jokaisen terveydenhuoltoyhteisön tulee jatkossakin pitää se mielessä. Yhteistyö on avainasemassa, jotta potilaiden hoidon optimaalisen toimitus voidaan varmistaa. (Coronado & Wong, 2014.)

5 YHTEENVETO

Tähän mennessä kyberhyökkäysten pääasiallinen tavoite terveyden huollon sektorilla on ollut rahallinen hyötyminen, eikä datan eheys ole vaarantunut esimerkiksi verikokeiden tai muiden testitulosten sormeilun muodossa. Vaikka näin ei ole vielä tapahtunut, tulee datan eheyden säilyttäminen olemaan ongelma tulevaisuudessa, jos riskeihin ei reagoida ajoissa. Lehdon (2017) mukaan kyberrikolliset kehittävät jatkuvasti uusia keinoja hyökätä organisaatioihin, sillä mustilla markkinoilla datasta ja informaatiosta maksetaan hyvin. Uudet terveydenhuollon teknologiat ja implementaatiot tuovat toki uusia riskejä ja kyberuhkia, mutta terveydenhuollon organisaatiot eivät voi kääntyä verkkopalveluiden, mobiiliuden, Big Datan tai pilvipalveluiden tuomista hyödyistä. Kyberrikollisia vastaan toimiminen vaatii uudenlaisia keinoja tulevaisuudessa ja IT:n, kyberturvallisuuden ja liiketoiminnan tulee toimia yhdessä päätöksiä tehdessä. Kyberrikollisuuden torjumiseen tarvitaan avoimuutta ja kommunikointia yritysten, sekä organisaatioiden välillä. Terveydenhuollon ympäristössä potilasturvallisuus tulee aina mukaan ennen kyberturvallisuuden vaatimuksia. Haasteena on ollut kaventaa näiden kahden tavoitteen välistä kuilua pyrkien vähentämään riskejä, tekemällä kompromisseja ja varmistaa potilasturvallisuus ja samalla reagoida kehittyvään kyberuhkien ympäristöön.

Tämän tutkielman aiheena oli kyberturvallisuuden uhat terveydenhuollossa, ja sen tavoitteena oli tuoda esille yleisimpiä ongelmakohtia, jotka liittyvät potilasturvallisuuden kysymyksiin. Tutkielmassa haluttiin myös tuoda esille kyberturvallisuuteen liittyvää sanastoa ja selkeyttää siihen liittyviä ristiriitaisia käsityksiä. Tutkielmassa esitettiin kaksi tutkimuskysymystä, jotka olivat: ” Mitkä ovat tyypillisimmät terveydenhuoltoon kohdistuvat kyberuhat?” ja ” Miten potilastietojen turvallisuus voidaan varmistaa tulevaisuudessa?”. Tutkimustapana toimi kirjallisuuskatsaus. Kirjallisuuskatsauksessa käytettyjä lähteitä on haettu Google Scholarin, Jykdokin ja IEEE Xplore Digital Libaryn tietokannoista. Tärkeimpiä hakusanoja ovat olleet: ”cybersecurity”, ”cyberhreats” ja ”healthcare”. Kirjallisuuskatsauksessa suosittiin kirjallisuutta, joka oli JUFO-luokitukseltaan vähintään perustasoa. JUFO-luokituksen alittaneisiin lähteisiin huomioitiin erityisen tarkkaa lähdekritiikkiä ja väitteiden paikkaansa pitävyyttä

tarvittaessa varmistettiin muiden lähteiden avulla. Tutkimusaineistoa oli riittävästi kattamaan vastauksia tutkimuskysymyksiin, vaikka terveydenhuoltoon liittyvä kyberturvallisuuden tutkimus on suhteellisen uutta. Kirjallisuuskatsauksessa käytetty kirjallisuus on pääosin viimeisen kymmenen vuoden ajalta, josta valta osa on peräisin Yhdysvalloista. Lähdekirjallisuuden tietojen hyödyntäminen suoraan käytännössä vaatisi tarkempaa lisätutkimusta paikalliselta tasolta. Kuitenkin tutkielmassa esiteltyjä ohjenuoria voidaan soveltaa kyberturvallisuuteen liittyvien haavoittuvuuksien tunnistamisessa ja ratkaisemisessa.

Tutkielma koostuu kokonaisuudessaan viidestä kappaleesta. Ensimmäinen kappale on johdanto. Johdannossa on esitetty lyhyesti tutkimuksen taustaa, tutkimusmenetelmät, motivaatio tutkimukselle ja sen tavoitteen. Samalla esittelin tutkimuskysymykset. Toisessa kappaleessa esitellään kyberturvallisuuden määritelmiä ja aiheeseen liittyvää perussanastoa, jotta kyberturvallisuuden yhteys terveydenhuoltoon olisi helpompi ymmärtää. Toinen kappale vastaa ensimmäiseen tutkimuskysymykseen, jossa esitellään yleisimpiä ja tyypillisimpiä kyberuhkia. Samalla tuotiin esille kyseisten uhkien luonnetta, sekä hyökkääjien motiiveja. Kolmannessa kappaleessa keskitytään kyberturvallisuuden haasteisiin ja haavoittuvuuksien muodostumiseen. Tässä kappaleessa painotettiin digitalisaation vaikutusta terveydenhuollon toimintaympäristöön. Uusien teknologioiden implementoiminen toi mukanaan uusia haasteita terveydenhuollon piirin, joihin ei osattu valmistautua oikeiden toimenpiteiden, standartien tai resurssien muodossa. Neljäs kappale vastaa toiseen tutkimuskysymykseen, jossa pyritään löytämään ratkaisua ajankohtaisiin potilasturvallisuutta ympäröiviin kysymyksiin. Tutkimuksen pohjalta voidaan kuitenkin todeta, ettei yhtä ratkaisutapaa ongelmiin ole vaan ratkaisuun tarvitaan yhteistyötä eri alojen viranomaisten kanssa, jotta terveydenhuoltoon pystytään määrittämään selkeät vastuuroolit ja standartit, jotka ovat tarkoitettu juuri terveydenhuollon ympäristön vaatimaan tilanteeseen. Myös budjetointiin, tietoisuuteen ja koulutukseen liittyviä toimintamalleja voidaan kehittää potilasturvallisuuden parantamiseksi. Viimeinen kappale on yhteenvetokappale, jossa kootaan yhteen tutkimuksen kulku, rakenne ja tutkimustulokset, joiden pohjalta arvioidaan tutkimuksen onnistumista, antia, sekä jatkotutkimusaiheita.

Tutkielman aiheen jatkotutkimus voisi liittyä johtamisstrategioiden kehittämiseen, sekä asianmukaisten ja terveydenhuoltoon räätälöityjen standartien pohtimiseen. Myös lääkinnällisten laitteiden valmistajien prosessien kuvaaminen voisi tuoda valoa siitä, miten lääkinnällisten laitteiden tuotantoa valvotaan ja seurataan. Myös paikallista tutkimustyötä olisi hyvä harjoittaa, koska toimintaympäristöt vaihtelevat myös terveydenhuollon organisaatioiden välillä. Tutkimuksen luonteen olisi hyvä olla mahdollisimman käytännön läheistä, jotta kyberturvallisuuden tilaa voidaan parantaa matalammalla kynnyksellä. Myös mobiililaitteiden ja terveyssovelluksiin liittyvän tutkimuksen avulla voitaisiin tunnistaa mahdollisia tulevaisuuden haavoittuvuuksia.

LÄHTEET

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the U.S. healthcare industry. Business Horizons, 62(4), 539–548. https://doi.org/10.1016/j.bushor.2019.03.010

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 146. https://doi.org/10.1186/s12911-020-01161-7

AT&T. (2015). Decoding the Adversary. AT&T Cybersecurity Insights, Volume 1.

Conaty-Buck, S. (2017). Cybersecurity and healthcare records. American Nurse Today, 12(9), 62-64.

Coronado, A. J., & Wong, T. L. (2014). Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. Biomedical Instrumentation & Technology, 48(s1), 26–30. https://doi.org/10.2345/0899-8205-48.s1.26

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

ENISA. (2011.) The National Cyber Security Strategy (NCSS).

FDA, U. (2014). Content of premarket submissions for management of cybersecurity in medical devices: Guidance for industry and food and drug administration staff.

Health, C. for D. and R. (2019). How to Determine if Your Product is a Medical Device. FDA. https://www.fda.gov/medical-devices/classify-your-medical-device/how-determine-if-your-product-medical-device

IMDRF Software as a Medical Device (SaMD) Working Group. (2014). "Software as a Medical Device": Possible Framework for Risk Categorization and Corresponding Considerations. International Medical Device Regulators Forum.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1–10. https://doi.org/10.3233/THC-161263

Latif, S., Qadir, J., Farooq, S., & Imran, M. A. (2017). How 5G Wireless (and Concomitant Technologies) Will Revolutionize Healthcare? Future Internet, 9(4), 93. https://doi.org/10.3390/fi9040093

Lehto, M. (2021). Digitaalisen kybermaailman ilmiöitä ja määrittelyä, 139.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi, 79.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? BMJ, 358, j3179. https://doi.org/10.1136/bmj.j3179

Millard, W. B. (2017). Where Bits and Bytes Meet Flesh and Blood: Hospital Responses to Malware Attacks. Annals of Emergency Medicine, 70(3), A17–A21. https://doi.org/10.1016/j.annemergmed.2017.07.008

Nweke, L. O. (2017). Using the cia and aaa models to explain cybersecurity activities. PM World Journal, 6, 1-2.

Razaque, A., Amsaad, F., Jaro Khan, M., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access, 7, 168774–168797. https://doi.org/10.1109/ACCESS.2019.2950849

Reagin, M. J., & Gentry, M. V. (2018). Enterprise cybersecurity: Building a successful defense program. Frontiers of health services management, 35(1), 13-22.

Rowe, K. (2016). How Has Ransomware Shifted the Landscape of Healthcare Data Security? 2016, 1.

Simi, J. (2017). Tiedon luokittelu osana organisaation kokonaisarkkitehtuurin riskienhallintaprosessia.

Turvallisuuskomitea. (2018), Kyberturvallisuuden sanasto. Noudettu 10. lokakuuta 2021, osoitteesta https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Uma, M., & Padmavathi, G. (2013). A Survey on Various Cyber Attacks and Their Classification. 7.

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? Information & Computer Security, 26(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

When Hackers Target Hospitals. (2016). Noudettu 25. marraskuuta 2021, osoitteesta https://www.reliasmedia.com/articles/137468-hackers-target-hospitals-with-ransomware

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices (Auckland, N.Z.), 8, 305–316. https://doi.org/10.2147/MDER.S50048