Tampereen yliopisto

Jutta Lukkala

KYBERTURVALLISUUDEN YLLÄPITÄMINEN TERVEYDENHUOLLOSSA

Lääketieteen ja terveysteknologian tiedekunta
Kandidaatintyö
Toukokuu 2022

TIIVISTELMÄ

Jutta Lukkala: Kyberturvallisuuden ylläpitäminen terveydenhuollossa
Kandidaatintyö
Tampereen yliopisto
Bioteknologia ja biolääketieteen tekniikka
Toukokuu 2022

Kyberturvallisuus on noussut nyky-yhteiskunnassa niin valtiollisella tasolla kuin yritysmaailmassakin yhä enemmän keskustelua herättäväksi aiheeksi. Kybermaailma sekä siihen kuuluva Internet ovat osa jokapäiväistä elämää ja lähes kaikki asiat voidaan hoitaa sähköisesti verkon välityksellä. Digitalisaation kehitys jatkuu edelleen ja sen vaikutus näkyy vahvasti myös terveydenhuollossa. IoT ja älykkäät lääkinnälliset laitteet yhdessä monien tietojärjestelmien kanssa luovat yhä moninaisemman, kyberhyökkäyksille alttiin kokonaisuuden. Terveydenhuollon toimivuus on välttämätön osa yhteiskunnan turvallisuutta ja sen takia terveydenhuollon kyberturvallisuudesta huolehtiminen on tärkeää.

Terveydenhuollon kyberturvallisuus on laaja kokonaisuus, johon liittyy strategisen tason päätösten lisäksi henkilöstön kyberosaamisen varmistaminen sekä käytännön tekninen toteutus. Tässä kandidaatintyössä on käsitelty terveydenhuollon kyberturvallisuutta ja sen ylläpitämistä Suomessa erityisesti teknisellä tasolla.

Aluksi on määritelty, mitä kyberturvallisuus tarkoittaa ja mitä se pitää sisällään. Sen jälkeen on perehdytty syvemmin terveydenhuollon kyberturvallisuuteen sekä sen sisältämiin haavoittuvuuksiin. Keskeisimmät terveydenhuollon haavoittuvuudet liittyvät verkkoon kytkettyihin lääkinnällisiin sekä niiden muodostamiin etäyhteyksiin.

Haavoittuvuuksista on siirrytty kyberturvallisuuden uhkiin ja esitetty muutamia terveydenhuoltoon kohdistuneita kyberhyökkäyksiä Suomessa. Tämän jälkeen on vielä lyhyesti pohdittu terveydenhuoltoon kohdistuvissa uhissa tapahtunutta muutosta viime vuosina.

Lopuksi on perehdytty teknisen tason ratkaisuihin, joilla kyberturvallisuutta ylläpidetään. Tietoa juuri suomalaisen terveydenhuollon kyberturvallisuuden teknisistä menetelmistä löytyi melko vähän. Yleisesti eri organisaatioiden kyberturvallisuuden ylläpitämisen keinoista löytyi kuitenkin enemmän tietoa. Tästä voidaan päätellä, että terveydenhuollon kyberturvallisuutta ylläpidetään käyttäen samoja ratkaisuja kuin muissakin organisaatioissa. Päätelmää vahvisti myös haastattelu terveydenhuollon parissa työskennelleen kyberturvallisuusammattilaisen kanssa. Keskeisimmiksi teknisen tason ratkaisuiksi kyberuhilta suojautumiseen nousivat verkon segmentointi ja erilaiset palomuuriratkaisut sekä verkon valvonta ja salaus.

Yhteenvetona voidaan todeta, että terveydenhuollon kyberturvallisuuden ylläpitämisen merkitys kasvaa jatkuvasti. Samalla kun älykkäät laitteet ja järjestelmät terveydenhuollossa lisääntyvät, myös terveydenhuollon kyberarkkitehtuuriin kohdistuu uusia uhkia ja kyberhyökkäysten riski kasvaa. Potilaiden turvallinen hoito ja yksityisyys on tästä huolimatta pystyttävä varmistamaan myös tulevaisuudessa.

Avainsanat: kyberturvallisuus, terveydenhuolto, tekniset ratkaisut, kyberuhat, haavoittuvuudet

LYHENTEET

PC	Personal computer. Kompakti henkilökohtaiseen käyttöön tarkoitettu mikroprosessoria käyttävä tietokone.
CIA	Confidentiality, Integrity, Availability. Luottamuksellisuus, eheys ja saatavuus ovat tietoturvan ja samalla kyberturvallisuuden peruspilarit.
AA	Oikeutettu pääsy (engl. Appropriate Access)
AAA-malli	Mallin avulla saavutetaan kyberturvallisuuden tavoitteet. Sisältää todentamisen, valtuutuksen ja kirjanpidon (engl. authentication, authorization and accounting).
ATTAT-kaava	Kybertoimintaympäristön muuttuvat lainalaisuudet aika, tila, tunnistamattomuus, asymmetrisyys ja tehokkuus.
CPS	Kyberfyysinen järjestelmä (engl. Cyber-Physical system)
IoT	Esineiden Internet (engl. Internet of Things)
IoMT	Lääketieteellisten esineiden Internet (engl. Internet of Medical Things)
IMD	Implantoitavat lääketieteelliset laitteet (engl. Implantable medical device)
SQL	Strukturoitu kyselykieli (engl. structured query language)
TYKS	Turun Yliopistollinen Keskussairaala
VLAN	Virtuaalilähiverkko (engl. Virtual Local Area Network)
MGN	Lääketieteellisen tason tietoverkko (engl. Medical Grade Network)
VPN	Virtuaalinen yksityisverkko (engl. Virtual Private Network)
SOC	Security Operations Center. Tietoturvavalvomo.
SSH	Suomalainen tietoturvayhtiö
AES	Advanced Encryption Standard -salausmenetelmä

SISÄLLYSLUETTELO

1. JOHDANTO

Digitalisaation jatkuvan kehittymisen myötä kyberturvallisuus on yhä tärkeämmässä roolissa nyky-yhteiskunnassa niin yksilön kuin organisaatioidenkin kannalta. Kaikki ihmiset ovat yhteydessä internetiin. Terveydenhuollon hallitsema data, niin potilas-, laite- ja järjestelmätiedot kuin päivityksetkin, ovat verkossa. Myös terveydenhuollon lääkinnälliset laitteet, kuten kuvantamis- ja muut diagnostiikkalaitteet, ovat yhteydessä verkkoon. Turvallisuus- ja kemikaaliviraston, Tukesin mukaan terveydenhuollossa käytettäviä laitteita eli lääkinnällisiä laitteita ovat erilaiset instrumentit ja laitteistot tai niiden kaltaiset välineet, jotka ovat valmistajan mukaan määritelty käytettäväksi sairauden diagnosoinnissa, ehkäisyssä, tarkkailussa, hoidossa tai lievityksessä. Näihin kaikkiin liittyy kyberturvallisuuden riskejä. On tunnistettava haavoittuvuudet ja etenkin suunniteltava, millaisilla strategisilla ja teknisillä menetelmillä terveydenhuollon kriittistä dataa suojellaan. Lisäksi on tärkeää luoda toimintamalli, jota noudatetaan, jos joudutaan kyberhyökkäyksen kohteeksi. Väärät tahot voivat päästä organisaation sisäiseen verkkoon ja sitä kautta käsiksi latteisiin sekä niiden sisältämään dataan esimerkiksi, kun laitteisiin muodostetaan etäyhteyksiä laitteenvalmistajan toimesta.

Tässä työssä kartoitetaan kirjallisuuskatsauksen muodossa terveydenhuollon kyberturvallisuuden kokonaisuutta painottaen erityisesti sen ylläpitämistä teknisin ratkaisuin Suomessa. Tutkielman tavoitteena on selvittää, mitkä ovat keskeisimmät teknisen tason ratkaisut, joilla kyberturvallisuutta pyritään terveydenhuollossa ylläpitämään. Jotta saadaan käsitys siitä, mitä varten näitä ratkaisuja käytetään, perehdytään ensin terveydenhuollon haavoittuvuuksiin ja uhkiin. Tutkielmassa on pyritty käsittelemään esitettyjä aiheita suomalaisen terveydenhuollon näkökulmasta saatavilla olevan aineiston pohjalta. Suomalaisen terveydenhuollon kyberturvallisuutta koskevia artikkeleita löytyi verrattain vähän, joten tutkielmassa on käytetty myös muualla maailmalla tehtyjä tutkimuksia ja artikkeleita aiheeseen liittyen. Tutkielman motivaationa on kyberturvallisuus -aiheen ajankohtaisuus sekä terveydenhuollon tietojärjestelmäarkkitehtuurin muutos uusien älykkäiden lääkinnällisten laitteiden ja järjestelmien lisääntyessä. Tähän liittyen olennaisimpana taustalla olleena kysymyksenä on se, miten jatkuvasti muuttuvan kokonaisuuden kyberturvallisuus ja sitä kautta sekä potilaiden turvallisuus että yksityisyys voidaan varmistaa.

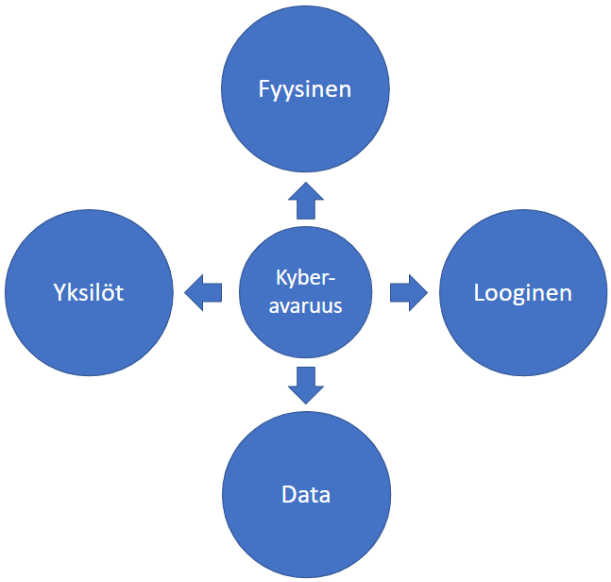
Työn toisessa luvussa tarkastellaan kyberturvallisuutta yleisesti sekä siihen liittyviä käsitteitä ja osa-alueita. Lisäksi käsitellään tarkemmin kyberturvallisuuden linkittymistä terveydenhuoltoon. Kolmas luku avaa terveydenhuollon haavoittuvuuksia sekä terveydenhuoltoon kohdistuvia kyberuhkia. Lisäksi kolmannessa luvussa esitellään muutamia Suomessa tapahtuneita kyberhyökkäyksiä ja niiden seurauksia sekä kyberuhissa tapahtunutta muutosta viime vuosina. Neljännessä luvussa perehdytään teknisiin ratkaisuihin, joiden avulla Suomessa pyritään takaamaan kyberturvallisuus terveydenhuollossa.

2. KYBERTURVALLISUUS

2.1 Kyberturvallisuuden määritelmä

Kyberturvallisuuden käsitteen ymmärtämiseksi on ensin määriteltävä käsitteet kybertoimintaympäristö eli niin kutsuttu kyberavaruus (engl. cyberspace) (Padallan 2019, s. 30) sekä kyberuhka, tietoturva ja tietoturvauhka. Kyber-etuliitteen sisältävä käsite on tavallisesti yhteydessä digitaalisen datan käsittelyyn. Kyberturvallisuus on jatkuvasti kehittyvä ja yhä enemmän sekä keskustelua että viestintää herättävä ala, minkä vuoksi on olennaista määritellä siihen keskeisesti liittyvät käsitteet. (Turvallisuuskomitea 2018) Terveydenhuollossa sähköisiin järjestelmiin siirtyminen on johtanut erilaisiin kyberturvallisuuden haavoittuvuuksiin. Kyberrikollisten näkökulmasta terveydenhuolto onkin houkutteleva kohde, sillä terveydenhuollon tietojärjestelmät sisältävät paljon arkaluontoisia ja henkilökohtaisia potilastietoja. (Kruse et al. 2017)

Kybertoimintaympäristö voidaan määritellä toimintaympäristönä, joka koostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä (Turvallisuuskomitea 2018). Se on interaktiivinen monista kerroksista koostuva ympäristö, joka sisältää sekä internetin että muut tietojärjestelmät. Sillä on kyky varastoida, muokata ja välittää tietoa. Kyberavaruus voidaan jakaa osiin seuraavan kuvan esittämällä tavalla.



Kuva 1: Kybertoimintaympäristön muodostavat komponentit. Perustuu lähteeseen (Padallan 2019, s. 32)

Padallanin (2019) mukaan kyberympäristö koostuu komponenteista, joita ovat fyysiset systeemit (engl. physical), loogiset rakennuspalikat (engl. logical building blocks), kyberavaruudessa liikkuva data sekä dataa hallitsevat ja välittävät yksilöt eli käyttäjät. Loogiset rakennuspalikat ovat esimerkiksi ohjelmistoja. Terveydenhuollossa palomuurit ovat tavallisimpia rakennuspalikoita, kun turvataan älykästä terveydenhuoltoympäristöä (Anwar et al. 2021). Jokaisella mainitulla kyberavaruuden komponentilla on kolme tärkeää ominaisuutta: verkosto, nopeus ja muisti.

Kyberavaruuden yhteydet kaikkialle maailmaan luovat verkoston. Ihmisten toiminnasta kertyy dataa, joka lisääntyy ja jonka kattavuus paranee yhä useampien ihmisten liittyessä internetiin. Tapahtumasarjaa kutsutaan positiiviseksi verkoston vaikutukseksi. Nopeudella viitataan nopeuteen, jolla kybertoimintaympäristö muuttuu. Puolijohteet sekä transistorien määrän kasvu tietokonesiruissa (engl. PC-chip, personal computer) on johtanut nopeuden kasvuun kybertoimintaympäristössä. Transistorien määrän kasvaessa myös PC-sirujen prosessointiteho kasvaa jatkuvasti, mikä puolestaan mahdollistaa yhä nopeampaa hakutulosten tuottamista. (Padallan 2019, s.35) Nopeudella on positiivinen vaikutus digitaaliseen maailmaan ja sen vahvistumiseen.

Verkon nopea toiminta vaatii varastointitilaa. Varastointi pitää sisällään niin laitteen kapasiteetin kuin myös sen suorituskyvyn. Nämä datavarastot kiinnostavat tavallisten käyttäjien lisäksi myös hakkereita. On huomattava, että kaikista edellä mainituista ominaisuuksista ja niiden kehittymisestä hyötyy niitä tarvitsevien osapuolten lisäksi myös väärinkäyttäjät. Ominaisuuksia ei ole mahdollista parantaa niin, etteivät uudet menetelmät olisi myös hakkereiden ulottuvilla. (Padallan 2019, s.36)

Kyberuhka on kybertoimintaympäristöön kohdistuva vahingollinen tapahtuma tai tapahtumaketju, joka voi mahdollisesti toteutua. Tapahtumaketjun toteutuminen aiheuttaa kybertoimintaympäristöstä riippuvan toiminnon vaarantumisen. (Turvallisuuskomitea 2018) Nykyisessä yhä verkottuneemmassa maailmassa kyberuhkien lähteet voivat olla odottamattomia (Choo, 2011).

Tietoturvalla voidaan tarkoittaa useampaa eri asiaa, kuten tavoitetilaa, erilaisia järjestelyjä tai akateemista ainetta. Tämän takia on tärkeää määritellä tietoturvan käsite. Määrittelyn jälkeen voidaan vastata kysymykseen siitä, mitä tietoturva on. (Lundgren & Möller 2019) Tietoturva kattaa järjestelyt, kuten kulunvalvonnan, tietojen salauksen ja varmuuskopioinnin sekä palomuurien käytön. Näiden toimien tarkoituksena on varmistaa, että tieto on saatavilla, eheää ja luottamuksellista. Tietoturvauhalla puolestaan tarkoitetaan

tietoturvaan kohdistuvaa vahingollista tapahtumaa tai tapahtumaketjua, joka mahdollisesti toteutuu ja toteutuessaan on vaaraksi tietoturvalle. (Turvallisuuskomitea 2018)

Aiemmin mainittujen käsitteiden ymmärtäminen auttaa muodostamaan peruskäsityksen siitä, mistä kyberturvallisuudessa on kyse. Toisin kuin yleisesti voidaan kuulla puhuttavan, kyberturvallisuudella ei siis tarkoiteta vain omiin digitaalisiin laitteisiin kuten puhelimeen ja tietokoneeseen tai internetin selaamiseen liittyvää tietoturvaa (Padallan 2019, s.31). Kyberturvallisuus on kyberuhkien tunnistamista, niiden vaikutusten ehkäisyä ja varautumista digitaaliseen omaisuuteen kohdistuvia kyberuhkia vastaan erilaisin toimenpitein. Näiden toimenpiteiden avulla voidaan sopeutua vallitseviin kyberuhkiin sekä niiden vaikutuksiin. Kyberturvallisuuden erona tietoturvaan on se, että kyberturvallisuudella pyritään estämään luvaton sähköinen pääsy tietoihin (Turvallisuuskomitea 2018). Tietoturva käsittää missä muodossa tahansa olevan tiedon turvaamisen.

2.2 Kyberturvallisuuden periaatteet

Kyberturvallisuuden periaatteet pohjautuvat tietoturvan peruspilareihin, jotka kyberturvallisuus pyrkii varmistamaan. Ne ovat CIA eli luottamuksellisuus, eheys ja saatavuus (engl. confidentiality, integrity and availibility) sekä lisäksi kiistämättömyys (engl. non-repudiation). (Padallan 2019, s. 37–38) CIA-mallin lisäksi käytetään AAA-mallia, jonka avulla voidaan saavuttaa kyberturvallisuuden tavoitteet. AAA-malli pitää sisällään todentamisen, valtuutuksen ja kirjanpidon (engl. authentication, authorization and accounting). (Obiora Nweke 2017)

CIA-mallia on hyödynnetty erilaisin muunnelmin esimerkiksi ISO-standardeissa, kansallisissa standardeissa, käsikirjoissa ja artikkeleissa (Lundgren & Möller 2019). Ei ole varmaa tietoa siitä, milloin CIA-malli vakiintui, mutta sen tärkeys perustuu siihen, että sen avulla voidaan muodostaa selkeä ajatus kyberturvallisuuden vaatimuksista (IntelliPaat 2021).

2.2.1 Periaatteiden määrittely

Luottamuksellisuudella tarkoitetaan, että tietoja pääsee tarkastelemaan vain sellaiset käyttäjät, prosessit ja laitteet, joilla on valtuudet kyseisten tietojen käyttöön (Klemm & Johnson 2010). Tällaisia tietoja ovat esimerkiksi tiedostot, käyttäjänimet ja salasanat. Terveydenhuollossa luottamuksellisuus varmistetaan erilaisilla varmenteilla ja toimikorteilla. Digi- ja väestötietoviraston mukaan tietosuojan ja tietoturvan toteutuminen sosiaali- ja terveydenhuollon valtakunnallisissa tietojärjestelmäpalveluissa edellyttää henki-

lön vahvan sähköisen tunnistautumisen. Varmenteiden avulla turvataan luotettava sähköinen tunnistautuminen eri järjestelmiin ja todennetaan kortinhaltijan henkilöllisyys samoin kuin myös varmenteeseen liittyvien tietojen oikeellisuus, eheys ja alkuperäisyys. Tämän lisäksi sähköiset allekirjoitukset esimerkiksi potilasasiakirjoihin tai lääkemääräyksiin toteutetaan varmenteiden avulla. (Digi- ja väestötietovirasto) Potilaiden osalta tietoturva esimerkiksi Kanta-palveluissa eli kansallisessa potilastiedon arkistossa on turvattu käyttämällä kirjautumiseen pankkitunnuksia, henkilökorttia tai mobiilivarmennetta. Myös Kanta-palveluiden yhteys on suojattu, joten ulkopuolisilla tahoilla ei ole mahdollisuutta nähdä luottamuksellisia tietoja. (Kanta 2021)

Eheys viittaa siihen, että siirretty, varastoitu tai käsitelty tieto ei sisällä tahallisesti tai tahattomasti tehtyjä muutoksia, jolloin tieto olisi kadonnut tai tuhoutunut, vaan se on täysin alkuperäistä (Klemm & Johnson 2010; Obiora Nweke 2017). Luvussa kolme käsitellään terveydenhuollon yleisimpiä ja tyypillisimpiä kyberuhkia, joista yksi on datan korruptointi. Eheyden takaaminen tässä yhteydessä tarkoittaa siis sitä, ettei esimerkiksi potilastietoja ole väärennetty, mikä saattaisi asettaa potilaan vaaraan. (Martin et al. 2017)

Tiedon saatavuus tarkoittaa, että tiedon käyttöön valtuutetut käyttäjät pääsevät helposti käsiksi tietoon siten, että mahdollisen kyberturvallisuushäiriön ilmetessä järjestelmän kuormitus ja toleranssi ovat jatkuvasti tasapainossa. (Klemm & Johnson 2010; Obiora Nweke 2017) Kiistämättömyys tulee esiin tilanteissa, joissa on sekä tiedon lähettäjä että tiedon vastaanottaja. Kiistämättömyys tarkoittaa että, on olemassa todiste siitä, että lähettäjä on lähettänyt tietoja ja vastaanottaja puolestaan ottanut tietoja vastaan. Kiistämättömyyden avulla voidaan varmistaa, ettei kumpikaan osapuoli voi jälkikäteen kieltää käsitelleensä kyseessä olevaa tietoa. (Klemm & Johnson 2010; Padallan 2019, s.40)

Lähteestä riippuen käytetään joko määritelmää AA (Appropriate Access) eli oikeutettu pääsy tai aiemmin mainittua AAA – mallia (Obiora Nweke 2017; Lundgren & Möller 2019). AA:n määritelmä on uusi ja se on syntynyt lisäyksenä täydentämään ongelmaksi muodostuneita aukkoja CIA:n määrittelyssä. Yleisesti AA tarkoittaa sitä, että käyttäjä pääsee tietoihin käsiksi vain siinä tapauksessa, että on varmistettu käyttäjän olevan se, kenen nimissä hän pyrkii niitä päästä tarkastelemaan. (Lundgren & Möller 2019) AAA – mallista Appropriate Access kattaa todentamisen ja valtuutuksen. Todentaminen tarkoittaa käyttäjän henkilöllisyyden todistamista siksi, joka hän väittää olevansa ja valtuutus tarkoittaa, että käyttäjälle myönnetään pääsy tietoihin, jotka ovat todennetulle henkilöllisyydelle myönnetty. Kolmas A eli kirjanpito (Accounting) on mahdollisen kyberhyökkäyksen sattuessa tärkeä todiste toimista, jotka ovat saattaneet olla hyökkäyksen aiheutta-

mien vahinkojen takana. Kirjanpito tarkoittaa siis sitä, että käyttäjän toiminta järjestelmässä tallennetaan ja näihin tietoihin on mahdollista palata tarvittaessa. (Obiora Nweke 2017)

2.2.2 Kybertoimintaympäristön lainalaisuudet

Kybertoimintaympäristö on jatkuvasti muuttuva dynaaminen kokonaisuus. Jotta olisi mahdollista ymmärtää kybertoimintaympäristössä vallitsevia uhkia ja varautua niihin, on ymmärrettävä kybertoimintaympäristön muuttuvia lainalaisuuksia. Muuttuvat lainalaisuudet muodostavat ATTAT-kaavan. Kirjaimet tulevat sanoista aika, tila, tunnistamattomuus, asymmetrisyys ja tehokkuus. Aika kybermaailman lainalaisuutena tarkoittaa sitä, että toiminnot, joille on annettu käsky tapahtua, tapahtuvat välittömästi. Tämä tarkoittaa, ettei fyysiseen maailmaan sidottua viivettä ei kybermaailmassa tunneta. Odottelua ei siis ole ja aika menettää merkityksensä. (Limnéll 2014, s.63)

Myös välimatkat menettävät kybermaailmassa merkityksensä, kun kuka tahansa voi kommunikoida kenen kanssa tahansa, vaikka henkilö olisikin toisella puolella maapalloa. Tila siis ikään kuin häviää. Kybertoimintaympäristö on myös keinotekoinen tila, sillä sitä on mahdollista muokata halutunlaiseksi toisin kuin fyysistä maailmaa. Kybertoimintaympäristöä muokataankin jatkuvasti esimerkiksi turvallisuusvaatimusten mukaiseksi. Lisäksi kyberympäristöä muuttavat jatkuvasti erilaiset teknologiapäivityksen ja verkostojen muutokset, minkä seurauksena kybertoimintaympäristö, kybertila muuttuu ennakoimattomasti ilman ennakkovaroituksia. Kybertilassa tapahtumien ja toimien alkuperästä ei voida olla lähestulkoon ollenkaan varmoja ja näiden tietojen selvittäminen on likimain mahdotonta. Fyysistä tilaa on mahdollista jakaa siten, että tietty alue on jonkun ihmisen, yrityksen tai valtion omistuksessa, mutta tällaiset lait eivät päde kybertilassa. Kybertila kuuluu kaikille eikä siellä tunneta rajoja. (Limnéll 2014, s.65)

Tunnistamattomuus on myös yksi kybermaailman lainalaisuuksista. Sillä tarkoitetaan, että kybertoimintaympäristön käyttäjiä ja toimijoita voi olla mahdotonta tunnistaa eikä heidän identiteettinsä tai sijaintinsa välttämättä ole tunnistettavissa. Bittien maailmassa on mahdollista toimia tunnistamattomana tai jopa useammalla eri identiteetillä. (Limnéll 2014, s.67) Tähän liittyen onkin tarpeen miettiä, millainen tunnistamisen varmuuden taso halutaan, kun kyse on esimerkiksi yritysten tai valtion toimintoihin tunnistautuminen. Terveydenhuolto on esimerkki siitä, että henkilön identiteetin tunnistaminen on välttämätöntä, jotta tietoja voidaan käsitellä luottamuksellisesti.

Kybertoimintaympäristön asymmetrisyys kuvaa sitä, miten heikompi eli tässä pienempi joukko käyttää valtaa vahvempaa, suurempaa joukkoa vastaan. Esimerkiksi muutamat

toimijat kuten hakkerit tai alan ammattilaiset pystyvät käyttämään rajoittamattomia resursseja suurta joukkoa vastaan. Näiden toimien onnistumista ei käytännössä estä mikään, ja kyberhyökkäyksiä on mahdollista tehdä rajattomasti ilman resurssien kulumista. Juuri kybertoimintaympäristön haavoittuvuudet ovat asymmetrisyyden haasteena.

Viimeinen kyberympäristön ATTAT – kaavan lainalaisuus on tehokkuus. Kybermaailman tehokkuus tulee esiin esimerkiksi joukkoistamisen muodossa sekä siten, että lukuisa määrä asioita on mahdollista toteuttaa samanaikaisesti. Joukkoistamisella tarkoitetaan yksinkertaisesti sitä, että verkossa yhden tietyn rajatun tavoitteen saavuttamiseksi voidaan käyttää rajatonta joukkoa. Kybertoimintaympäristön tehokkuutta on myös se, että kenellä tahansa on mahdollisuus lisätä kybermaailman kyvykkyyttä. Tehokkuus on lainalaisuus, joka on vahvasti seurausta aikaisemmin mainittujen lainalaisuuksien yhteisvaikutuksesta. (Limnéll 2014, s.68–71)

Kaikki edellä mainitut kybermaailman lainalaisuudet aiheuttavat haasteita myös terveydenhuollon kyberturvallisuuden ylläpitämisessä.

2.3 Terveydenhuollon kyberturvallisuuden yleiset piirteet

Terveydenhuollon kyberturvallisuus on laaja kokonaisuus, joka koostuu useista eri osa-alueista. Julkisella terveydenhuollolla on toimintastrategia, joka sisältää muun muassa tietojenhallintastrategian sekä kyberstrategian. Näiden pohjalta muodostuu julkisen terveydenhuollon tietoturvapolitiikka eli se, miten organisaatiossa toteutetaan tietoturvaa. Tietoturvapolitiikka taas pitää sisällään henkilöstön koulutuksesta ja tietoisuudesta huolehtimisen eli sen, millainen on henkilöstön kypsyystaso tietoturvaa koskevissa asioissa. Tästä päästään edelleen kyberturvallisuuden tekniseen alueeseen, joka kattaa erilaiset kyberturvallisuuden kontrollit, niiden monitoroinnin ja seurannan. Tekninen alue pitää sisällään uhkien jaottelun ja mallinnuksen, joiden perusteella suunnitellaan, miten näiltä uhkilta voidaan suojautua teknisin menetelmin. (Tolonen 2022)

Jotta yhteiskunnan elintärkeät toiminnot voidaan ylläpitää, kriittisen infrastruktuurin eli perusrakenteiden, palvelujen ja niihin liittyvien prosessien on välttämätöntä toimia moitteettomasti (Vuorinen 2019). Yhteiskunnan turvallisuusstrategiaan sisältyy talouden, infrastruktuurin ja huoltovarmuuden varmistaminen, mikä kattaa myös terveydenhuollon tietojärjestelmien toimivuuden turvaamisen. Toimiva ja turvattu terveydenhuolto on koko yhteiskunnan toimivuuden kannalta välttämätön. Tämän takia sekä asiakas- ja potilastietojen että muiden terveydenhuollon hallussa olevien tietojen kyberturvallisuus täytyy

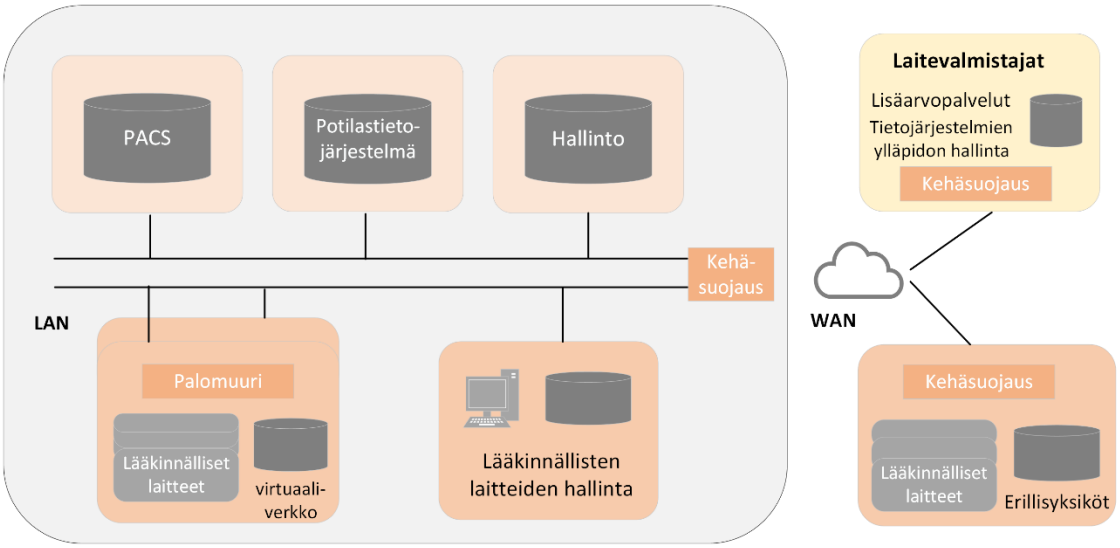
varmistaa. Tämä koskee myös digitaalisten diagnostiikkalaitteiden ja muiden tietoverkkoihin kytkettyjen laitteiden kyberturvallisuutta. (Yhteiskunnan turvallisuusstrategia 2017)

Aiemmin mainittiin, että tieto- ja kyberturvallisuuteen liittyen tärkeimmät asiat ovat tietojen eheyden, luottamuksellisuuden ja saatavuuden takaaminen. Terveydenhuollossa tämä korostuu entisestään, kun kyseessä ovat potilastiedot ja potilaiden turvallinen hoito. Sen lisäksi, että potilastietojen suojaaminen on tärkeää yksityisyyden suojan kannalta, pitää ottaa myös huomioon potilastietojen rikollisen käytön mahdollisuus ja sen ehkäiseminen (Lehto & Lehto 2017).

2.3.1 Kybertoimintaympäristönä terveydenhuolto

Paikalliset, alueelliset ja kansalliset järjestelmät muodostavat terveydenhuollon kansallisen tietojärjestelmäarkkitehtuurin. Operatiivisiksi päivittäin käytettäviksi järjestelmiksi luetaan paikalliset ja alueelliset järjestelmät. Tietojen varastointi ja jakelu ovat kansallisten järjestelmien vastuulla ja niitä koskevien tietoliikenneyhteyksien suojauksen ja valvonnan eteen on nähty paljon vaivaa. Tällaisia kansallisia järjestelmiä ovat esimerkiksi Kanta-palvelut sekä koodistopalvelu. (Vuorinen 2019)

Sairaala on yksi toimintaympäristö, jossa terveydenhuollon tietojärjestelmiä käytetään merkittävästi (Vuorinen 2019). Toimiva sairaalaympäristö vaatii useita tietojärjestelmiä ja niistä muodostuvia kokonaisuuksia. Sairaalan tietojärjestelmäkokonaisuus on näistä yksi ja se sisältää edelleen useampia alajärjestelmiä. Potilastietojärjestelmät ovat paikallisia ja terveydenhuollon tietojärjestelmistä keskeisimmässä osassa. Niiden ydinjärjestelmiin kuuluvat lähetteiden käsittely ja ajanvaraus sekä hoitotietojen kirjaaminen. Potilastietojärjestelmien avulla potilaaseen liittyviä tietoja kuten diagnooseja, hoitotoimenpiteitä, tutkimuksia ja lausuntoja kirjataan ylös koko palveluprosessin ajan. Myös erilaiset raportit ja tilastot sekä kustannus- ja laskutustiedot johdetaan potilastietojärjestelmien avulla. (Integrating the Healthcare Enterprise 2015) Seuraavassa kuvassa on esitetty sairaalan geneerinen tietojärjestelmien kokonaisuus.



Kuva 2: Sairaalan tietojärjestelmäkokonaisuus (Muokattu lähteestä Integrating the Healthcare Enterprise 2015, s. 21)

Operatiivisten ydinjärjestelmien lisäksi on olemassa yksikkökohtaisia erillisjärjestelmiä, jotka täydentävät ydinjärjestelmiä. Tutkimus- ja toimenpidetiedot potilaan hoidon ajalta kerätään erillisjärjestelmiin, joita ovat esimerkiksi laboratoriojärjestelmät, röntgenosastojen työnohjausjärjestelmät (engl. Radiology Information System, RIS) sekä digitaalisen kuvan arkistointi (engl. Picture Archiving Communications Systems, PACS). (Pöyhönen et al. 2019)

Erilaisten järjestelmien arkkitehtuurin lisäksi myös lääkinnällisille laitteille voidaan muodostaa yksinkertaistettu malli niihin kuuluvista komponenteista, jotka ovat erityisesti kyberturvallisuuden kannalta oleellisessa asemassa. Lääkinnällisten laitteiden keskeiset komponentit ovat laite itse (engl. Hardware), erillinen laitteen hallinta- ja valvontakomponentti sekä laitteen COTS käyttöjärjestelmä (engl. Commercial off-the-shelf Operating System), joka sisältää laitteen ohjelmiston (engl. software). Laitteen hallinta- ja valvonta pitää sisällään testauksen ja kalibroinnin, monitoroinnin ja lokit, turvamekanismien hallinnan sekä versioidenhallinnan. Lääkinnällinen laite on yhteydessä TCP/IP verkkoon. (Integrating the Healthcare Enterprise 2015, s.16) Verkkoyhteyden tyyppi, joka yhdistää sairaalaympäristön laitteet, riippuu muun muassa sen käyttötarkoituksesta. Esimerkiksi elektronisiin potilastietoihin voi olla verkkoyhteys langallisesti tai langattomasti. Kuva- tai tallennusvarastolle on oma yhteys, samoin kuin erilaisille etäyhteyksille (esim. potilastiedot/-tulokset), etäpalveluille, -ohjaukselle, -hallinnalle ja laitteiden väliselle viestinnälle. (Grimes 2016, s.11)

2.3.2 Teollisuus 4.0 terveydenhuollossa

Myös terveydenhuollossa on nähtävissä Teollisuus 4.0 eli neljäs teollinen vallankumous (engl. Industry 4.0). Se on olennainen osa, kun puhutaan terveydenhuollon kyberturvallisuudesta tänä päivänä, sillä Teollisuus 4.0. tuo mukanaan monia haasteita ja riskejä lukuisten hyötyjen rinnalle. Teollisuus 4.0: n myötä palvelu- ja tuotantomaailma muuttuu ja uudet tieto- ja viestintätekniikat ottavat jalansijaa. (Aceto et al. 2020) Tämä on näkyvissä myös muuttuvassa sähköisessä terveydenhuollossa, joka on etenemässä kohti Healthcare 4.0: aa eli neljättä teollista vallankumousta terveydenhuollossa. Teollisuus 4.0 perustuu käsitteeseen kyberfyysisestä järjestelmästä (engl. Cyber-Physical system, CPS). Kyberfyysisellä järjestelmällä tarkoitetaan tietojenkäsittelyn, viestinnän ja ohjauksen integroimista yhdeksi verkossa toimivaksi kokonaisuudeksi, joka kontrolloi fyysisiä laitteita. (Aceto et al. 2020; Lehto et al. 2019) CPS on riippuvainen kolmesta tekijästä: Esineiden Internet (engl. Internet of Things, IoT), pilvipalvelut (engl. Cloud computing) ja Big Data analytiikka (Aceto et al. 2020). Näistä keskeisimpinä kyberturvallisuuden kannalta ovat IoT: n ja pilvipalveluiden mukanaan tuomat haasteet.

Terveydenhuollon kyberturvallisuuteen liittyvät olennaisesti tietoverkot, joita voidaan hyödyntää erilaisten sairaalapalveluiden tarjoamiseen. Kasvavissa määrin sairaaloiden lääkinnälliset laitteet ovat yhteydessä internettiin tai sairaaloiden tietoverkkoon sekä muihin laitteisiin (Vuorinen 2019). Tästä käytetään nimitystä esineiden internet eli IoT (engl. Internet of Things) (Kumar Bhoi 2021). IoT:llä tarkoitetaan verkossa yhdessä toimivia laitteita kuten mobiililaitteita, antureita, näyttöpäätteitä (Aceto et al. 2020) ja terveydenhuollon tapauksessa myös lääkinnällisiä laitteita, jotka pystyvät lähettämään tai vastaanottamaan tietoa. Terveydenhuollossa käytetään myös termiä Lääketieteellisten Esineiden Internet (engl. Internet of Medical Things, IoMTs) (Rathore et al. 2018). IoMT-laitteita ovat esimerkiksi verkkoon kytketyt langattomat EKG-monitorit sekä magneettikuvantamislaitteet (Karhunen 2020, Candia 2021). Frost and Sullivan (2017) esitti, että vuonna 2017 jo liki 60 % terveydenhuolto-organisaatioista on ottanut käyttöön IoMTs:n. IoMTs:n avulla terveydenhuoltoa on mahdollista muuttaa enemmän proaktiiviseen eli ennakoivaan toimintaan reaktiivisen sijaan. Potilaan tilaa voidaan tarkastella säännöllisesti IoMT-monitorien avulla, jolloin potilaaseen otetaan yhteyttä tilan muuttuessa sen sijaan, että potilas ottaisi yhteyttä. (Rathore et al. 2018)

Esineiden Internetiin liittyy erityisiä tarpeita tietoturvaratkaisujen ja käytön aikaisen turvallisuuden kehittämiselle, sillä se lisää tietoturvariskejä. Terveydenhuollossa IoT:tä käytetään yhä enemmän (Sosiaali ja terveysministeriö 2019). Sen käyttö terveydenhuolto-ympäristössä on kuitenkin vasta alussa ja tällä hetkellä suojausprotokollat eivät vielä täytä vaatimuksia yksityisyysriskien ja turvallisuuden takaamiselle. Kokonaisvaltaisen

kyberturvallisuuden tarve on avain asemassa IoT:n kehittämisessä. (Aceto et al. 2020) Pilvipalvelut tarjoavat sekä erilaisia viestintäresursseja apuohjelmina että rajattoman määrän tallennustilaa, joka on IoT:n toiminnan kannalta melkein jopa vaadittua. Vaikka pilvipalvelut mahdollistavat erilaiset korkean tason toiminnot, tietoanalyysin sekä järjestelmät ja terveydenhuollon tarjoamisen etäpalveluna, siihen liittyy myös tietosuojahaasteita. (Aceto et al. 2020) Pilvipalvelut ovat alttiita potilastietojen väärinkäytölle, mikä heikentää potilaan yksityisyyden suojaa ja turvallisuutta (Razaque 2019).

3. KYBERTURVALLISUUDEN UHAT

Kyberturvallisuus on tällä hetkellä puhututtava ja pinnalla oleva aihe. Muun muassa Ylen uutisoinnista on selkeästi nähtävissä, että yksityishenkilöihin, yrityksiin ja myös valtioon kohdistuvien kyberuhkien ja hyökkäysten määrä on kasvanut (Yle 2022). Myös puolustusvoimat ovat ottaneet kantaa tilanteeseen ja toimivat kyberhyökkäysten torjumiseksi (Kerkelä 2022). Uhat kohdistuvat yhtä lailla myös terveydenhuoltoon. Huoltovarmuusorganisaation Digipoolin (2020) julkaisemassa KPMG:n tekemässä selvityksessä kyberturvallisuuden nykytilasta eri toimialoilla terveydenhuollon kyberturvallisuuden kypsyystasoksi oli arvioitu 3,69. Tulos on yli keskinkertaisen tason. (Huoltovarmuuskeskus 2020) Myös Digibarometrissa vuodelta 2020 Suomen kyberturvallisuuden tason on todettu olevan yli keskiarvon muihin Euroopan maihin verrattuna. Huomiona on kuitenkin myös mainittu, että kyberturvallisuuden kehityksen saralla Suomi on jäämässä jälkeen kärkimaita. (Mattila et al. 2020)

Tässä luvussa käsitellään kyberturvallisuuden keskeisimpiä uhkia terveydenhuollossa paneutumatta syvemmin mihinkään yksittäiseen uhkaan. Tarkoituksena on avata käsitystä siitä, minkälaisia haavoittuvuuksia ja uhkia on olemassa sekä perustella jatkon kannalta, miksi erilaisia menetelmiä kyberturvallisuuden takaamiseksi käytetään eli millaisia ja minkä tason uhkia niillä pyritään ehkäisemään. Lisäksi avataan muutamaa tapausta Suomessa terveydenhuoltoon kohdistetuista kyberhyökkäyksistä.

3.1 Terveydenhuollon haavoittuvuudet

Kyberuhkia samoin kuin kyberturvallisuutta yleisesti voidaan analysoida käyttäen apuna kybermaailman tarkasteluun Martin C. Libickin toimesta luodusta nelikerroksisesta rakenteesta johdettua viisikerroksista mallia, joka sisältää fyysisen, syntaktisen, semanttisen sekä palvelu- ja kognitiivisen kerroksen (engl. physical, syntactic, semantic) (Norri-Sederholm et al. 2019). Malli ja sen tasojen sisältö on esitetty kuvassa 3.

Kuva 3: Viisikerroksinen verkostomalli ja sen tasojen sisältö (Muokattu lähteestä Norri-Sederholm et al. 2019)

Kuvassa 3 jokainen kerros tuottaa palveluja ylempänä olevalle kerrokselle ja vastaavasti käyttää alla olevan kerroksen tarjoamia palveluja.

Semanttiselle tasolle voidaan sijoittaa haavoittuvuuksia kuten puutteellinen tietosuojaus, heikko varmuuskopiointi sekä ohjelmistovirheet (Norri-Sederholm 2019, s.91). Ohjelmistojen virheitä, jotka altistavat tietoturva tai tietosuojaloukkauksille, kutsutaan ohjelmistojen haavoittuvuuksiksi. Huonossa tapauksessa ohjelmistojen haavoittuvuuksien avulla voidaan esimerkiksi levittää haittaohjelmia, suorittaa mielivaltaisia komentoja, laajentaa käyttöoikeuksia, paljastaa salassa pidettäviä tietoja tai estää ohjelmiston tai järjestelmän toiminta. (Kyberturvallisuuskeskus 2016)

3.1.1 Tietoverkkoon kytketyt laitteet

Syntaktisen tason haavoittuvuudet liittyvät laitteisiin, jotka ovat kytkettynä tietoverkkoon (Norri-Sederholm 2019, s.91). Esimerkiksi terveydenhuollossa käytettävät mobiili- ja lääkinnälliset laitteet sekä niihin liittyvät heikosti suojatut etäyhteydet kuuluvat kyseiseen kategoriaan. Mobiililaitteiden tapauksessa käyttöä ei välttämättä ole rajattu rakenteellisesti suojattuun tilaan, vaan se on mahdollista missä vaan (Pöyhönen et al. 2019). Toisin kuin Pöyhönen et al. (2019) esittää nykyään mobiililaitteiden kyberturvallisuus on jopa

paremmalla tasolla kuin perinteisissä tietokoneissa, sillä mobiililaitteiden käyttöjärjestelmät ovat rajatumpia eikä käyttäjä voi ohjelmoida niitä uudelleen (Hyppönen 2020, s.74–75). Terveydenhuollossa sairaalajärjestelmiin liittyvien tietoteknisten laitteiden ja ohjelmistojen, mukaan lukien mobiililaitteet, on kuuluttava tietohallinnon hallinnan piiriin (Pöyhönen et al. 2019, s.17). Tällä tavoin pysytään selvillä niistä laitteista, jotka käsittelevät organisaation tietoja, ja esimerkiksi kadonnut laite on mahdollista poistaa käytöstä tai päivitystä vaatiessa päivittää (Kyberturvallisuuskeskus 2016). Mobiililaitteiden välinen tiedonsiirto ja puhe tapahtuu yleisten matkapuhelinverkkojen kautta, minkä takia on erityisen tärkeää harkita, käytetäänkö mobiililaitteita terveydenhuollon kriittisissä toiminnoissa. (Pöyhönen et al. 2019, s.17)

Myös lääkinnälliset laitteet ja niiden etäyhteydet muodostavat merkittävän riskin kyberturvallisuudelle. Terveydenhuollossa laitteiden, järjestelmien, internetin ja ohjelmistojen integroiminen on yhä yleisempää ja tarjoaa lisäkapasiteettia ja kykyä vastata potilaiden tarpeisiin (Williams & Woodward 2015). Integrointi aiheuttaa kuitenkin myös uhkia kyberturvallisuuden kannalta. IoT:ä tukeville lääkinnällisille laitteille kyberturvallisuus on yksi suurimmista haasteista (Razaque et al. 2019). Langattomia yhteyksiä käytetään yhä enemmän ja lääkinnälliset laitteet ovat yhdistettynä internetiin. Laitteiden keräämää tietoa halutaan hyödyntää muissa terveydenhuollon järjestelmissä, mikä lisää niiden alttiutta kyberuhille. (Williams & Woodward 2015) Lääkinnällisten laitteiden kautta on mahdollista tehdä hyökkäyksiä, jotka vaarantavat potilasturvallisuuden ja samalla on mahdollisuus myös suurempaan, jopa organisaation laajuiseen hyökkäykseen (Integrating the Healthcare Enterprise 2015). Internetin saatavuus lääkinnällisissä laitteissa mahdollistaa sen, että hakkerit voivat saada käsiinsä arkaluontoisia potilastietoja. Lisäksi huonossa tapauksessa IoT-laitteille voidaan ladata haittaohjelmia, jotka vaarantavat potilasturvallisuuden. (Razaque et al. 2019)

Terveydenhuollon laitoksissa sijaitsevien laitteiden haavoittuvuuksien lisäksi nykyään on myös otettava huomioon erilaisten potilaisiin kiinnitettävien implanttien kyberturvallisuus. IoMTs määritelmään sisältyy muun muassa implantoitavat lääkinnälliset laitteet (engl. Implantable medical device, IMD) (Rathore et la. 2018). Potilaisiin voidaan asettaa esimerkiksi internetiin yhteydessä olevia infuusiopumppuja, implantoitavia kuvantamisjärjestelmiä, sydämentahdistimia, defibrillaattoreita sekä kehon ulkopuolelle jääviä EKG-antureita (Williams and Woodward 2015, Razaque et al. 2019). Tolonen (2022) mainitsi spesifinä esimerkkinä välikorvaimplantin, sillä se on laite, jonka ääniprosessori on mahdollista liittää bluethoothin tai prosessorin sisältämän puhelinkelan välityksellä ulkoisiin laitteisiin kuten matkapuhelimeen (Hearing Link 2021). Keskeistä on siis se, miten voidaan turvata implantoidun digitaalisen laitteen turvallisuus suojatun verkon ulkopuolella.

Langattoman yhteyden avulla IMD:n tietoja on mahdollista nähdä etänä esimerkiksi lääkärin toimesta. Langattomuus antaa kuitenkin hyökkääjille mahdollisuuden nähdä potilaan tietoja tai jopa ohjelmoida laitetta uudelleen potilasta vahingoittavalla tavalla. (Rathore et al. 2018) Rathoren et al. (2018) mukaan viime vuosina IMD:n suojaamiseen on ehdotettu erilaisia menetelmiä kuten biometristä tai kryptografista menetelmää todentamiseen, koneoppimismenetelmiä poikkeamien havaitsemiseen sekä ulkoisia puettavia laitteita, jotta langaton yhteys voitaisiin suojata. Ongelma langattomissa laitteissa on kuitenkin se, että niiden ylläpito muistirajoitteisilla laitteilla on järjestelmälle raskasta ja lisäksi ne voivat vaatia muita vaihtoehtoisia puettavia laitteita toimiakseen (Rathore et al. 2018).

3.1.2 Verkkoyhteydet ja ohjelmistot

Terveydenhuollon laitteiden ja järjestelmien säännöllinen päivittäminen on tärkeää kyberturvallisuuden kannalta. Ohjelmistopäivitykset takaavat järjestelmän tehokkuuden ja turvallisuuden. Turvallisuuspäivitykset ovat yleisiä terveydenhuollon järjestelmissä ja niiden pääasiallisena tarkoituksena on turvata arkaluontoiset potilastiedot ja pitää terveystiedot yleisesti turvallisessa ympäristössä. (MedicalDirector 2018) Päivittämättömät järjestelmät ovat yksi terveydenhuollon haavoittuvuuksista. On huolehdittava, että laitteiden puolustusjärjestelmät kuten haittaohjelmien torjunta ja tietoturvakorjaukset ovat jatkuvasti ajan tasalla (Sardi et al. 2020). Laitteiden päivitykset laitteenvalmistajien toimesta ovat myös riski kyberturvallisuudelle, sillä usein päivitykset tai ongelmatilanteet hoidetaan etäohjauksella (Kyberturvallisuuskeskus 2016). Laitteenvalmistajilla on laitteissaan aina oma varusohjelmisto ja yleensä he pitävät sopimuksella oikeuden siihen, ettei laitteiden ohjelmistoa voi päivittää muut tahot kuin laitteenvalmistaja. Tämän taustalla on se, että laitteen toimivuus halutaan valmistajan taholta varmistaa. Terveydenhuollossa tällaiset laitteet esimerkiksi kuvantamislaitteet voidaan eristää verkon segmentoinnin avulla. Tällöin laite on omassa segmentissään, joka eristetään palomuurein muusta tietoverkosta. (Kyberturvallisuuskeskus 2016; Tolonen 2022)

Fyysiselle tasolle kuuluvat haavoittuvuudet liittyen verkkoihin ja langattomiin yhteyksiin. Hyökkäykset, jotka toteutetaan verkon kautta tähtäävät verkkoon liitettyjen laitteiden haavoittuvuuksien tunnistamiseen ja sitä kautta niiden hyödyntämiseen. Verkon kautta hyökkäykset kohdistuvat tavallisesti verkkopalvelimiin, tietokantoihin tai sovellusohjelmistoihin. Verkkopalvelinten haavoittuvuuksien tunnistamista varten on mahdollista jopa ladata Internetistä ohjelmia, joita hyökkääjä pystyy käyttämään hyväkseen suunnitellessaan hyökkäystä.

Laitteet ja järjestelmät tallentavat tiedot yleensä johonkin tietokantaan. (Williams and Woodward 2015) Nykyään sairaalat käyttävät jo suurelta osin pilvipalveluja tietojen tallentamiseen kiinteiden tietovarastojen sijaan, mutta myös näihin kiinteisiin tietovarastoihin liittyy kyberturvallisuuden riskejä (Razaque et al. 2019). Kiinteisiin tietovarastoihin, jotka käyttävät strukturoitua kyselykieltä (engl. structured query language, SQL), on mahdollista kohdistaa SQL-injektio. Se on vakava hyökkäys, joka on seurausta SQL-kielen väärin määrittelystä. Sen seurauksena tietoturvan tavoitteet luottamuksellisuus, eheys ja saatavuus heikentyvät. (Williams and Woodward 2015)

3.2 Kyberuhat ja -hyökkäykset

Jotta olisi mahdollisuus suojautua kyberuhkia vastaan, on tehtävä arviointi uhista, joita organisaatioon, tässä tapauksessa terveydenhuoltoon, kohdistuu. Tämän lisäksi on arvioitava uhkien vakavuusastetta. Keskeisimmät kysymykset arvioitaessa kyberturvallisuuden uhkia siis ovat: Miltä turvataan? Mitä turvataan? ja Miten turvataan? Nämä kysymykset koskevat mitä tahansa turvallisuuden osa-aluetta ja sen parantamisen pohdintaa. (Limnéll 2014, s.37-38) Uhka-analyysi on avainroolissa terveydenhuollon kyberturvallisuuden takaamisessa.

Uhkien arviointi on oleellinen osa organisaation riskienhallintaa. Häiriötilanteissa riskienhallinta takaa organisaation toiminnan jatkumisen. Kriittiset riskit voidaan tunnistaa riskienhallinnan avulla. Se tarkoittaa palveluiden ja järjestelmien tärkeyden analysoimista organisaation toiminnan kannalta sekä niihin vaikuttavien uhkien, myös tietoturva- ja kyberturvallisuusuhkien, merkitystä palveluiden ja järjestelmien toimintakykyyn. Turvallisuusmenettelyjä koskien organisaatiolla on oltava yksiselitteiset toimintaperiaatteet. (Vuorinen 2019, s.22)

Terveydenhuollon yleisimpiä ja tyypillisimpiä kyberuhkia ovat:

1. Tietovarkaus taloudellisen hyödyn saamiseksi
2. Tietovarkaus sen aiheuttaman vaikutuksen vuoksi
3. Kiristyshaittaohjelmat
4. Datan korruptointi
5. Palvelunestohyökkäykset
6. Yrityssähköpostin vaarantaminen
7. Organisaation työntekijät, jotka tietämättään ja tahattomasti aiheuttavat kyberuhkia (Martin et al. 2017).

Taulukkoon 1 on kerätty mainittujen uhkien määrittelyt.

Taulukko 1: Terveydenhuollossa ilmenevät tyypillisimmät ja yleisimmät kyberuhat (muokattu lähteestä Martin et al. 2017)

1.	Taloudellisen hyödyn saamiseksi tehdyllä tietovarkaudella tavoitellaan yleensä henkilökohtaisia tietoja kuten nimiä, henkilöturvatunnuksia, osoitteita tai taloustietoja.
2.	Hyökkäyksen tekeminen sen aikaansaaman vaikutuksen takia tarkoittaa, että sen avulla pyritään varastamaan ja julkaisemaan arkaluonteisia terveystietoja esimerkiksi vaikutusvaltaisista tai tunnetuista henkilöistä.
3.	Kiristyshaittaohjelman toiminta perustuu siihen, että se estää käyttäjien pääsyn heidän omiin tietoihinsa tai järjestelmiinsä tai jopa uhkaa poistaa tietoja, ellei käyttäjä maksa pyydettyä summaa.
4.	Datan korruptointi on tahallista esimerkiksi testitulosten peukalointia, jonka tavoitteena on hyötyä siitä henkilökohtaisesti tai poliittisesti.
5.	Palvelunestohyökkäys (engl. denial-of-service attack, DDoS) on hyökkäysmuoto, jossa verkkoon tai järjestelmään aiheutetaan häiriö kiristykseen, kostoon tai aktivismiin tähtäävillä tarpeettomilla pyynnöillä.
6.	Taloudellisen hyödyn tavoitteleminen hankkimalla petollisesti maksuja tai henkilökohtaisia tietoja käyttämällä väärennettyä viestintäkanavaa vaarantaa yrityssähköpostin.
7.	Vanhentuneiden ja riskialttiiden järjestelmien käyttäminen työntekijöiden toimesta altistaa tahattomasti tietojen menetykselle ja järjestelmien häiriöille.

Voidaan huomata, että terveydenhuoltoa uhataan monella eri tavalla, minkä takia olisikin tärkeää, että terveydenhuollon organisaatioissa käytettäisiin tarpeeksi varoja ja keskitettäisiin huomiota kyberturvallisuuteen ja sitä käsitteleviin koulutuksiin.

Inhimilliset tekijät ovat myös yksi terveydenhuollon kyberturvallisuuden haavoittuvuus. Järjestelmien käyttötavat ja mahdollisten kyberuhkien tunnistaminen terveydenhuollon ammattilaisten keskuudessa vaikuttavat organisaation kyberturvallisuuteen. Syynä henkilöstön kyvyttömyyteen tunnistaa mahdolliset hyökkäykset, esimerkiksi tietojenkalastelu, on muun muassa tietämättömyys terveydenhuollon ja sairaaloiden kohtaamista kyberuhista ja siten myös henkilöstön aiheeseen liittyvän koulutuksen puute. (Nifakos et al. 2021, s.17) Osaava ja valpas henkilökunta vähentää osaltaan potilastietoihin kohdistuvia tietosuojaloukkausyrityksiä.

3.2.1 Terveydenhuoltoon kohdistuneita kyberhyökkäyksiä

Suomessa niin terveydenhuoltoon kuin muuhunkin infrastruktuuriin on kohdistunut viime vuosina yhä useampia kyberhyökkäyksiä ja niiden uhka kasvaa koko ajan. Kiristyshaittaohjelmat ja hakkerointi ovat yleisimpiä tapauksia, kun tarkastelussa on terveydenhuoltoon kohdistuneet kyberhyökkäykset (Lehto et al. 2019). Viime vuosina tapahtuneita

enemmän huomiota saaneita kyberhyökkäyksiä ovat esimerkiksi Turun yliopistollisessa keskussairaalassa (TYKS) 2017 tapahtunut hyökkäys kuvantamislaitteisiin, psykoterapiakeskus Vastaamon tietomurto loppuvuodesta 2020, Terveystalon ajanvarausjärjestelmään kohdistunut tietojen kalastelu keväällä 2020 sekä Lahden kaupungin tietoverkkoon ujutettu haittaohjelma kesällä 2019.

WannaCry on vuonna 2017 ympäri maailmaa levinnyt kiristyshaittaohjelma (Yle 13.5.2017), joka leviää itsenäisesti ja pitää uhrin tietoja salattuna, kunnes vaaditut lunnaat on maksettu. WannaCry-epidemia on historian yksi suurimmista kiristyshaittaohjelma hyökkäyksistä ja sen vaikutukset ulottuivat sairaaloihin, yrityksiin ja kuluttajiin yli 150 maassa. (Chen & Bridges 2017) TYKS:n muutamat kuvantamislaitteet saastuivat harrastelijoiden toimesta muunnellulla WannaCry -kiristyshaittaohjeman kakkosversiolla. Kohteena olleet lääkinnälliset laitteet olivat päivittämättömiä laitteita, joihin vain laitteen toimittaja kykeni tekemään päivityksiä. Seurauksena haittaohjelmasta olivat laitteiden järjestelmien kaatuilu ja hidastuminen. Aiemmin samana vuonna ilmenneiden hyökkäysten jälkeen muihin laitteisiin oli jo tehty tarvittavat päivitykset. Hyökkäyksen jälkeen kuvantamislaitteiden päivitykset käytiin laitteiden toimittajien kanssa läpi. Tässä tapauksessa palomuuri ehkäisi ohjelman yhteyden TYKS:n verkosta ulospäin. (Yle 10.6.2017)

Lahdessa tapahtui kesäkuussa 2019 laajuudeltaan merkittävä ja vakava kyberhyökkäys, kun kaupungin tietoverkkoon ujutettiin haittaohjelma. Sen seurauksena verkko kuormittui ja haittaohjelma levisi koneelta, jolla se oli havaittu noin tuhanteen muuhun työasemaan. Vaikutuksia hyökkäyksestä olivat muun muassa merkittävät häiriöt terveysasemilla ja hammashoidossa, kun potilaskertomusten tiedot eivät näkyneet eikä laboratoriovastaukset ja röntgenkuvat olleet käytettävissä. Haittaohjelma tunnistettiin ja eristettiin virustorjunnan avulla. (Yle 12.6.2019) Hyökkäyksen seurauksena Lahden tietoliikenneverkko jaettiin pienempiin hallinnollisiin osiin ja tietoliikenteen valvonnalle kehitettiin sitä tukevia järjestelmiä. Myös tietoturvapoikkeamien jäljitettävyyttä parannettiin. Näiden toimenpiteiden avulla tietoliikenneverkon turvallisuutta pyrittiin parantamaan. (Yle 8.8.2019)

Terveystalo sai helmikuussa 2020 kiristysviestin, jonka johdosta tuli esille, että sähköisessä verkkoajanvarausjärjestelmässä ollutta haavoittuvuutta oli käytetty hyödyksi ja sen seurauksena oli tietovuoto. Haavoittuvuus oli siis ollut jo tiedossa aiemmin, mutta sille ei vielä ollut ehditty tekemään toimenpiteitä. Tietojenkalastelun seurauksena asiakkaiden henkilötietoja, kuten nimiä ja henkilötunnuksia joutui mahdollisesti ulkopuolisten käsiin. Tapauksen seurauksena ajanvarausjärjestelmän teknistä valvontaa lisättiin ja myöhemmin siinä otettiin käyttöön myös vahva tunnistautuminen. (Yle 3.2.2020)

Psykoterapiakeskus Vastaamoon tehtiin tietomurto 29.9.2020. Yhtiöltä vietiin asiakkaiden luottamuksellisia tietoja. Hyökkääjä julkaisi osan varastetuista tiedoista Tor-verkossa ja uhkasi julkaista lisää, jos lunnaita ei makseta. Kiristäjä ei kuitenkaan julkaissut lisää tietoja. Tietoturvayhtiö F-Securen tutkimusjohtaja Mikko Hyppösen mukaan kyseessä oli kansainvälisesti poikkeuksellinen tietomurto, sillä aiemmin ei vastaavalla mittakaavalla ole tapahtunut kiristystä psykoterapiatiedoilla. (Yle 25.10.2020)

Näiden Suomessa tapahtuneiden kyberhyökkäysten perusteella voidaan huomata, miten merkittävät vaikutukset terveydenhuoltoon kohdistuvilla kyberuhilla voi olla. Vaikutukset ovat merkittäviä siksi, että hyökkäysten yhteydessä häiriöitä on aiheutunut myös reaaliaikaisiin palveluihin kuten potilastietojärjestelmiin (Lehto et al. 2019). Terveydenhuollon haavoittuvuuteen vaikuttaa monia tekijöitä. Rajalliset resurssit, hajanainen hallinto ja kulttuurinen käyttäytyminen kuvastavat terveydenhuollon haavoittuvuutta. Muihin aloihin verrattuna terveydenhuollossa rahoitus IT-infrastruktuuriin on alimitoitettu. (Martin et al. 2017, s.2) Perehtyneisyys tietotekniikkaan, erilaisiin uhkahahmotelmiin ja organisaation työskentelytapoihin ovat edellytyksiä sille, että organisaation kyberturvallisuutta voidaan kehittää. Kyberturvallisuusalan osaajat työskentelevät terveydenhuoltoorganisaatioiden tietojenhallintayksiköissä, jotka muun muassa tuottavat verkkoyhteydet lääkinnällisille laitteille. Suurin tarve heidän osaamiselleen on kuitenkin lääkinnällisten laitteiden ylläpidon parissa, sillä laitteet aiheuttavat terveydenhuollon kyberturvallisuuden kannalta suurimpia uhkia. Lääketieteellisen tekniikan yksiköllä on vastuu lääkinnällisten laitteiden ylläpidosta eikä heidän keskeisin prioriteettinsa ole kyberturvallisuus vaan potilaiden hyvä ja tehokas hoito. Ongelmana siis on, että tarvittava osaaminen on hajallaan. Poikkihallinnolliset asiantuntijaryhmät voisivat olla yksi ratkaisu tähän ongelmaan. (Kyberturvallisuuskeskus 2016)

3.2.2 Uhkien muutokset viime vuosina

Digitalisaatiolla ja sen kehityksellä on suuri merkitys terveydenhuoltoon kohdistuvissa kyberuhissa ja niiden muutoksessa. Digitalisaation kehitys jatkuu edelleen ja se muodostaa täysin uudenlaisen toimintaympäristön terveydenhuollontoimijoille. Laajemmat hallittavat kokonaisuudet muodostuvat uusista lääkinnällisistä laitteista, älykkäistä sensoreista, ohjelmistoista sekä tekoälystä ja robotiikasta. Myös tehokkaammat tietoverkot ja pilvipalvelut uusien laitteiden ja ohjelmistojen tehokkaan toiminnan mahdollistajina

muokkaavat toimintaympäristöä edelleen. (Nuorten Lääkärien Yhdistys 2020) Tässä korostuu henkilöstön digikoulutuksen ja ajan tasalla säilyvän, uuteen toimintaympäristöön liittyvän osaamisen tärkeys.

Kyberturvallisuusosaaminen ei ole kaikilla toimialoilla keskiössä tai edes lähellä sitä. Tällaisilla aloilla olisi ensisijaisen tärkeää parantaa henkilöstön kyberturvallisuusosaamista kertoo Huoltovarmuusorganisaation Digipoolin julkaisu (2020) Kyberturvallisuuden nykytila eri toimialoilla. Terveydenhuolto voidaan lukea mukaan näihin toimialoihin, mutta koulutukset ja suunnitellut harjoitukset ovat olleet hiljattain osana kyberturvallisuuden esille tuomisessa myös terveydenhuollossa. (Huoltovarmuuskeskus 2020)

Sairaaloissakin käytössä yleistyneet IoT-laitteet itsessään sekä niiden käyttämä nopea 5G-verkko tuovat mukanaan uusia kyberuhkia. Ongelmana on laitteiden suojaus, sillä niiden tietoliikenne ei kulje sairaalaorganisaation omien tietoturvakontrollien läpi, vaan on suorassa yhteydessä palveluntarjoajaan. Ongelma on tämän lisäksi myös siinä, ettei laitteita ole salasanan lisäksi välttämättä suojattu tietoturvaa ylläpitävästi mitenkään. (Vertainen 2021) Paloalto Networks (2020) analysoi 1,2 miljoonaa IoT-laitetta ja niistä 98 prosentilla oli käytössä heidän tutkimuksensa mukaan salaamaton tiedonsiirtoyhteys. Tutkimuksessa huomattiin myös, että kuvantamislaitteisiin kohdistuu terveydenhuollon IoT-laitteista eniten häiriöitä ja vanhentuneita käyttöjärjestelmiä oli käytössä 83 prosentilla tutkituista laitteista. Tästä voidaan muistaa myös aiemmin mainittu TYKS:ssä tapahtunut hyökkäys, joka käytti hyväkseen nimenomaan päivittämättömiä kuvantamislaitteiden järjestelmiä.

Oman vaikutuksensa kyberuhkien muutokseen on tuonut osaltaan myös koronapandemia. Koronan aikana uhat lääkealaa ja terveydenhuoltoa kohtaan lisääntyivät ja tietojenkalastelu sekä kohdennetut kiristyshaittaohjelmat yleistyivät muun muassa koronarokotteita jakavilla tahoilla. Kyberturvallisuuskeskus arvioi, että vuodesta 2019 verkkohuijausten määrä on jopa viisinkertaistunut. (Elinkeinoelämän tutkimuslaitos 2020; Security Intelligence 2020) Koronapandemian aikana digitaaliset terveydenhuoltosovellukset kuten etävastaanotot ja -palvelut ovat lisääntyneet. Terveydenhuollon etäpalvelut voivat sisältää esimerkiksi potilaan tutkimisen, diagnostiikan, seurannan tai hoitoon liittyvien päätösten teon verkkoyhteydellä esimerkiksi videon välityksellä (Valvira 2022). Etäpalveluihin kohdistuu luonnollisesti myös mahdollisia kyberuhkia. Asianmukaiset laitteet, yhteydet ja järjestelmät sekä tilat ja koulutettu henkilökunta ovat oltava kunnossa etäpalvelun antajalla (Valvira 2022). Etäpalveluissa on otettava huomioon potilasturvallisuus ja palveluiden on oltava lääketieteellisesti asianmukaisia. Kyberturvan näkökulmasta on tär-

keää, että etäpalveluissa käytettävien tietojärjestelmien salassapitoa, tietosuojaa ja tietoturvaa koskevat säädökset täyttyvät, jotta potilastietojen välitys ja tallennus on turvallista. (Valvira 2022)

3.3 Uhkien yhteenveto

Julkinen terveydenhuolto on infrastruktuuria, joka kohtaa kasvavan digitalisaation kynnyksellä paljon kyberturvallisuuden uhkia ja joka myös sisältää paljon erilaisia haavoittuvuuksia liittyen terveydenhuollon tietoverkon suojaamiseen, pilvipalveluihin, lääkinnällisiin laitteisiin, näyttöpäätteisiin sekä tunnistautumiseen ja tietojen salaukseen. Uudet teknologiat ja järjestelmät kehittyvät ja muuttuvat paljon nopeammin, kuin niitä pystytään suojaamaan. Turvallisuusjärjestelmiä tulisi päivittää ja rakentaa jatkuvasti vastaamaan muuttuvia teknologioita ja yhä moninaisempia uhkia (Kruse et al. 2017).

Krusen et al. (2017) tekemässä tutkimuksessa käsiteltiin terveydenhuollon kyberturvallisuuden uhkia koskevia artikkeleita ja niissä tehtyjä päätelmiä sekä koottiin yhteenveto yleisimmin tunnetuista uhista ja haavoittuvuuksista. Tutkimukseen kootuissa artikkeleissa oli nähtävissä yhdenmukaisuus siitä, että terveydenhuoltoon kohdistuvat kyberuhat kasvavat jatkuvasti ja näihin uhkiin ei olla valmistauduttu riittävällä tasolla. Toisin kuin ennen, lääkinnälliset laitteet ovat nyt yhteydessä tietoverkkoon, jolloin ne ovat muiden IT-järjestelmien tavoin alttiita kyberhyökkäyksille (Kruse et al. 2017). Ongelmana on myös se, että lääkinnällisten laitteiden valmistajat kehittävät verkkointegraatiota jatkuvasti, mutta siitä aiheutuvat kyberuhat ja niihin varautuminen jätetään liian vähälle huomiolle (Rios 2015; Wu & Eagles 2016).

Terveydenhuollon organisaatiot pyrkivät huolehtimaan arkaluontoisten terveystietojen suojelemisesta, mutta uusia kyberhyökkäysmenetelmiä syntyy koko ajan ja niiden vaikutus on pysyvä. Terveydenhuolto pyrkii haasteiden keskellä jatkuvasti kehittämään IT-teknologioitaan ja samaan aikaan huolehtimaan turvallisuusvaatimuksista. Tämä on tärkeää, sillä terveydenhuolto on yksi kyberhyökkäysten pääkohteista arkaluontoisinen tietoineen. Kun terveydenhuoltoa verrataan muihin johtaviin teollisuuden aloihin, kyberturvallisuudessa ja tärkeiden tietojen turvaamisessa ollaan jäljessä. Kehitystä tapahtuu jatkuvasti ja turvallisuusalan yritykset pyrkivät yhdessä hallituksen kanssa hidastamaan kyberhyökkäysten leviämistä. (Kruse et al. 2017) Ennakoiva toiminta ja uhkiin varautuminen on haastavaa muuttuvassa kybertoimintaympäristössä, mutta sitä on kutenkin tavoiteltava. Terveydenhuollossa rahoitusta on kohdistettava riittävästi ja kasvavissa määrin potilastietojen ja terveydenhuollon teknologioiden kuten lääkinnällisten laitteiden suojaamiseen sekä sopeutumiseen uusiin kyberturvallisuuden trendeihin, jotta voidaan taata potilaiden turvallinen hoito ja potilastietojen luottamuksellisuus (Kruse et al. 2017).

4. KYBERTURVALLISUUDEN RATKAISUT SUOMESSA

Terveydenhuollon kyberturvallisuuden ylläpitäminen ulottuu monelle tasolle. Kyberturvallisuutta voidaan tarkastella sekä hallinnollisella että teknisellä tasolla. Tässä luvussa keskitytään teknisiin menetelmiin ja jo aiemmin esitetyn kybermaailman viisikerroksisen mallin fyysiseen kerrokseen. Terveydenhuollon lääkinnällisten laitteiden, niiden ohjelmistojen ja järjestelmien suojaaminen tapahtuu muun muassa palomuurien, verkon segmentoinnin ja salausten sekä valvonnan avulla. Nämä ratkaisut pyrkivät pitämään ei toivotut tunkeilijat kuten hakkerit organisaation sisäverkon ulkopuolella, jotta he eivät pääse aiheuttamaan siellä vahinkoa kiristyshaittaohjelmien, palvelunestohyökkäysten tai muiden tietomurtomenetelmien avulla.

Suomalaisessa terveydenhuollossa käytetyt tietoturvaratkaisut tulevat pääosin maailmalta, eivätkä siten eroa merkittävästi muualla maailmassa käytettävistä teknisistä ratkaisuista (Tolonen 2022). Suomalaisia kyberturvallisuusratkaisuja tuottaa esimerkiksi tietoturvayhtiö WithSecure™ (WithSecure™ 2022).

4.1 Tekniset menetelmät

Tärkeimpiä turvatoimenpiteitä organisaatiossa kuten sairaalaympäristössä ovat verkon segmentointi ja siihen liittyvät palomuurit, verkon valvonta ja tunkeutumisten havainnointi, vankka salaus sekä käytön todennus ja valtuutus (ENISA 2016, s. 53). Kaksi viimeistä kuuluvat aiemmin mainittuun AAA-malliin, jonka avulla kyberturvallisuuden periaatteet voidaan toteuttaa. Terveydenhuollon toimijoiden pääsy esimerkiksi potilastietoihin vaatii henkilöllisyyden todentamisen (Pöyhönen et al. 2019, s.25). Aiemmin tuli esille, että henkilöllisyyden todentamiseen voidaan käyttäjätunnusten ja salasanojen lisäksi käyttää vahvaa tunnistautumista. Vahva tunnistautuminen kattaa verkkopankkitunnukset, mobiilivarmenteet sekä erilaiset henkilö- ja toimikortit. (Astala 2022) Jotta terveydenhuollon kyberturvallisuutta voidaan parantaa, tarvitaan kattava ymmärrys niin tietoturvasta kuin myös terveydenhuollon toimintatavoista.

Terveydenhuoltoon kohdistuvien uhkien yhteydessä mainittiin, että terveydenhuollon lääkinnällisiin laitteisiin liittyy kyberuhkia. Oikeastaan suurimmat uhat kohdistuvatkin niihin (Pöyhönen et al. 2019, s.16). Pöyhönen et al. (2019, s.26) mainitsee, että yleisen käsityksen mukaan huomattava rooli organisaatioiden kyberturvallisuuden kehittämisen

kannalta on eri tahojen tekemällä yhteistyöllä ja tiedonvaihdolla. Verkkorikollisuuden riskienhallinnassa on mukana laajalti eri sidosryhmiä, joten erityisesti kun kyseessä on lääkinnälliset laitteet ja järjestelmät sekä niiden kyberturvallisuuden kehittäminen, on huomioitava yhteistyön ja tiedonvaihdon toimivuus. Kehitystyöhön osallistuvia sidosryhmiä ovat laitteiden valmistajat ja käyttäjät, järjestelmäintegraattorit sekä terveydenhuollon omat ICT-yksiköt. (Pöyhönen et al. 2019, s.26) Terveydenhuollossa kuten missä tahansa muussakin organisaatiossa halutaan varmasti luoda mahdollisimman korkea turvallisuuden taso. Tämä tarkoittaa kuitenkin myös korkeita kustannuksia varsinkin silloin, kun kyberturvallisuuden kehittyessä myös huipputekniset turvallisuusratkaisut ovat mahdollisia (Pöyhönen et al. 2019, s.25). Kustannukset ovatkin yleensä yksi rajoittava tekijä, joten tietyssä pisteessä on hyväksyttävä tietoturvariskit, jotka organisaatiolle jää käsiteltäviksi erilaisista menetelmistä huolimatta (Pöyhönen et al. 2019, s.25).

4.2 Verkon segmentointi

Ensisijaisesti haittaohjelmien tarttumista ja leviämistä pyritään ehkäisemään käyttäjien turvallisilla laitteiden käyttötavoilla, päivitetyillä ja turvallisesti määritetyillä ohjelmistoilla sekä virustorjuntaohjelmistoilla. Verkon segmentointi on keino, jonka merkitys tulee ilmi hyökkäystilanteessa, kun haittaohjelma pääsee saastuttamaan organisaation hallitseman laitteen. Verkon segmentoinniksi kutsutaan sitä, kun tietoverkko jaetaan pienempiin osakokonaisuuksiin sen mukaan, mihin tarkoitukseen siihen liitetyt laitteet ovat (Vuorinen 2019, s.61). Toisin sanoen verkko siis jaetaan toiminnallisiin lohkoihin muun muassa sen perusteella, miten kriittistä siihen liitettyjen laitteiden toiminta on ja miten turvattuja niiden tulee olla. Sellaiset tietojärjestelmät, jotka ovat toiminnan jatkuvuuden kannalta kriittisiä, ovat parhaiten suojattu. (Pöyhönen et al. 2019, s. 37) Vuorisen (2019) mukaan useissa sairaaloissa riittävä segmentointi kuitenkin uupuu, mikä on tietenkin riski päätelaitteen saastuessa.

Terveydenhuollossa olisi erityisen tärkeää, että lääkintälaitteet on erotettu potilashoitoon liittyvistä - ja toimistotyöasemista (Vuorinen 2019, s.61). Lisäksi myös etähallittavat laitteet on syytä segmentoida omaan verkko lohkoonsa, jotta voidaan välttää organisaation sisäverkon vaarantuminen etähallittavien laitteiden haavoittuvuuksista aiheutuvista syistä (Kyberturvallisuuskeskus 2016; Norri-Sederholm et al. 2019, s.95). Etähallittavien laitteiden tapauksessa segmentoinnin lisäksi on myös huolehdittava, että tietojen suojaamiseen ja vastuukysymyksiin liittyvät asianmukaiset sopimukset ovat kunnossa. Muun muassa palomuurien käyttö, vahva tunnistautuminen, yhteyden salaus sekä

etäyhteyden käytön mahdollistavat henkilökohtaiset tunnukset kuuluvat näiden sopimusten piiriin. (Kyberturvallisuuskeskus 2016)

Verkon segmentointi on osa sairaalajärjestelmien vyöhykesuojausta. Vyöhykesuojauksessa suojausvaatimukset ja -tasot määrittelevät sairaalajärjestelmän jaon eri vyöhykeisiin, jotka on erotettu toisistaan fyysisin ja tietoteknisin menetelmin. Eri verkkosegmentit erotetaan toisistaan esimerkiksi palomuurien avulla. (Pöyhönen et al. 2019, s.37) Segmentoinnin avulla verkkoon yhdistettyjä laitteita on mahdollista suojata paremmin (Norri-Sederholm et al. 2019, s.95), kun tarpeettomia yhteyksiä eri laitteiden välillä katkaistaan, eikä hakkereiden ole tällöin mahdollista edetä laitteesta toiseen (Cybernet 2020). Segmentointia siis toteutetaan, jotta mahdollisen haittaohjelman tarttuessa laitteeseen, esimerkiksi toimistotietokoneeseen, sen leviämistä voidaan rajoittaa (Vuorinen 2019, s. 61). Verkon segmentoinnin tärkeydestä kertoo myös se, että se on mainittu NIST:in (National Institute of Standards and Technology) julkaisussa SP800-125 (Scarfone et al. 2011).

Verkon segmentointiin on erilaisia menetelmiä. Se voidaan toteuttaa verkkolaitteilla ja erillisillä galvaanisilla johdotuksilla, palomuurien avulla tai käyttämällä esimerkiksi virtuaalilähiverkkoa (engl. Virtual Local Area Network, VLAN), joka on yksi verkkolaitteiden erotustoiminto. Myös näiden menetelmien yhdistelmät ovat mahdollisia. (Vuorinen 2019) VLAN:t ovat yksi mahdollinen ja suosittu ratkaisu toteuttaa verkon jakaminen pienempiin aliverkkoihin. VLAN:ien avulla voidaan jakaa verkko niiden laitteiden käyttöön, joiden kommunikointi on potilaanhoidon kannalta välttämätöntä ja puolestaan erottaa ne laitteet ja osastot, joiden välinen yhteys ei ole välttämätöntä tehokkaan hoidon takaamiseksi. (Cybernet 2020) Segmentointia voidaan toteuttaa terveydenhuollon jakeluorganisaatioissa esimerkiksi siten, että kaikki verkkoon tai toisiin laitteisiin kytketyt lääkinnälliset laitteet sijoitetaan omalle vyöhykkeelleen samoin kuin laitteet, joita käyttää useammat henkilöt. Tällaisia ovat esimerkiksi magneetti- ja röntgenkuvantamislaitteet. Segmentointi voidaan toteuttaa myös esimerkiksi kiinteistön kerrosten mukaan tai siten, että työntekijöiden omat laitteet on segmentoitu erikseen sairaalan omistamista laitteista. (Wolf 2019)

Karhunen (2020) tutki Pro Gradu -tutkielmassaan muun muassa Tampereen ja Kuopion Yliopistollisten Keskussairaaloiden verkon segmentointikäytäntöjä. Tutkimuksen mukaan perinteiset verkonsegmentointikäytännöt ovat vahvasti näiden sairaaloiden verkon segmentoinnin toteutuksen pohjana. Sairaaloissa verkoilla on pääasiassa yhteinen fyysinen johdotuksien avulla luotu verkko, jonka segmentointi on toteutettu aliverkoilla ja VLAN-yhteyksillä. Tutkimuksessa nousi esiin ainakin kolme erilaista segmentointimetodia, jotka erosivat toisistaan siinä, miten lääketieteellinen VLAN (engl. medical VLAN) eli

verkkoon kytketyille lääkinnällisille laitteille tarkoitettu verkko oli toteutettu. (Karhunen 2020)

4.3 Palomuurit

Palomuurit ovat ohjelmistoihin tai laitteistoihin liitettyjä esteitä, joiden avulla aliverkkoihin pääsyä rajoitetaan ja valvotaan. Palomuurien toiminnan tarkoituksena on estää tietoturvaloukkauksia. Aliverkkoja on erilaisia kuten täysin organisaation sisäinen aliverkko eli intranet, ulkoinen aliverkko eli extranet sekä eteisverkko (engl. demilitarized zone), joka on asetettu organisaation sisäverkon ja internetin väliin. Eteisverkkoa ei suojata eikä siihen myöskään luoteta ja sen kummassakin rajapinnassa on palomuurit. Palomuuri asetetaan tavallisesti suojausalueiden väliin ja on yleistä, että palomuuri on verkon sisääntulopisteessä. Tämän lisäksi palomuureja voidaan sijoittaa verkkoon rajaamaan eri turvallisuusvyöhykkeitä. (Brooks 2014, s.126) Kuten aiemmin mainittiin, palomuurien käyttö on myös yksi verkon segmentoinnin menetelmä. Palomuureja voidaan käyttää siis suojautumaan sekä ulkoa tulevilta hyökkäyksiltä, että organisaation verkon sisällä ehkäisemään hyökkäysten leviämistä.

Aiemmin mainittiin, että IoT: n integraatio kasvaa myös terveydenhuollossa älykkäiden lääkinnällisten laitteiden muodossa. Sen lisäksi, että nämä laiteet tuovat hyötyjä, kuten mahdollisuuden potilaiden etäseurantaan sekä kriittisen sairaanhoidon tarjoamiseen etänä, ne tekevät terveydenhuolto-organisaation verkosta myös haavoittuvamman. (Somasundaram & Thirugnanam 2020). Nykyään ensimmäisen puolustuslinjan suurien hyökkäysten varalle muodostavat palomuurit, jotka vaikuttavat sekä perinteiseen että nykyaikaiseen verkkoon (Anwar et al. 2021). Sähköisten terveystietojen ja verkossa toimivien lääkinnällisten laitteiden turvallinen käyttö niin organisaation sisäisessä verkossa kuin sen ulkopuolella, varmistetaan palomuurien avulla (Perakslis 2014). Jotta palomuuri voi täyttää tehtävänä sen on toimittava suodattimena organisaation sisäisestä verkosta lähteville ja sinne saapuville tietopaketeille. Palomuurijärjestelmän tehokkuuteen vaikuttaa muun muassa palomuurin sijainti sekä suojattavien tietojen luonne. (Anwar et al. 2021)

Palomuurien tärkeys korostuu terveydenhuollossa erityisesti siksi, että älykkäät terveydenhuollon laitteet yleistyvät. Koska terveydenhuollon suurimmat kyberturvallisuuden uhat kohdistuvat juuri lääkinnällisiin laitteisiin, on olennaista pohtia sitä, millaisia palomuureja näiden laitteiden käyttämien verkkojen suojaamiseen käytetään. Perinteisten palomuurien lisäksi enenevissä määrin korostuu myös pilvipohjaisten palomuurien rooli älykkäiden terveydenhuollon laitteiden suojaamisessa (Anwar et al. 2021).

Palomuurit voivat olla joko laite- tai verkkopohjaisia. Vain data, joka on turvallista ja harmitonta, pääsee läpi palomuureista sekä sisä- että ulkopuolelta. Palomuureille asetetaan sääntöjä, jotka perustuvat tietokoneiden IP-osoitteisiin ja internetprotokolliin. Näiden perusteella datapaketit joko läpäisevät palomuurin tai eivät. (Anwar et al. 2021)

Palomuureja on sekä pilvipohjaisia että perinteisiä palomuureja (Anwar et al. 2021). NIST on listannut julkaisussaan (Special Publication 800–101) kolme perinteisten palomuurien luokkaa ja ne ovat pakettisuodatuspalomuurit, tilalliset palomuurit sekä välityspalvelinpalomuurit (Ajijola et al. 2014). Palomuurien toiminta voi perustua pakettisuodatukseen, verkko-osoitteiden muuntamiseen tai välityspalvelimiin (engl. Packet filtering, Network address translation or Proxy service). Pakettisuodatuksessa palomuuri sisältää sääntöjä liittyen paketin tulo- ja kohdeportteihin sekä IP-osoitteisiin (engl. Internet Protocol address). Näiden sääntöjen perusteella paketti joko päästetään läpi tai hylätään. Verkko-osoitteiden muuntamisen tarkoituksena on muuttaa organisaation sisäisiä IP-osoitteita, jotta niitä ei voi ulkoisesti valvoa. (Brooks 2014, s. 126) Välityspalvelimet toimivat suodattamalla ja varastoimalla tiedostoja, joita verkossa siirretään. Niitä hyödyntävät palomuurit ovat sovellustason palomuureja, jotka eivät anna lähettää paketteja suoraan sovelluksesta käyttäjälle eikä toisinpäin. (Anwar et al. 2021)

Pilvipohjaisia palomuureja ovat virtuaaliset palomuurit (engl. Virtual Firewalls), seuraavan sukupolven palomuurit (engl. Next Generation Firewalls) sekä web-sovellustason palomuurit (engl. Web application firewalls). Virtuaaliset palomuurit ovat pääsääntöisesti ohjelmistoja, joten ne toimivat hyvin virtuaaliympäristöjen kuten julkisten ja yksityisten pilviympäristöjen suojaamisessa. Virtuaalisten palomuurien toimintaperiaate on samanlainen kuin laitteistopalomuurien eli ne myöntävät tai hylkäävät pääsyn verkkoon. (Anwar et al. 2021)

Seuraavan sukupolven palomuurit hyödyntävät perinteisiä palomuuriominaisuuksia verkon suojauskäytäntöjen valvomiseen, mutta niiden toiminta yhdistyy myös muihin verkkolaitteiden suojaustoimintoihin. Tällaisia suojaustoimintoja ovat esimerkiksi syväpakettitarkistusta (engl. Deep-packet Inspection) sekä tunkeutumisenestojärjestelmiä (engl. intrusion prevention system) hyödyntävät sovelluspalomuurit. Tällä palomuuriluokalla on myös muita ominaisuuksia, kuten verkkosivustojen suodatus-, virustentorjunta-, tietoliikenteen luokittelu ja priorisointi, sekä kaistanleveysanalyysiominaisuudet. Web-sovellustason palomuuri on erityisesti verkkoturvallisuutta varten kehitetty ja sillä on merkittävä rooli verkkopalvelimien ja verkkosovellusten sekä niihin liittyvien osien, kuten istunnonkäsittelyn ja evästeiden turvaamisessa. (Anwar et al. 2021)

Älykkäässä terveydenhuoltoympäristössä oikein valittu palomuuri ehkäisee tehokkaasti hyökkäyksen aiheuttamia vaikutuksia (Ranathunga et al. 2016). Haittaohjelmien lisäksi palomuurit suojaavat älykästä terveydenhuoltoa myös tietojenkalastelulta ja muilta kyberturvallisuusuhilta (Anwar et al. 2021)

4.4 Verkon valvonta ja salaus

Aiemmin on jo käynyt ilmi, että terveydenhuollon tietoverkko on monella tapaa poikkeuksellinen verrattuna muiden organisaatioiden tietoverkkoihin. Terveydenhuollon erityispiirteenä on monenlaiset hallittavat toimintaympäristöt. Terveydenhuolto sisältää toimistoverkon, lääkinnälliset laitteet sekä potilas- ja esimerkiksi laboratoriotietojärjestelmät. (Kakanakov 2012; Huoltovarmuuskeskus 2020) Terveydenhuollon tietoverkon on määritelty olevan lääketieteellisen tason tietoverkko (engl. Medical Grade Network, MGN). Tietojen johdonmukaisuuden, datan katoamisen, reaktioajan ja turvallisuuden herkkyys kuvaavat MGN: a, joka on erityislaatuinen organisaatioverkko. Skaalautuvuuden luotettavuuden ja turvallisuuden lisäksi MGN: n on oltava interaktiivinen ja joustavasti uudelleen konfiguroitavissa oleva kokonaisuus. MGN voi täyttää nämä vaatimukset, mikäli se tarjoaa helposti muokattavat ja älykkäät suojausratkaisut, joiden avulla voidaan kattaa niin väliaikaiset kuin pysyvätkin verkon käyttäjät. Tämän lisäksi MGN: n tulisi olla helposti laajennettavissa ja vastaavasti myös supistettavissa. (Kakanakov 2012)

Sen lisäksi, että terveydenhuolto-organisaation tietoverkkoa suojataan palomuurien ja segmentoinnin avulla, on pystyttävä turvaamaan myös sairaalaympäristön ulkopuolelle lähetetyt tiedot. Tähän tarkoitukseen käytetään salattua tietoverkkoa eli virtuaalista yksityisverkkoa (engl. Virtual Private Network, VPN) (Betuel et al. 2017; Arfaoui et al. 2018). Sen avulla on mahdollista taata luotettava ja turvallinen pääsy potilaan terveystietoihin myös etäyhteydellä. VPN on menetelmä, jonka toiminta perustuu salattujen, dynaamisten tunnelien luomiseen julkisten tietoverkkojen yli. VPN: n avulla voidaan muodostaa etäyhteys yksityiseen lähiverkkoon Internettiä tai muuta suojaamatonta julkista verkkoa käyttämällä lähettäen datapaketteja näitä salattuja tunneleita pitkin. (Betuel et al. 2017; Arfaoui et al. 2018) VPN: t ovat muiden verkkoyhteyksien tavoin kutenkin myös alttiita hyökkäyksille. Koska älykkäät terveydenhuollon laitteet sisältävät muun muassa sovellusrajoituksia, pyritään VPN-yhteys eri laitteiden välillä turvaamaan käyttäen mukautuvaa ja sopivinta mahdollista salaus- ja varmennusmenetelmää. Erityisesti nykyään, kun IoT-laitteet ovat yhä enemmän käytössä myös terveydenhuollossa mahdollistamassa potilaiden etämonitoroinnin, verkkoyhteydensalaus on keskeisessä asemassa. (Arfapui et al. 2018)

Verkon salaamisen lisäksi myös lähetettävää tietoa voidaan salata erilaisin salausmekanismein siten, että tietoja pystyy tarkastelemaan vain tietyn salausavaimen omaava taho (Brooks 2014, s. 76). Tietojen salaus ja siihen liittyvät ratkaisut (engl. encryption) on omanlainen, laaja kokonaisuus, jota Suomessa toteuttaa esimerkiksi tietoturvaratkaisuja toimittava SSH Communications Security Oyj. SSH käyttää ratkaisuissaan muun muassa AES (engl. Advanced Encryption Standard) salausmenetelmää, jonka on todettu olevan sopivin ja varmin ratkaisu erityisesti kriittisiä sovelluksia kuten terveydenhuollon sähköistä potilastietojärjestelmää salattaessa (Alharam & Elmedany 2017; Ylönen 1996).

Terveydenhuollossa kuten myös muunlaisissa organisaatioissa verkon valvonnasta huolehtii Security Operations Center, SOC (Demertzis et al. 2018; Tolonen 2022). Se on järjestäytynyt organisaation toiminto, jonka tekninen kyberturvallisuuden ammattitaito on keskitetty tiimiksi valvomaan, estämään ja analysoimaan kyberturvallisuushäiriöitä. SOC: in toiminta perustuu kykyyn analysoida ja käsitellä suuria tietovirtoja sekä kybertapahtumien yhteyksiä. (Demertzis et al. 2018)

5. YHTEENVETO

Kyberturvallisuudella tarkoitetaan kybertoimintaympäristöön liittyvää turvallisuutta. Se kattaa tietoliikenteen ja toiminnan niin internetissä kuin erilaisissa tietojärjestelmissäkin. Kyberturvallisuus muodostaa kokonaisuuden, johon kuuluu kyberuhkien havainnointi, tunnistaminen ja niihin varautuminen erilaisten toimenpiteiden avulla. Lisäksi kyberturvallisuuteen kuuluu uhista aiheutuvien vaikutusten ehkäisy. Haasteita kyberturvallisuuden ylläpitämisessä aiheuttavat kybertoimintaympäristön dynaamisuus ja siitä seuraava jatkuva muutos. Tämän seurauksena on selvää, että erilaisia teknisiä kyberturvallisuuskontrolleja on päivitettävä tiheästi ja päivityksistä huolimatta kyberturvallisuuden ratkaisut ovat aina askeleen jäljessä. Vaikka kybertoimintaympäristö on turvallisuuden kannalta haasteellinen kokonaisuus, kyberturvallisuuden tavoitteena on varmistaa kybertoimintaympäristössä liikkuvan sähköisen datan luottamuksellisuus, eheys ja saatavuus.

Kyberturvallisuus on vahvasti liitoksissa terveydenhuoltoon. Ihmisten henkilökohtaiset terveyteen liittyvät tiedot ovat arvokasta ja haluttua dataa verkkorikollisten keskuudessa. Terveydenhuolto sisältää laajan tietojärjestelmäkokonaisuuden ja älykkäiden lääkinnällisten laitteiden käyttö terveydenhuollossa lisääntyy. Tämän seurauksena hallittavat kokonaisuudet terveydenhuollon kyberarkkitehtuurissa muuttuvat ja kasvavat. Samalla myös kyberturvallisuuden merkitys lisääntyy, kun uudet järjestelmät, älykkäät IoT-laitteet ja niiden muodostamat etäyhteydet tuovat mukanaan lisää haavoittuvuuksia. Terveydenhuollossa merkittävimpiä kyberturvallisuuden uhkia kohdistuu lääkinnällisisiin laitteisiin, jotka nykyään yhä enemmän ovat integroituja verkkoon. Laitteenvalmistajien ja terveydenhuollon sovellusten tarjoajien onkin tärkeää huolehtia verkkointegraation kehittämisen lisäksi myös tuotteidensa kyberturvallisuudesta.

Teknisellä tasolla kyberturvallisuutta ylläpidetään terveydenhuollossa kuten muissakin organisaatioissa. Ratkaisuja kyberturvallisuuden ylläpitämiseen ovat muun muassa verkon segmentointi, salaus ja valvonta sekä laite- ja verkkopohjaiset palomuurit. Perinteisten palomuuriratkaisujen lisäksi myös pilvipohjaiset palomuurit ovat yleistymässä. Pilvipohjaisia palomuureja tarvitaan, sillä IoT-laitteet tallentavat tietoa pilvipalveluihin, jotka tarvitsevat omanlaisensa turvallisuusmenetelmät. Myös verkon segmentoinnin tärkeys korostuu älykkäiden lääkinnällisten laitteiden lisääntyessä. Näiden ratkaisujen lisäksi terveydenhuollossa hyödynnetään salattua VPN-yhteyttä, kun lähetetään dataa esimerkiksi terveydenhuolto-organisaatioiden välillä tai käytetään etähallittavaa lääkinnällistä laitetta. Tärkeä osa kyberturvallisuuden teknistä hallintaa ovat myös ammattilaisten tuotta-

mat SOC-palvelut. SOC vastaa organisaation verkon valvonnasta kyberturvallisuushäiriöiden varalta ja reagoi, kun häiriöitä ilmenee. Näillä edellä mainituilla kyberturvallisuuden ratkaisuilla voidaan tehokkaasti ehkäistä kyberhyökkäyksiä, kuten erilaisia haittaohjelmia, tietojenkalastelua ja palvelunestohyökkäyksiä. Ulkoisilta uhilta suojaavien teknisten ratkaisujen lisäksi Suomessa on käytössä muun muassa terveydenhuollon toimijoille tarkoitettuja toimikortteja ja varmenteita, joiden avulla voidaan varmistaa potilastietoihin pääsy vain valtuutetuilta henkilöiltä.

Erilaiset kyberhyökkäykset ovat lisääntyneet merkittävästi niin Suomessa kuin myös muualla maailmassa. Suomessa kyberturvallisuuden taso on niin yleisesti kuin myös terveydenhuollossa keskiarvon yläpuolella. Uusia kyberhyökkäyksiä ja -hyökkäysmenetelmiä kehitetään kuitenkin jatkuvasti, minkä takia kyberturvallisuuden merkitys tulee vain kasvamanaan tulevaisuudessa. Tämän takia Suomessa olisikin kohdistettava riittävästi resursseja kyberturvallisuuden kehittämiseen ja ylläpitämiseen.

Terveydenhuollon kyberturvallisuus on laaja kokonaisuus, joka muodostuu niin organisaation strategisen tason päätöksistä, yhteisten toimintatapojen luomisesta aina tekniseen toteutukseen asti. Työn tulosten pohjalta voidaan todeta, että terveydenhuolto-organisaatiossa on välttämätöntä toteuttaa kokonaisvaltaista kyberturvallisuutta yhteistyössä henkilöstön, toiminnallisten yksiköiden ja IT-ammattilaisten kanssa, jotta voidaan tulevaisuudessakin taata potilaiden turvallinen hoito ja yksityisyys.

LÄHTEET

Aceto, G., Persico, V., & Pescapé, A. (2020). Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0 [Article]. *Journal of Industrial Information Integration*, *18*, 100129. Saatavissa (viitattu 17.3.2022): https://doi.org/10.1016/j.jii.2020.100129

Ajijola, A., Zavarsky, P., & Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012. *2014 World Congress on Internet Security, WorldCIS 2014*, 66–73. https://doi.org/10.1109/WorldCIS.2014.7028169

Alharam, A. & Elmedany, W. (2017). The Effects of Cyber-Security on Healthcare Industry. *2017 9th IEEE-GCC Conference and Exhibition (GCCCE)*, 1–9. https://doi.org/10.1109/IEEEGCC.2017.8448206

Anwar, Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. *Applied Sciences*, *11*(19), 9183–. https://doi.org/10.3390/app11199183

Arfaoui, A., Kribeche, A., Senouci, S. M., & Hamdi, M. (2018). Game-Based Adaptive Remote Access VPN for IoT: Application to e-Health. *2018 IEEE Global Communications Conference, GLOBECOM 2018 - Proceedings*. https://doi.org/10.1109/GLOCOM.2018.8648064

Astala, Helena. (26.1.2022). Mediconsult. Saatavilla (viitattu 10.4.2022): https://www.mediconsult.fi/blogi/miten-yllapitaa-tietoturvaa-sosiaali-ja-terveydenhuollon-tietojarjestelmia-hyodyntavissa-organisaatioissa

Betuel, S., Machuve, D., & Kalegele, K. (2017). An experiment to analyze performance of virtual private network approach to information exchange between health facilities. *Applied Medical Informatics, 39*(1), 21-29. Retrieved from https://libproxy.tuni.fi/login?url=https://www.proquest.com/scholarly-journals/experiment-analyze-performance-virtual-private/docview/1926452915/se-2?accountid=14242

Brooks, Richard R. (2014). *Introduction to Computer and Network Security: Navigating Shades of Gray*. Chapman and Hall/CRC. https://doi.org/10.1201/b14801

Candia, Tanya. (7.7.2021). 5 Steps to Secure Internet of Medical Things Devices. HealthTech. Saatavilla (viitattu 11.5.2022): https://healthtechmagazine.net/article/2021/07/5-steps-secure-internet-medical-things-devices

Chen, Q. and Bridges, R. A. (2017). Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware. *16th IEEE International Conference on Machine Learning and Applications (ICMLA)*. pp. 454-460. doi: 10.1109/ICMLA.2017.0-119.

Choo, K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions [Article]. *Computers & Security*, *30*(8), 719–731. Saatavissa (viitattu 17.3.2022): https://doi.org/10.1016/j.cose.2011.08.004

Cybernet. (9.7.2020). How to build an effective healthcare network segmentation strategy. Saatavilla (viitattu 12.4.2022): https://www.cybernetman.com/blog/healthcare-network-segmentation-strategy/

Demertzis, K., Kikiras, P., Tziritas, N., Sanchez, S. L., & Iliadis, L. (2018). The next generation cognitive security operations center: Network flow forensics using cybersecurity intelligence. *Big Data and Cognitive Computing*, *2*(4), 1–17. https://doi.org/10.3390/bdcc2040035

Digi- ja väestövirasto. Varmenteet ja kortit sosiaali- ja terveydenhuollolle. Saatavissa (viitattu 14.3.2022): https://dvv.fi/varmenteet-sosiaali-ja-terveydenhuollolle#

Elinkeinoelämän tutkimuslaitos. (2020). Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? ETLA Muistio No 93. Saatavilla (viitattu 3.4.2022): https://www.etla.fi/julkaisut/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/

ENISA. (2016). Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures. ENISA:n raportti. Saatavilla (viitattu 5.4.2022): https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Frost and Sullivan. (2017). Internet of Medical things. Forecast to 2021, market report. Saatavilla (viitattu 28.3.2022): https://store.frost.com/internet-of-medical-things-forecast-to-2021.html

Grimes, S. T. (2016). Part 1 of 3: Best Practices for Medical Device Cybersecurity Management. CE-IT Collaboration Town Hall Series 23 - 24. Saatavissa (viitattu 21.3.2022): https://docplayer.net/35473652-Part-1-of-3-best-practices-for-medical-device-cybersecurity-management.html

Hearing Link. (Nettisivu tarkistettu: Huhtikuu 2021). Middle ear implants. Saatavilla (viitattu 2.4.2022): https://www.hearinglink.org/your-hearing/implants/middle-ear-implants/

Huoltovarmuuskeskus. (2020). Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot. Saatavilla (viitattu 2.4.2022): https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf

Hyppönen, Mikko. (2021). Internet. WSOY.

Limnéll, Jarno. (2014). Kyberturvallisuus (Klaus. Majewski & Mirva. Salminen, Eds.) [Book]. Docendo.

Integrating the Healthcare Enterprise. (2015). HE Patient Care Device (PCD) White Paper 10 Medical Equipment Management (MEM): Medical Device Cyber Security –Best Practice Guide. Saatavilla (viitattu 20.3.2022): http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf

IntelliPaat (updated 3.11.2021) Saatavissa (viitattu 9.3.2022): https://intellipaat.com/blog/the-cia-triad/

Kakanakov. (2012). Evaluating a Medical Grade Network through Network Calculus. *2012 Proceedings of the 35th International Convention MIPRO*, 715–720.

Kanta. (Päivitetty 29.10.2021) Tietosuoja ja -turva. Saatavissa (viitattu 14.3.2022): https://www.kanta.fi/omakanta-tietoturva

Karhunen, P. (2020). Improving Information Security in Healthcare Networks With Software-Defined Networking. Theseus. Saatavilla (viitattu 19.4.2022): https://www.theseus.fi/bitstream/handle/10024/340055/Thesis-master_L4833-KarhunenPetri.pdf?sequence=2&isAllowed=y

Kerkelä, Lasse. (7.4.2022). Rajavartiolaitos perustaa kyberyksikön torjumaan vihamielisiä hyökkäyksiä – Syynä ”yleinen turvallisuustilanne”. Helsingin Sanomat. Saatavilla (viitattu 11.5.2022): https://www.hs.fi/kotimaa/art-2000008733450.html

Klemm, D., & Johnson, D. (2010). *Committee on National Security Systems National Information Assurance (IA) Glossary*. Saatavissa (viitattu 15.3.2022): www.cnss.gov.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. In *Technology and Health Care* (Vol. 25, Issue 1, pp. 1–10). IOS Press. Saatavissa (viitattu 16.3.2022): https://doi.org/10.3233/THC-161263

Kumar Bhoi, Akash. (2021). *Hybrid Artificial Intelligence and IoT in Healthcare.* (P. Kumar. Mallick, Mihir. Narayana Mohanty, & V. H. C. de. Albuquerque, Eds.) [Book]. Springer Singapore Pte. Limited. Saatavilla (viitattu 18.3.2022): https://link.springer.com/content/pdf/10.1007%2F978-981-16-2972-3.pdf

Kyberturvallisuuskeskus. 2016. Liikenne- ja viestintävirasto. Saatavilla (viitattu 22.3.2022): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Terveydenhuoltoalan_kyberuhkia.pdf

Lehto, M., & Lehto, M. (2017). *KYBERTURVALLISUUS SAIRAALA-JÄRJESTELMISSÄ: OSA 1*. Jyväskylän Yliopisto. Saatavilla (viitattu 22.3.2022): https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/kyberturvallisuus-sairaalassa_-14-8-17.pdf

Lehto, M., Pöyhönen, J., & Lehto, M. (2019). *Kyberturvallisuus sosiaali- ja terveydenhuollossa*. Saatavilla (viitattu 20.3.2022): https://jyx.jyu.fi/bitstream/handle/123456789/63325/Kyberturvallisuus_Vol2FINAL.pdf?sequence=1&isAllowed=y

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. Saatavissa (viitattu 2.3.2022): https://doi.org/10.1007/s11948-017-9992-1

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

Mattila, J., Mäkäräinen, K., Pajarinen, M., Seppälä, T., Ali-Yrkkö, J. & Tervo, E. (2020). Digibarometri 2020: Kyberturvan tilannekuva Suomessa. Saatavilla (viitattu 17.5.2022): https://www.etla.fi/julkaisut/digibarometri-2020-kyberturvan-tilannekuva-suomessa/

MedicalDirector. (25.7.2018). Data & Security. What is a health software update and why do I need it? Saatavilla (viitattu 28.3.2022): https://www.medicaldirector.com/news/data-security/2018/07/what-is-a-health-software-update-and-why-do-i-need-it

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021, August 1). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*. MDPI AG. https://doi.org/10.3390/s21155119

Norri-Sederholm, T., Laitinen, T., Lehto, M., Kari, M. J., Maanpuolustuskorkeakoulu, J., & Ja, H.; (2019). Terveydenhuolto ja kyberuhkat. In FinJeHeW (Vol. 11, Issue 3). Saatavilla (viitattu 22.3.2022): https://doi.org/10.23996/fjhw.74183

Nuorten Lääkärien Yhdistys. (2020). Kyberosaaminen lääkärin arjen taitona. Saatavilla (viitattu 1.4.2022): https://www.nly.fi/kyberosaaminen-laakarin-arjen-taitona/

Obiora Nweke, L. (2017). *PM World Journal Using the CIA and AAA Models to explain Cybersecurity Activities www.pmworldjournal.net Commentary by Livinus Obiora Nweke Using the CIA and AAA Models to Explain Cybersecurity Activities: Vol. VI*. Saatavissa (viitattu 16.2. 2022): www.pmworldlibrary.net

Padallan, J. O. (2019). Cyber Security. Arcler Press. Saatavilla (viitattu: 23.2.2022): https://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,uid&db=e000xww&AN=2324327&site=ehost-live&scope=site

Paloalto Networks. (2020). 2020 Unit 42 IoT Threat Report. Saatavilla (viitattu 2.4.2022): https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Perakslis, Eric D. (2014). Cybersecurity in Health Care. *The New England Journal of Medicine*, *371*(5), 395–397. https://doi.org/10.1056/NEJMp1404358

Pöyhönen, J., Lehto, M., & Lehto, M. (2019). *Kyberturvallisuus sairaalajärjestelmissä: osa 2 Toiminnan kehittäminen*. Saatavilla (viitattu 20.2.2022): https://www.jyu.fi/it/fi/tutkimus/julkaisut/tekes-raportteja/kyberturvallisuus_sairaalajarjestelmissa_osa_2_toiminnan_kehittaminen.pdf

Rathore, Fu, C., Mohamed, A., Al-Ali, A., Du, X., Guizani, M., & Yu, Z. (2018). Multi-layer security scheme for implantable medical devices. *Neural Computing & Applications*, *32*(9), 4347–4360. Saatavilla (viitattu 28.3.2022): https://doi.org/10.1007/s00521-018-3819-0

Ranathunga, D., Roughan, M., Hung N., Kernick, P., & Falkner, N. (2016). Case Studies of SCADA Firewall Configurations and the Implications for Best Practices. *IEEE eTransactions on Network and Service Management*, *13*(4), 871–884. https://doi.org/10.1109/TNSM.2016.2597245

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 [Article]. *IEEE Access*, *7*, 168774–168797. https://doi.org/10.1109/ACCESS.2019.2950849

Rios, B. (2015). Cybersecurity expert: Medical devices have “a long way to go” [Article]. *Biomedical Instrumentation & Technology*, *49*(3), 197–200. Saatavilla (viitattu 18.3.2022): https://doi.org/10.2345/0899-8205-49.3.197

Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020, September 1). Cyber risk in health facilities: A systematic literature review. *Sustainability (Switzerland)*. MDPI. https://doi.org/10.3390/su12177002

Scarfone, K., Souppaya, M., & Hoffman, P. (2011). SP 800-125. Guide to Security for Full Virtualization Technologies. NIST. National Institute of Standards and Technology. Saatavilla (viitattu 18.4.2022): https://csrc.nist.gov/publications/detail/sp/800-125/final

Security Intelligence. (2020). IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain. Saatavilla (viitattu 3.4.2022): https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/

Somasundaram, R., & Thirugnanam, M. (2020). Review of security challenges in healthcare internet of things. *Wireless Networks*, *27*(8), 5503–5509. https://doi.org/10.1007/s11276-020-02340-0

Tolonen, Petri. (11.3.2022). Henkilöhaastattelu. Cyber Security Specialist.

Turvallisuus- ja kemikaalivirasto, Tukes. Saatavilla (viitattu 21.3.2022): https://tukes.fi/tietoa-tukesista/materiaalit/kemikaalit/laakinnalliset-laitteet-reach-ja-clp-asetuksessa#

Turvallisuuskomitea. (2018), Kyberturvallisuuden sanasto. Saatavissa (viitattu 9.2.2022): https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Valvira. Sosiaali- ja terveysalan lupa- ja valvontavirasto. (Päivitetty 8.2.2022). Potilaille annettavat terveydenhuollon etäpalvelut. Saatavilla (viitattu 3.4.2022): https://www.valvira.fi/terveydenhuolto/yksityisen_terveydenhuollon_luvat/potilaille-annettavat-terveydenhuollon-etapalvelut

Vertainen, Vesa. (2021). Ajankohtaiset kyberuhat terveydenhuollossa. Jamk, blogit. Saatavilla (viitattu 2.4.2022): https://blogit.jamk.fi/techtothefuture/2021/01/11/ajankohtaiset-kyberuhkat-terveydenhuollossa/

Vuorinen, Sari. (2019). Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille. Valtioneuvosto, Sosiaali- ja terveysministeriö. Saatavilla (viitattu 17.3.2022): http://urn.fi/URN:ISBN:978-952-00-4085-7

Williams, & 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

WithSecure™. (2022). Verkkosivu. Saatavilla (viitattu 26.4.2022): https://www.withsecure.com/fi/home

Wolf, D. Principal Security Researcher. (16.10.2019). Network segmentation is a security best practice, but is adoption lagging in healthcare? Forescout. Saatavilla (viitattu 19.4.2022): https://www.forescout.com/blog/network-segmentation-is-a-security-best-practice-but-is-adoption-lagging-in-healthcare/

Wu, F., & Eagles, S. (2016). Cybersecurity for Medical Device Manufacturers: Ensuring Safety and Functionality [Article]. *Biomedical Instrumentation & Technology*, *50*(1), 23–33. https://doi.org/10.2345/0899-8205-50.1.23
Yhteiskunnan turvallisuusstrategia. 2017 Valtioneuvoston periaatepäätös, Turvallisuuskomitea 2.11.2017. Saatavilla (viitattu 16.3.2022): https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

Yle. (13.5.2017). Cyber-attack ransomware detected in Finland. Saatavilla (viitattu 31.3.2022): https://yle.fi/news/3-9612110

Yle. (10.6.2017). Tyksin uusi kyberhyökkäys johtui harrastelijoiden muuntamasta viruksesta. Saatavilla (viitattu 31.3.2022): https://www.ts.fi/uutiset/3543514

Yle. (12.6.2019). Krp tutkii: Kyberhyökkäys Lahden verkkoon haittaa merkittävästi terveyspalveluita – sähköiset reseptit eivät toimi, verikokeissa ongelmia. Saatavilla (viitattu 31.3.2022): https://yle.fi/uutiset/3-10827423

Yle. (8.8.2019). Kyberhyökkäys on maksanut Lahden kaupungille lähes 690 000 euroa. Saatavilla (viitattu 31.3.2022): https://yle.fi/uutiset/3-10914550

Yle. (3.2.2020). Terveystalon verkkoajanvarauksesta kalasteltu henkilötietoja – järjestelmän haavoittuvuus oli tiedossa jo etukäteen. Saatavilla (viitattu 1.4.2022): https://yle.fi/uutiset/3-11189706

Yle. (25.10.2020, päivitetty 2.11.2020). Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa. Saatavilla (viitattu 1.4.2022): https://yle.fi/uutiset/3-11612399

Yle. (2022). Kyberturvallisuuteen liittyvät artikkelit aikaväliltä 1.1.2022-11.5.2022. Saatavilla (viitattu 11.5.2022): https://haku.yle.fi/?query=kyberturvallisuus&service=uutiset&time=custom&timeFrom=2022-01-01&timeTo=2022-05-11&type=article

Ylönen, Tatu. (1996). SSH - Secure Login Connections over the Internet.
Proceedings of the 6th USENIX Security Symposium, pp. 37-42, USENIX.