Informaatioteknologian tiedekunnan julkaisuja
No. 75/2019

Jouni Pöyhönen, Martti Lehto
ja Miikael Lehto

Kyberturvallisuus sairaalajärjestelmissä: osa 2
Toiminnan kehittäminen

JYVÄSKYLÄN YLIOPISTO

Informaatioteknologian tiedekunnan julkaisuja
No. 75/2019

Editor: Pekka Neittaanmäki
Covers: Petri Vähäkainu ja Matti Savonen

ISBN 978-951-39-7699-6 (verkkoj.)
ISSN 2323-5004
Jyväskylä 2019

Kyberturvallisuus sairaalajärjestelmissä: osa 2

TOIMINNAN KEHITTÄMINEN

Jouni Pöyhönen

Martti Lehto

Miikael Lehto

Tämä julkaisu on toteutettu osana WHC-hanketta, johon Jyväskylän yliopisto on saanut rahoituksen Business-Finlandilta.

Business Finland-hanke: WHC

TIIVISTELMÄ

Yleinen teknologian ja digitalisaation nopea kehittyminen näkyy myös terveydenhuollossa, jonka takia on mahdollista tuottaa esimerkiksi sairaalapalveluja uusilla tavoilla aiempaa laajemmin erityisesti tietoverkkoja hyödyntämällä. Kehitykseen liittyvät erityisesti sellaiset laitteet, jotka ovat osana tämän hetken teknologista älykkyyden kasvua. Kehityskulku on nähtävissä esimerkiksi esineiden internetin jatkuvana laajentumisena. Tulevaisuudessa lääkinnälliset laitteet ovat merkittävänä osana tätä IoT-laitteiden maailmanlaajuista käytön lisääntymistä, jossa kymmenet miljardit älykkäät laitteet ja sensorit kokoavat, välittävät ja hyödyntävät digitalisessa muodossa olevaa tietoa. Verkkojen ja niihin kytkeytyvien älykkäiden laitteiden muodostama kokonaisuus tietovarantoineen aiheuttaa toisaalta myös yleistä huolta niiden toiminnallisesta luotettavuudesta. Kyberturvallisuuden osalta siitä esimerkkinä ovat toimivat tilanteet, joissa esiintyy haavoittuvia laitteita ja ohjelmistosovelluksia osana hoidossa käytettävää verkottunutta toimintaympäristöä ja siten myös osana kyberfyysisiä järjestelmiä aiempaa laajemmin. Terveydenhuollossa haavoittuvuudet voivat johtaa vaaratilanteisiin, joilla on potentiaalinen vaikutus kliiniseen hoitoon ja potilasturvallisuuteen. Tämän huolen tulee koskea laajasti terveydenhuollon alueella eri toimijoita ja sidosryhmiä.

Viime vuosina terveydenhuolto on ollut erilaisten datamurtojen kohteena merkittävällä tavalla. Vuonna 2017 tietomurron kohteeksi joutui 5,5 miljoonaa potilastietoa. Tämän tutkimuksen tausta-aineistoksi tutkittiin pääosin vuosina 2013-2018 raportoituja kyberhyökkäyksiä. Niissä korostuvat tietojen kalastelumenetelmät, kiristysohjelmat, palveluestohyökkäykset, hakkeroinnit, virusohjelmat ja laitteiden sekä tallenteiden varkaudet tai katoamiset. Tapahtumat sijoittuvat organisaation kyberrakenteen eri kerroksille. Haitalliset tapahtumat voivat levitä rakenteessa laajalle organisaatioon eri verkkojen kautta ja siten löytää väyliä teknillisiin järjestelmiin tunkeutumiselle, joista on suora yhteys esimerkiksi kyber-fyysiseen vaikutukseen sairaalan toimintaprosesseissa.

Organisaatioiden strategisella tasolla yksi merkittävistä kybertoimintaympäristön uhkatrendeistä on eri tavoin koko organisaation toiminnan tuhoamiseen tähtäävät hyökkäykset. Hyökkääjät ovat tuhonneet kriittisien toimintaprosessien järjestelmiä, ovat julkaisseet luottamuksellista tietoa ja kiristäneet yrityksiä sekä ovat pilkanneet organisaatioiden johtoa.

Tulevaisuuden Teollisuus 4.0:n mukainen teknologian kehittyminen yhdessä tähän asti tapahtuneen digitalisaation kehityskulun kanssa mahdollistavat tulevaisuuden älykkäiden sairaaloiden suunnittelun ja toteutuksen. Älykkään sairaalan ratkaisut tulevat edelleen lisäämään haitantekijöille hyökkäysmahdollisuuksia ICT-rakenteisiin. Niihin liittyy myös organisaation oman henkilöstön ja muiden sidosryhmien toiminta yhä monimutkaistuvassa teknillisessä kokonaisuudessa. Fyysisiä hoitolaitteita ja muita toimintaan liittyviä teknillisiä laitteita on voitava tarkkailla jatkuvasti niin toiminnan kuin sijoittumisenkin osailta. Laitteista ja niiden liikuttelusta eri paikoissa on pidettävä

yhä parempaa huolta. Toiminnallisesti rakenteesta muodostuu näin ollen kompleksinen kokonaisuus, jolloin erityistä huomiota tulee kiinnittää sen kyberturvallisuuteen liittyviin ratkaisuihin.

Terveydenhuoltoalalla tietojenkäsittelyyn kohdistuu aivan erityisiä vaatimuksia. Potilastietojen eheys ja saatavuus ovat äärimmäisen tärkeitä potilaiden turvallisen hoidon kannalta. Toisaalta tietojen luottamuksellisuutta on suojattava paitsi yksityisyyden suojan takaamiseksi, myös henkilötietojen rikollisen käytön estämiseksi. Erityisen huomionarvoista on, että koko sairaalaympäristön toimivuus on kriittisen tärkeää potilaiden hoidolle. Tällöin tarkasteluun on otettava sairaalan koko internettiin kytkeytyvä digitaalinen järjestelmä- ja laiteympäristö.

Sairaalajärjestelmistä ja -laitteista sekä niiden käytöstä eri tarkoituksiin muodostuvan kokonaisuuden tarkasteluun soveltuu systeemiajattelun mukainen lähestyminen. Systeemiajattelu mahdollistaa monimutkaisten ja kompleksisten järjestelmien eri osien vaikutusten ymmärtämisen niistä muodostuvaan kokonaisuuteen ja sitä kautta organisaation toimintaprosesseihin. Sairaalan ICT-järjestelmät ovat kyberrakenteeltaan kompleksisia kokonaisuuksia tässä raportissa kuvatulla tavalla, jolloin niiden sujaustoimenpiteitäkin on suositeltavaa tarkastella systeemitasolta.

Tämä raportti ottaa huomioon sairaalan eri päätöksentekotasoilla tarvittavien kyberturvallisuustoimenpiteiden tarpeellisuuden, mutta keskittyy pääosin sairaalaympäristön teknillis-taktisen tason kyberturvallisuustilanteen selvittämiseen ja kehittämiseen. Raportissa selvitetään sairaalaympäristön kybertoimintaympäristön rakenne, analysoidaan käytännön tasolta kerättyjä tietoja sairaalaympäristön kyberhyökkäyksistä ja etsitään vastaaviin uhkiin varautumiseksi eri keinoja uusista teknologisista ratkaisuista mahdollisimman korkean tiedon luotettavuuden, käytettävyyden ja eheyden saavuttamiseksi.

Tutkimuksen tausta-aineistona toimivat raportoidut kyberhyökkäykset ovat tutkimuksessa sijoitettu sairaalan ICT-järjestelmien kyberrakenteeseen. Uhkat kohdistuvat rakenteen jokaiselle kerrokselle ja muodostavat siten laajan kirjon erilaisia hyökkäysvektoreita järjestelmiin. Perinteisesti niiltä suojaudutaan vyöhykkeittäin. Vyöhykesuojauksen lisäksi tässä tutkimuksessa suositellaan systeemitason ajattelua kyberhyökkäysten havaitsemiseksi sekä torjumiseksi ja siten sairaalan toimintaprosessien toiminnan jatkuvuuden hallintaan. Tutkimuksessa kuvattu kyberturvallisuuden arkkitehtuuri näkökulmineen ja sisältöineen sekä uudet teknologiat antanevat tähän myös hyödyntämismahdollisuuksia. Tällöin tuloksena tulisi olla kyberturvallinen sairaalaympäristön arkkitehtuurirakenne, jonka perusteella voidaan muodostaa mahdollisimman turvallinen tulevaisuuden toiminta-alusta sairaalajärjestelmille.

Raportissa hyödynnetään Jyväskylän yliopiston **Watson Health Cloud Finland** - tutkimushankkeen yhteydessä saatuja IBM:n kyberturvallisuusratkaisuja esimerkkinä tavoitteen saavuttamiseksi.

KUVIOT

TAULUKOT

SISÄLLYSLUETTELO

1 Johdanto

Tekniikan nopea kehittyminen perustuu digitalisaation aikaan saamaan ”kierteeseen”, jossa esimerkiksi erilaiset tuotantoprosessit automatisoituvat ja digitalisoituvat aiempaa laajemmin. Tämä kehityskulku on monissa yhteyksissä nimetty Teollisuus 4.0: ksi. Siihen liittyvät oleellisina osina kyberfyysiset järjestelmät (Cyber-physical system, CPS) ja Internet of Things (IoT) eli asioiden internet. Kyberfyysinen järjestelmä on järjestelmä, jossa verkon avulla yhteen liitetyt ohjelmistot kontrolloivat fyysisiä laitteita. Kyberfyysiset järjestelmät ovat ohjelmistoalustoja, jotka valvovat, ohjaavat ja suojaavat fyysisiä toimintaprosesseja. (Sadeghi, Wachsmann & Waidner, 2015, 1.)

Viimeisten kahden vuosikymmenen aikana tietotekniikkaa on käytetty laajalti lääketieteessä. Sähköisiä terveystietoja, biolääketieteen tietokantaa ja kansanterveyttä on parannettu paitsi tietojen saatavuuden ja jäljitettävyyden lisäksi myös niiden taloudellinen arvo on tiedostettu. Terveydenhuoltoon liittyvät tiedot ovat erittäin luottamuksellisia, joten niiden tietojenkäsittelyyn, tallennukseen ja käsittelyyn liittyy haasteita seuraavasti: (Zhang, Qiu, Tsai, Hassan & Alamri, 2017, 88.)

1. Datan kasvu: SOTE-alan digitalisaatio ja erityisesti sairaalatietojärjestelmien kehittäminen on lisännyt lääketieteellisten tietojen määrää. Lisäksi kannettavien terveys/hyvinvointilaitteiden käytön lisääntyminen on kasvattanut terveydenhuollon dataa.
2. Tiedonkäsittelyn nopeus: Useimmat lääketieteelliset laitteet, erityisesti kannettavat/puettavat laitteet, keräävät jatkuvasti tietoja. Nopeasti tuotetut tiedot on käsiteltävä välittömästi, jotta erityisesti hätätilanteessa vasteaika saadaan minimoiduksi.
3. Erilaiset tietorakenteet: Kliininen tutkimus, hoito, seuranta ja muut terveydenhuollon laitteet tuottavat monimutkaisia ja heterogeenisiä tietoja (esim. tekstiä, kuvaa, ääntä tai videota), jotka ovat joko rakenteellisia, osin rakenteellisia tai ei-rakenteellisia.
4. Arvonlisäys: Mikäli tietoa ei saada käyttöön, sen arvo on rajoitettu. Sähköisten potilastietojen (Electronic Health Record, EHR) ja sähköisten terveystietojen (Electronic Medical Record, EMR) yhdistämisen avulla voidaan tehostaa terveydenhuollon tietojen arvonlisäystä kuten henkilökohtaisessa terveydenhuollossa ja kansanterveydessä.

Yleinen teknologian ja digitalisaation nopea kehittyminen näkyy myös terveydenhuollossa, jonka johdosta on mahdollista tuottaa esimerkiksi sairaalapalveluja uusilla tavoilla aiempaa laajemmin erityisesti tietoverkkoja hyödyntämällä. Kehitykseen liittyvät erityisesti sellaiset laitteet, jotka ovat osana tämän hetken teknologista älykkyyden kasvua. Kehityskulku on nähtävissä esimerkiksi esineiden internetin jatkuvana laajentumisena. Tulevaisuudessa lääkinnälliset laitteet ovat merkittävänä osana tätä IoT-laitteiden maailmanlaajuista käytön lisääntymistä, jossa kymmenet miljardit älykkäät laitteet ja sensorit kokoavat, välittävät ja hyödyntävät digitalisessa muodossa olevaa tietoa. Verkkojen ja niihin kytkeytyvien älykkäiden laitteiden muodostama kokonaisuus tietovarantoineen aiheuttaa toisaalta myös yleistä huolta niiden toiminnallisesta luotettavuudesta.

Kyberturvallisuuden osalta siitä esimerkkinä toimivat tilanteet, joissa esiintyy haavoittuvia laitteita ja ohjelmistosovelluksia osana hoidossa käytettävää verkottunutta toimintaympäristöä ja siten myös osana kyberfyysisiä järjestelmiä aiempaa laajemmin. Terveydenhuollossa haavoittuvuudet voivat johtaa vaaratilanteisiin, joilla on potentiaalinen vaikutus kliiniseen hoitoon ja potilasturvallisuuteen. Tämän huolen tulee koskea laajasti terveydenhuollon alueella eri toimijoita ja sidosryhmiä.

Organisaatioiden strategisella tasolla yksi merkittävistä kybertoimintaympäristön uhkatrendeistä on eri tavoin koko organisaation toiminnan tuhoamiseen tähtäävät hyökkäykset. Hyökkääjät ovat tuhonneet kriittisien toimintaprosessien järjestelmiä, ovat julkaisseet luottamuksellista tietoa ja kiristäneet yrityksiä sekä ovat pilkanneet organisaatioiden johtoa. (FireEye, 2016, 47.) Hyökkäyksistä on voinut olla seurauksena jopa koko organisaation olemassaolon tai toiminnan vakava vaarantuminen, ja siksi nämä uhkat ovat huomioitava organisaation kaikilla päätöksentekotasolla.

Organisaatioiden toimintaprosessit, niin ydinprosessit kuin tukiprosessitkin, muodostavat niiden operatiivisen toiminnan perustan. Hyökkääjät etsivät niistä heikkouksia ja pyrkivät siten löytämään väyliä erityisesti teknillis-taktisen tason järjestelmiin tunkeutumiselle, joista on suora yhteys kyber-fyysiseen vaikutukseen. Toimintaa liittyy usein yksityiskohtainen prosessituntemus, mikä on hyökkääjän osalta avainasemassa sekä hyökkäyksen suunnittelussa, että sen toteutusmahdollisuuksien analysoinnissa. Yhteiseurooppalainen verkko- ja tietoturvasta vastaava organisaatio ENISA (European Union Agency for Network and Information Security, ENISA) pitää raportissaan ”Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends” erityisen tärkeänä tunnistaa organisaation operatiivisella päätöksentekotasolla toimintaprosesseihin kohdistuvat uhkakuvat. (ENISA, 2016, 15.)

IBM Security on raportissaan ”IBM X-Force Threat Intelligence Index 2017” selvittänyt eri toimialojen joutumista kyberhyökkäysten kohteeksi vuonna 2016. Raportin mukaan terveystoimiala on yksi merkittävimmistä kyberhyökkäysten kohteista. Vuonna 2016 yli 100 miljoonaa potilastietoa varastettiin. (IBM Security, 2017, 12.)

Rikolliset ovat kiinnostuneita potilastiedoista, koska niistä maksetaan pimeillä markkinoilla hyvin; tyypillinen potilastieto sisältää luottokorttinumeroita, sähköpostiosoitteita, sairasvakuutusnumeroita, työnantajatietoja sekä sairaushistoriatietoja. Näillä on rikollisille arvoa, koska ne yleensä ovat voimassa vuosia. Kyberrikolliset käyttävät tietoja tietojenkalasteluhyökkäyksissä, petoksissa sekä identiteettivarkauksissa (Lehto, Limnéll, Innola, Pöyhönen, Rusi & Salminen, 2017, 18.).

Terveydenhuoltoalalla tietojenkäsittelyyn kohdistuu aivan erityisiä vaatimuksia. Potilastietojen eheys ja saatavuus ovat äärimmäisen tärkeitä potilaiden turvallisen hoidon kannalta. Toisaalta tietojen luottamuksellisuutta on suojattava paitsi yksityisyyden suojan takaamiseksi, myös henkilötietojen rikollisen käytön estämiseksi. Erityisen huomionarvoista on, että koko

sairaalaympäristön toimivuus on kriittisen tärkeää potilaiden hoidolle. Tällöin tarkasteluun on otettava sairaalan koko internettiin kytkeytyvä digitaalinen järjestelmä- ja laiteympäristö. Esimerkkinä tarkastelun laajuudesta toimii sairaalarakennusten kiinteistöautomaation kyberturvallisuuden tärkeä asema kokonaisuudessa. Viestintävirasto kartoitti keväällä 2015 suomalaisista internetiin kytketyistä verkoista suojaamattomia automaatiolaitteita. Kiinteistöautomaatioon liittyviä suojaamattomia laitteita löytyi tuhansia ja on todennäköistä, että osa niistä on terveydenhuollon organisaatioiden käytössä olevissa kiinteistöissä. (Halonen, 2016, 19 - 23.)

Tämä raportti ottaa huomioon sairaalan eri päätöksentekotasoilla tarvittavien kyberturvallisuustoimenpiteiden tarpeellisuuden, mutta keskittyy pääosin sairaalaympäristön teknillis-taktisen tason kyberturvallisuustilanteen selvittämiseen ja kehittämiseen. Raportissa selvitetään sairaalaympäristön kybertoimintaympäristön rakenne, analysoidaan käytännön tasolta kerättyjä tietoja sairaalaympäristön kyberhyökkäyksistä ja etsitään vastaaviin uhkiin varautumiseksi eri keinoja uusista teknologisista ratkaisuista mahdollisimman korkean tiedon luotettavuuden, käytettävyyden ja eheyden saavuttamiseksi.

Tällöin tuloksena tulisi olla kyberturvallinen sairaalaympäristön arkkitehtuurirakenne, jonka perusteella voidaan muodostaa mahdollisimman turvallinen tulevaisuuden toiminta-alusta sairaalajärjestelmille. Raportin loppuosassa sairaalajärjestelmien suojausta lähestytään systeemiajattelun kautta rakentuvien turvallisuusratkaisujen aikaansaamiseksi. Raportissa hyödynnetään Jyväskylän yliopiston **Watson Health Cloud Finland** - tutkimushankkeen yhteydessä saatuja IBM:n kyberturvallisuusratkaisuja esimerkkinä tavoitteen saavuttamiseksi.

2 Sairaala kybertoimintaympäristönä

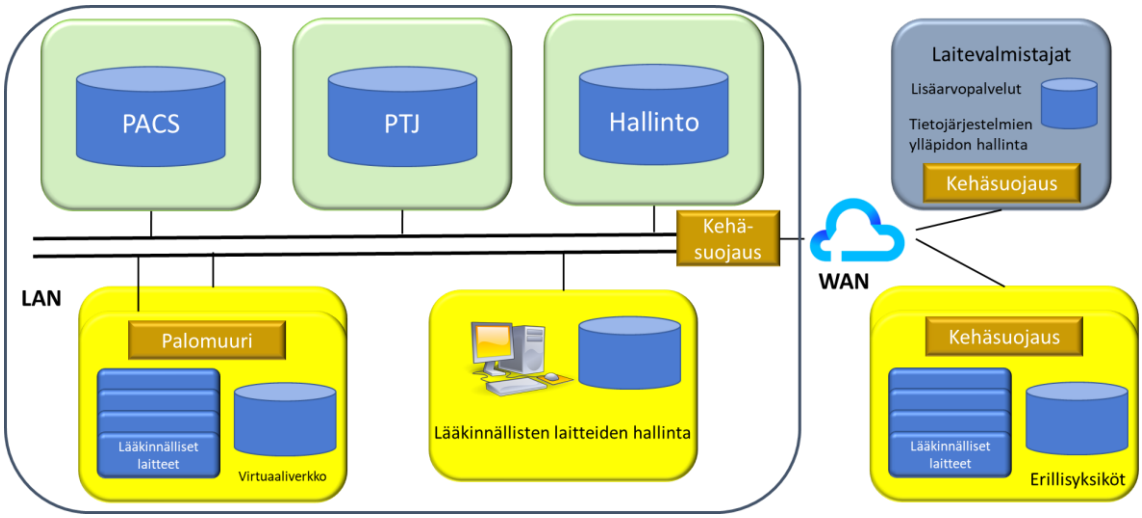
2.1 Sairaalan tietojärjestelmät ja laitteet

2.1.1 Yleistä sairaalajärjestelmistä ja -laitteista

Sairaalaympäristön toimivuus edellyttää useiden erilaisten tietojärjestelmä- ja automaatiojärjestelmäkokonaisuuksien hyödyntämistä. Niitä voidaan tunnistaa tarvittavaksi ainakin neljän eri prosessin alueella. Järjestelmät yleisellä tasolla ovat:

1. Hallinnon tietojärjestelmät
2. Sairaalan tietojärjestelmäkokonaisuus
3. Kiinteistön automaatiojärjestelmä
4. Turvajärjestelmä (kulunvalvonta)

Tämä tutkimus käsittää edellä mainituista sairaalan tietojärjestelmäkokonaisuuden. Muita järjestelmiä sivutaan niiltä osin, kuin ne ovat suoranaisesti vaikuttaneet sairaalan tietojärjestelmäkokonaisuuden toimintaan tutkimukseen liittyvien tietojen perusteella. Kuviossa 1 on esitetty geneerinen rakenne sairaalan tietojärjestelmästä.



KUVIO 1. Geneerinen sairaalan tietojärjestelmäkokonaisuus (Integrating the Healthcare Enterprise, 2015, 21)

Terveydenhuollon tietojärjestelmistä keskeisimpiä ovat potilastietojärjestelmät. Potilastietojärjestelmien ydinjärjestelmiä käytetään sairaaloissa laajasti. Ydinjärjestelmiä ovat muun muassa lähetteiden käsittely- ja ajanvarausjärjestelmät sekä hoitotietojen kirjausjärjestelmät. Niiden avulla hoidetaan sairaalaan saapuvien potilaslähetteiden kirjaus ja käsittelyn potilaan valvonta, ajanvaraukset toimenpiteisiin ja lääkäreiden vastaanotoille, potilaan sisäänkirjoittaminen tai ilmoittautuminen sekä tehtyjen hoitotoimenpiteiden ja diagnoositietojen kirjaaminen. Edellä mainittujen tietojen lisäksi potilastietojärjestelmiin tallennetaan yhä enemmän potilaan hoidollisia

tietoja kuten hoitoon tulon syy, hoidon tavoitteet, tehdyt toimenpiteet ja tutkimukset, erilaiset lausunnot, suunnitelmat, hoito-ohjeet, hoitopalautteet ja epikriisit (hoitotiivistelmät). Potilastietojärjestelmästä tuotetaan myös tarvittavat raportit, tilastot, kustannus- ja laskutustiedot. Potilastietojärjestelmät voidaan jakaa lähes kaikissa yksiköissä käytettäviin ja edellä kuvattuihin operatiivisiin ydinjärjestelmiin sekä niitä täydentäviin yksikkökohtaisiin erillisjärjestelmiin. (Integrating the Healthcare Enterprise. 2015, 11.)

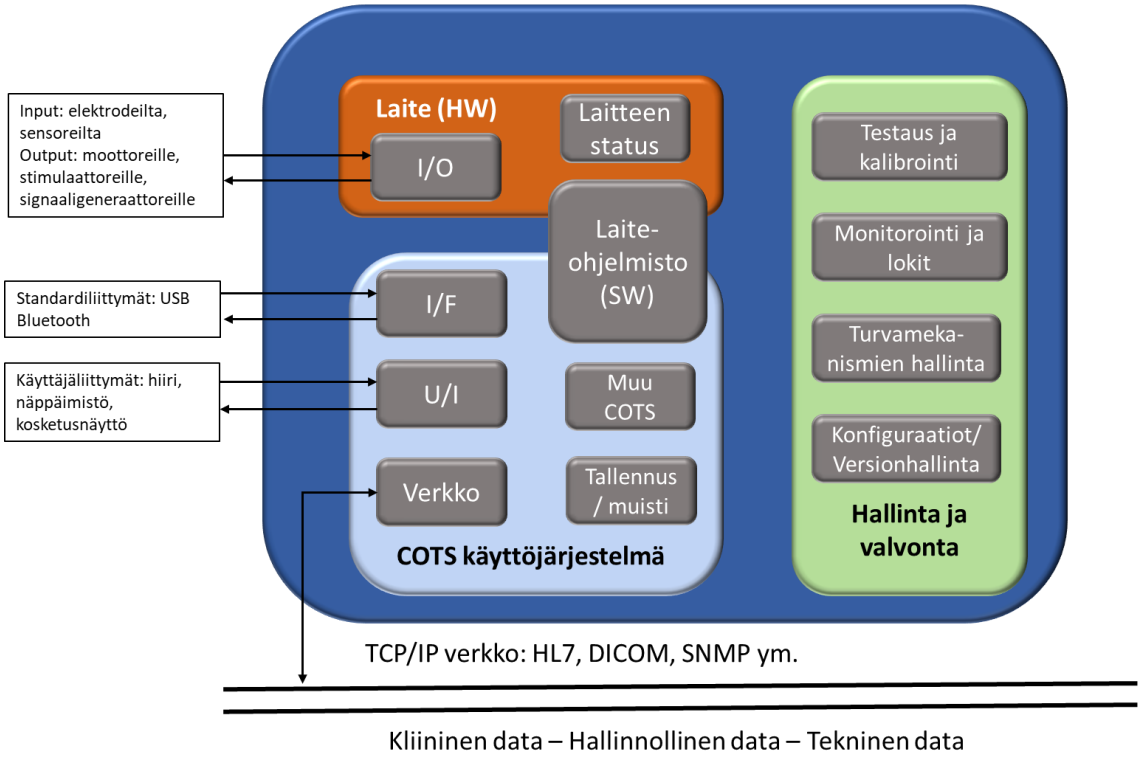
Yksikkökohtaiset erillisjärjestelmät keräävät potilaan hoitoketjun aikaiset tutkimus- ja toimenpidetiedot. Erillisjärjestelmistä keskeisimpiä ovat laboratoriojärjestelmät, joiden kautta tilataan tarvittavat tutkimukset, niihin syötetään tutkimustulokset ja hoidetaan tulosten välitys niitä pyytävään yksikköön. Muita erillisjärjestelmiä ovat mm:

- Röntgenosastojen työnohjausjärjestelmät eli RIS- tietojärjestelmät (Radiology Information System)
- Digitaalisen kuvan arkistointi PACS-järjestelmät (Picture Archiving Communications Systems)
- Muun digitaalisen kuvantamisen järjestelmät
- Anestesia- ja tehohoidon tietojärjestelmät
- Synnytysosastojen tietojärjestelmät
- Erilaisten tutkimusosastojen tarpeisiin kehitetyt järjestelmät

Järjestelmien sisältämien lääkinnällisten laitteiden tyyppikirjossa on ollut eksponentiaalista kasvua, joka on seurausta yleisestä älykkäiden laitteiden kehityksestä. Niihin lukeutuvat myös muun muassa matkapuhelimet, tablettitietokoneet ja erilaiset puettavat laitteet, joihin liittyy lääkinnällisiä sovelluksia/ohjelmistoja. Tällaisia laitteita on jo löydettävissä kodeista.

Kuviossa 2 on esitetty geneerinen malli lääkinnällisten laitteiden arkkitehtuurista ja keskeisistä komponenteista kyberturvallisuuden näkökulmasta.

Liitteessä 1 on ote WHO:n listauksesta lääkinnällisistä laitteista.



KUVIO 2. Geneerinen lääkinnällisten laitteiden arkkitehtuuri (Integrating the Healthcare Enterprise, 2015, 16)

Sairaalaympäristössä käytettäviä yleisiä laitteita yhdistävät verkkoyhteystyypit voidaan kuvata käyttötarkoituksineen seuraavasti (Grimes, 2016, 11):

- Langallisen tai langattoman verkon kautta yhteys elektronisiin potilastietoihin
- Yhteys kuva-/tallennusvarastoon (esim. PACS - kuvantumisjärjestelmä)
- Etäyhteys tietoihin/kuviin (esim. lääkäri)
- Etäpalvelu (esim. valmistajan päivitykset, vianetsintä, korjaus)
- Etähallinta (esim. kliiniset päivityksiä kuten lääkekirjastot infuusiopumpuille)
- Etäohjaus (esim. muuttaa hälytyksiä, asetuksia, hoidon määrää)
- Lääkinnällisten laitteiden välinen sisäinen viestintä (esim. diagnoosilaite "informoi" terapeuttisia laitteita ja valvoo lääkkeiden annostelua).

2.1.2 Sairaalajärjestelmiin ja -laitteisiin liittyviä kyberturvallisuusnäkymiä

Lääkinnällisten laitteiden turvallisuusriski on se, että ne voivat mahdollisesti altistaa sekä laitteeseen liittyvän datan, että itse laitteen hallinnan joutumisen ulkopuolisen haltuun. Tämä uhkakuva herättää luonnollisesti tarkastelutarvetta potilasturvallisuuden ja tietoturvallisuuden välillä. Siksi uhkakuva edellyttää jatkossa yhä tiiviimpää sidosryhmäyhteistyötä erityisesti järjestelmä-/laitesuunnittelun ja sääntelyn osalta. Sidosryhmäyhteistyöhön liittyvät sääntelyviranomaiset, laitevalmistajat, terveydenhuollon organisaatiot, IT-toimittajat ja potilaat. (Grimes, 2016, 18.)

Sairaalalaitteisiin liittyvät turvallisuusriskit heijastuvat myös järjestelmätasolle. Kyberturvallisuuden kannalta sairaala käsittää kriittisten järjestelmien kokonaisuuden, jotka sisältävät sekä toiminnallisia riskejä että erilaisia haavoittuvuuksia erityisesti laitehaavoittuvuuksien kautta, ja joihin siten kohdistuu myös kyberuhkia. Kuopion yliopistollisen sairaalan tietohallintojohtaja on nimennyt sairaalansa toiminnan osalta kriittisiksi järjestelmiksi seuraavat järjestelmät. (Pekkarinen, 2016, 9 - 10.):

- Potilastietojärjestelmät
- Laboratoriojärjestelmät
- Patologian järjestelmät
- Tehohoidon järjestelmät
- Veritilausjärjestelmät
- Anestesiatietojärjestelmät
- Leikkaustoiminnan ohjaus
- Tiedonvälitysrajapinta
- Kuvantamisen järjestelmät
- Synnytysosaston tietojärjestelmät
- Hoitajakutsujärjestelmät
- Keskusvalvontajärjestelmät
- Toiminnanohjausjärjestelmät
- Turvallisuusjärjestelmät

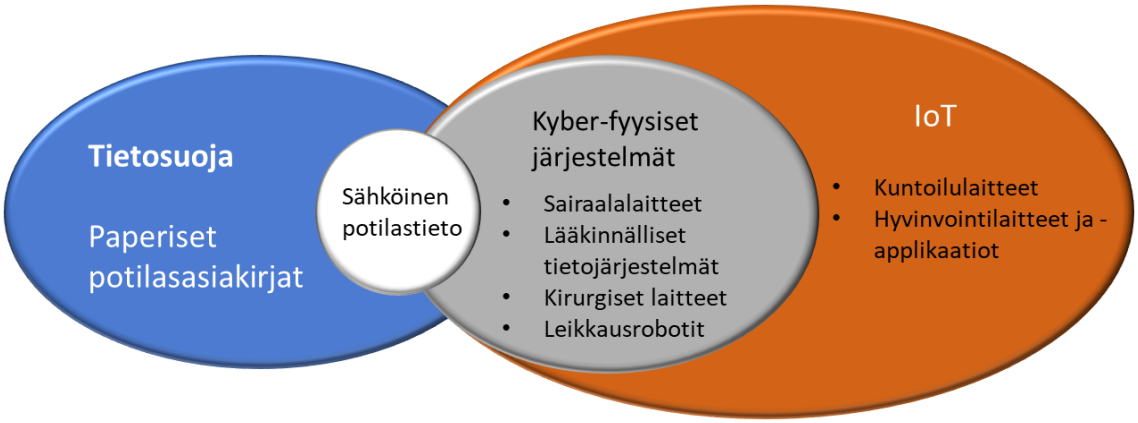
Kyberturvallisuuteen liittyvien riskien määrä kasvaa entisestään, kun terveydenhuollon organisaatiot ja kuluttajat omaksuvat käyttöönsä esineiden internetin (IoT) aiempaa laajemmin. Laitteiden verkottuminen, laskentateknologian ja eri ohjelmistojen kehityskulku on mahdollistanut sairaalan järjestelmien, kliinisen tekniikan ja eri toimijoiden entistä laajemman integroinnin etäyhteyksien kautta. Kehityskulkua ovat erityisesti mullistaneet pilvipalvelujen kehittyminen ja data-analytiikan käyttö. (Piggin, 2017, 5.)

Informaatioteknologian ja kliiniseen toimintaan liittyvät tekniikkasiilot ovat yhdistyneet verkottumisen kautta edellä kuvatun kehityksen seurauksena. Kehityskulku vaikuttaa myös kyberturvallisuusajatteluun. Asiaan liittyy haasteita erityisesti sidosryhmäviestinnän osalta, käytössä vielä olevien vanhojen teknologioiden osalta, sekä eriasteisten tietoturvahaavoittuvuuksien ja riittämättömien laitteiden hallintamenettelyjen osilta. Lisäksi lääkinnällisten laitteiden suunnittelu on keskittynyt potilaiden välittömän turvallisuuden suojelemiseksi, mutta se ei ole riittävästi huomioinut kyberturvallisuutta alan innovatiivisesta kehyksestä huolimatta. Itse asiassa eriasteisten teknologioiden järjestelmätasoinen integroituminen luo uusia hyökkäyspolkuja ja siten myös kyberturvallisuusriskejä. Uusia teknologioita otetaan käyttöön ja vanhoja lääkinnällisiä laitteita käytetään edelleen samaan aikaan. Vanhoissa laitteissa ei ole huomioitu tietoturvavaatimuksia ja lisäksi laitteita usein myös hallinnoidaan puutteellisesti. Lisääntynyt laitteiden yhdistettävyys ja langattomat teknologiat luovat

edelleen uusia mahdollisuuksia palvelun tarjoamiseen, etävalvontaan ja diagnostiikkaan, mutta voivat myös aiheuttaa odottamattomia seurauksia kyberturvallisuuden osalta. (Piggin, 2017, 19.)

Kyberturvallisuuteen liittyvät uhkatekijät, kuten kyberhyökkäykset edellä mainittua infrastruktuuria vastaan, ovatkin merkittävästi lisääntyneet. Lääkinnällisten laitteiden kyberturvallisuudesta onkin tullut ensisijainen terveydenhuollon turvallisuushuoli useiden potentiaalisesti haitta-asteeltaan vakavien tapahtumien jälkeen. Huoli on oikeutettu, sillä esimerkiksi kehittyneellä haittaohjelmalla saastuneella laitteella on mahdollisuus huonoimmassa tapauksessa sulkea sairaalan toiminnot, paljastaa arkoja potilastietoja, vaarantaa muiden kokonaisuuteen liitettyjen laitteiden toiminta ja vahingoittaa potilaita. Terveydenhuollon uudet lähestymistavat kasvavien kyberturvallisuuden uhkien torjumiseksi pitävät sisällään suosituksia siitä, että kaikki osapuolet toimisivat yhteistyössä tunnistaakseen ja arvioidakseen kyberturvallisuusuhkia sekä hallinnoidakseen niihin liittyviä riskejä. Tämä edellyttää monipuolisia suunnitelmia toiminnasta ja varautumisesta potilasturvallisuuden ja tietoturvallisuuden varmistamiseksi. (Piggin, 2017, 19 - 20.)

Kyberturvallisuusuhkien torjunnassa on yhä tärkeämpää tunnistaa digitalisaatiokehitys, joka tuo sairaalaympäristöönkin aiempaa laajemmin kyberfyysiset järjestelmät ja asioiden internetin laitteineen. Tämä muuttuva näkymä on esitetty kuviossa 3. (Piggin, 2017, 3.)



KUVIO 3. Terveydenhuollon toimintaympäristö (Piggin, 2017, 3)

Terveydenhuollon kyberturvallisuusympäristön kehityksen huomioiminen ja siihen liittyvien uhkatekijöiden tunnistaminen on tekniikan nopean kehityksen takia jatkossa yhä tärkeämpää. Jo tämänhetkisestä uhkien torjunnan tarpeellisuudesta antaa hyvän kuvan liiketoiminnan konsultointiyrityksen KPMG:n vuoden 2015 kyberturvallisuustutkimus. Kyselyssä 81% terveydenhuollon organisaatioihin oli hyökätty kahden viime vuoden aikana ja vain puolet niistä olivat riittävästi varautuneita hyökkäyksiin. Potilastietojen arvo pimeillä markkinoilla oli hyökkäysten tärkein motivaatio. Lisäksi myöhemmin esiintyneet tiedostojen käyttöä estävät kiristyshaittaohjelmat ovat lisääntyneet. Niissä rikolliset pyrkivät salaamaan kohteen tietoja ja sitten vaativat maksua digitaalisen valuutan avulla tietojen palauttamiseksi (ml. potilastiedot). Kohteina ovat olleet myös sairaalat useissa maissa, kuten Yhdysvalloissa, Isossa-Britanniassa ja Australiassa. (Piggin, 2017, 4 - 5.)

Valitettavasti huono kyberturvallisuus voi vaikuttaa potilaan terveyteen ja altistaa potilastietoja uhkatekijöille. Eriasteisten teknologioiden järjestelmätasoinen integroituminen, mobiiliteknologiat sekä sidosryhmien monimuotoisuus ovat lisänneet kyberturvallisuutta uhkaavia riskiä. Lääkinnällisten laitteiden kanssa toimivat yritykset ja terveydenhuollon eri organisaatiot kohtaavat jatkuvasti kyberhyökkäyksiä, joihin lukeutuvat sekä kohdistamattomat että yhä kehittyneemmät kohdistetut hyökkäykset. (Piggin, 2017, 4 - 5.)

Hyökkäyksistä aiheutuviin uhkiin lukeutuvat (Piggin, 2017, 5):

- Hoidon tai palvelun häiriöt (mahdollistaen vaikka potilaan kuolemantapaukset).
- Henkilöstön harhauttaminen huijaussähköpostilla tai väärennetyillä verkkosivustoilla kirjautumistunnusten hankkimiseksi tai haittaohjelmien asentamiseksi.
- Tahaton tai tarkoituksellinen "sisäpiiriläisen uhka", joka voi aiheuttaa merkittävän uhan koska heillä on luottamuksellinen asema organisaatiossa.
- Potilastietojen menetys - erityisesti elektroniset turvatut terveystiedot.
- Tietomurto, tietojen vuotaminen ja arvon menetys.
- Kiristys; kiristystä ja pakottamista arkaluonteisia vuotaneita tietoja hyödyntämällä.
- Immateriaalioikeuksien varastaminen.

Tutkimuksissa on osoitettu, että terveydenhuollon kyberturvallisuus painottuu edelleen potilastietojen suojaamiseen, mutta potilaiden terveyteen kohdistuviin todellisiin kyberturvallisuuden uhkiin ei puututa tarpeeksi. Ison-Britannian kansallinen tietosuojaorganisaatio antoikin äskettäin suosituksia uusista tietoturvastandardeista ja toimintapuitteista. Suositukset eivät kuitenkaan käsitelleet edelleenkään potilasturvallisuutta eikä lääkinnällisiä laitteita. (Piggin, 2017, 5.)

2.1.3 Sairaalaympäristö kyberhyökkäyskohteena

Ketkä ovat terveydenhuollon vihollisia ja mitkä ovat heidän motivaationsa? Uhat tulevat useista eri lähteistä kuten vihamielisyydestä, luonnollista syistä (mm. järjestelmän monimutkaisuudesta, inhimillisistä virheistä, tapaturmista tai laitehäiriöistä) sekä luonnonkatastrofeista. Uhkatekijöiksi tunnistettavilla hyökkäyskohteen vihollisryhmillä tai yksilöillä on erilaisia kykyjä, motiiveja ja resursseja, joita on lueteltu ohessa seuraavasti (Piggin, 2017, 6):

- Hyökkääjät (joihin kuuluvat myös 'haktivistit') ryhtyvät hyökkäyksiin jännityksen hakemiseksi, haasteen vuoksi tai aatteen puolesta. Hyökkäyksiä mahdollistavat työkalut ovat aiempaa kehittyneempiä, helppokäyttöisempiä ja vapaasti saatavissa, mikä on johtanut vähemmän teknistä taitoa omaavien henkilöiden tekemien hyökkäyksien lisääntymiseen.
- Bottiverkko-operaattorit ottavat tyypillisesti useita järjestelmiä haltuunsa suorittamaan hyökkäyksiä ja lähettämään tietojenkalasteluviestejä, haittaohjelmia ja roskaposteja.

Palveluja voidaan sittemmin myydä palvelunestohyökkäyksiin tai roskapostin ja tietojenkalastelun välittämiseen.

- Rikollisryhmät/järjestäytynyt rikollisuus hyökkää järjestelmiin rahallisen edun saamiseksi hyödyntäen roskaposteja, tietojenkalastelua, vakoiluohjelmia tai haittaohjelmia, joiden avulla he voivat tehdä identiteettivarkauksia ja verkkopetoksia. Teollisuusvakoilu, kiristyshaittaohjelmat ja uhkaaminen kyberhyökkäyksillä ovat potentiaalisia uhkia. Tiedot pääsystä tunkeuduttuun järjestelmään voidaan myydä kolmansien osapuolten rikollisille.
- Ulkomaiset tiedusteluviranomaiset käyttävät kybertyökaluja tiedusteluun, vakoiluun ja erilaisten vaikutusten luomiseen kuten sabotaasin. Valtiollisilla toimijoilla on hyökkäyskyvykkyyksiä, joita tuetaan aikomuksella laajentaa sodankäyntiä kybermaailmaan. He voivat pyrkiä hyödyntämään terveydenhuoltojärjestelmiä henkilötietojen saamiseksi ja heidän toimintansa voi jopa vahingoittaa potilaita.
- Sisäpiiriläiset työntekijät tai esimerkiksi tavarantoimittajat, joilla on rajoittamaton tai vähemmän rajoitettu pääsy järjestelmiin, ja he voivat joko tyytymättöminä tai tahattomasti tuoda haittaohjelmia tai ei-toivottuja muutoksia järjestelmiin.
- Tietojenkalastelijat yksilöitä tai ryhmiä, jotka käyttävät tietojenkalastelua varastamaan identiteettejä ja tietoja rahallista hyötyä varten.
- Roskapostin lähettäjät lähettävät ei-toivottuja sähköposteja, jotka mahdollisesti sisältävät piilotettuja tai vääriä tietoja, suorittavat tietojenkalasteluja tai palvelunestohyökkäyksiä.
- Vakoiluohjelmien tai haittaohjelmien tekijät tuottavat ja jakavat haittaohjelmia ilkeämielisiin tarkoituksiin tai rahallisen hyödyn saamiseksi.
- Terroristit pyrkivät häiritsemään, tuhoamaan tai hyödyntämään kriittistä infrastruktuuria voidakseen uhata kansallista turvallisuutta. Terroristit saattavat käyttää vakoilu- tai haittaohjelmia tai tietojenkalastelua toiminnan rahoittamiseen.
- Teollisuusvakoojat pyrkivät saamaan immateriaalioikeuksia ja tietämystä salakavalien menetelmien avulla. Yleisessä tiedossa on, että jotkut valtiot ja heidän valtuuttamansa toimijat ovat hyvin aktiivisina.

Eräänä merkittävimmistä sairaalajärjestelmien ja -laitteiden kyberturvallisuuden riskitekijöistä on pidettävä puutteellisesti testattuja laitepäivityksiä. Niistä aiheutuvia uhkia voivat hyödyntää niin sisäpiiriläiset kuin ulkopuoliset toimijatkin. Uhat voivat realisoitua myös digitaaliseen toimintaympäristöön liittyvistä luonnollisista tapahtumista. Niistä kaikista aiheutuvat tapahtumat voidaan luokitella passiiviksi tai aktiivisiksi. Passiiviset uhat käsittävät tiedon keräämisen tai verkossa liikkuvan tiedon sieppauksen työkaluja hyödyntämällä. Esimerkkinä toiminnasta on salasanojen kalastaminen. Aktiiviset uhat tulevat monissa muodoissa ja niihin sisältyy (Piggin, 2017, 6 - 7):

- Viestintä: verkko-/laiteviestinnän häiriöt.
- Tietokantainjektio: käytetään tietoihin tai järjestelmiin pääsemiseen ja tietojen varastamiseen.
- Toisto: tietojen toistaminen, jotta päästäisiin järjestelmiin tai tietojen väärennykseen.
- Väärentäminen tai jäljittely: laitteistolle tai ohjelmistolle tuleva kommunikaatio voi tulla muualta kuin alkuperäislähteestä.

- Sosiaalinen manipulointi: pyrkimys saada tietoa henkilöiltä harhauttamalla, jota voidaan käyttää tietokoneisiin, laitteisiin tai verkkoihin hyökätessä.
- Tietojenkalastelu: sosiaalisen manipuloinnin muoto, jossa käytetään väärennettyjä sähköposteja tai verkkosivustoja houkuttelemaan uhri paljastamaan tietoja.
- Väärennetty koodi: useita tarkoituksia, kuten kerätä tietoja, tuhota tietoja, tarjota keino päästä järjestelmään, väärentää järjestelmän tietoja tai raportteja tai aiheuttaa aikaa vievää ärsytystä käyttäjille ja ylläpidolle.
- Palvelunestohyökkäys (DDoS): vaikuttaa verkkojen ja tietojenkäsittelyresurssien saatavuuteen niitä huonontamalla (esim. käyttöjärjestelmät, kiintolevyt ja sovellukset).
- Käyttöoikeuksien eskalointi: tekniikka hyökkäyksen tehokkuuden lisäämiseksi saavuttamalla etuoikeutettu pääsy sellaisten toimien toteuttamiseen, jotka muuten olisivat estettyinä.
- Fyysinen tuhoaminen: hyökkäykset, joiden tarkoituksena on tuhota tai heikentää fyysisiä laitteita tai osia. Nämä voivat olla suoraan tai epäsuorasti kyberhyökkäyksen kautta fyysisiä vahinkoja aiheuttavia toimia (kuten Stuxnet-haittaohjelmia).

Kyberturvallisuuden attribuutit (luotettavuus, saatavuus, eheys) lääketieteellisissä järjestelmissä eroavat toisistaan niiden käyttötarkoituksen suhteen. Tiedon luottamuksellisuuden varmistaminen on sairaalajärjestelmien ensisijainen tavoite, kun tarkoitetaan tietomurtojen tai kiristyshaittaohjelmien aiheuttamien uhkilta suojautumista. Tiedon saatavuuden varmistaminen on etusijalla, kun potilaat tarvitsevat lääkinnällisiä laitteita osana hoitoa, mukaan lukien implantoitavat laitteet. "Ei-lääketieteellisillä" tai hyvinvointilaitteilla, kuten aktiivisuusrannekkeilla, on myös tiedon luottamuksellisuus etusijalla, vaikkakin niillä on pienempi vaikutus terveydenhuollossa kyberturvallisuuteen kuin edellä mainituissa tapauksissa. (Piggin, 2017, 12)

Kuten aiemmin on todettu, sairaaloiden keskeinen ongelma on henkilökohtaisia terveyttä koskevien tietojen houkuttelevuus ja merkitys rikolliselle toiminnalle. Näiden arkaluontoisten tietojen saatavuuden lisäksi hyökkääjät voivat myös päästä käsiksi esimerkiksi tietoihin reseptilääkkeistä. Kyberturvallisuustoimenpiteiden onkin oltava sairaaloissa kattavia tai muuten hyökkääjät yksinkertaisesti hyödyntävät puutteellisista suojaustoimenpiteistä aiheutuvia mahdollisuuksia. Hyökkääjä voi hyödyntää tilaisuutta haittaohjelmiensa avulla tunkeutumalla järjestelmiin tai laitteisiin niiden haavoittuvuuksien kautta. Useimmat haavoittuvuudet voivat myös lisätä ihmisten aiheuttamien tahallisten tai tahattomien toimintavirheiden todennäköisyyttä ja vaikutusta sekä järjestelmä tai laitevikoja. Vakavia ja vaikeasti hallittavia haavoittuvuuksia aiheutuu erityisesti käytettäessä esineiden internetin laitteita verkon aktiivisina osina. IoT-ratkaisuissa laitteiden komponentit valitaan vielä turhan usein kustannuslähtöisesti eikä näin ollen huomioida niihin liittyviä turvallisuuden vaatimia erillisominaisuuksia. Näin muodostuvan puutteellisen kyberturvallisuuden takia aiheutuvat turvallisuuskustannukset (mm. potilasturvallisuuteen ja tietoturvallisuuteen kohdistuvat) voivat olla merkittäviä niihin käytettävien mahdollisimman turvallisten komponenttien kustannusten rinnalla. (ENISA, 2016, 6 - 7.)

Verkottuneisiin sairaalajärjestelmiin ja lääkinnällisiin laitteisiin liittyvät kyberturvallisuuden merkittävimmät riskit voidaan koota luetteloksi seuraavasti: (The Deloitte Center for Health Solutions, 2013, 1 - 2.)

- Sähkömagneettinen häirintä.
- Testaamaton tai viallinen ohjelma ja laiteohjelmisto.
- Verkottuneiden lääkinnällisten laitteiden varkaus tai häviäminen (ulkoiset tai kannettavat).
- Turvallisuus ja yksityisyyden haavoittuvuudet
    - väärin määritellyt verkot tai huonot turvallisuuskäytännöt
    - valmistajien tietoturvapäivitysten ja korjaustiedostojen asennuksien laiminlyönti lääkinnällisiin laitteisiin ja huolenaiheet palvelun häiriöiden aiheutumisesta toimiville laitteille
    - potilastietojen tai datan virheellinen hävittäminen, mukaan lukien testitulokset tai terveystiedot
    - salasanojen hallitsematon jakaminen, kuten työntekijän huolimattomuus, kun jätetään salasana näkyville valvomattomaan paikkaan, salasanojen ottaminen pois käytöstä tai ennalta asennetut salasanoja ohjelmistoihin, jotka on tarkoitettu rajoitettuun pääsyyn lääkinnällisiin laitteisiin (esim. hallinnointiin, tekniselle tuelle ja huoltopalvelulle)
    - manipulaatio, varkaus, tuhoaminen, valtuuttamaton julkistaminen tai potilaiden tietojen saatavuuden puute tarjoajille.
- Luvaton laitteen asetusten muuttaminen, uudelleenohjelmointi tai tartunta haittaohjelmien avulla.
- Palvelunestohyökkäykset
- Hyökkäykset mobiiliterveydenhuollon laitteisiin, jotka hyödyntävät langattomia teknologioita pääsyyn potilastietoihin, niiden valvontajärjestelmiin ja istutettuihin lääkinnällisiin laitteisiin.

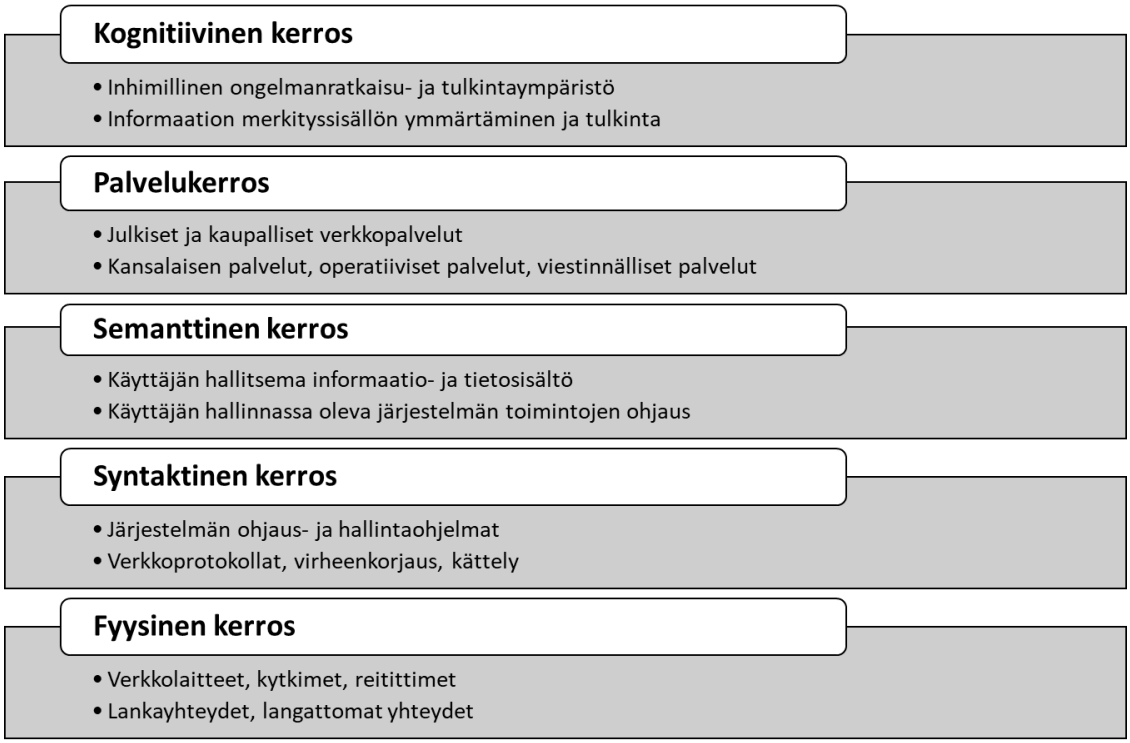
2.2 Sairaalaympäristön tietojärjestelmien kyberrakennemalli

Sosiaali- ja terveydenhuollon organisaatiokohtaisia tietojärjestelmiä ovat sairaalan tietojärjestelmät, perusterveydenhuollon tietojärjestelmät, laboratorion, erillisyksikköjen tietojärjestelmät (esimerkiksi radiologia) sekä sosiaalitoimen tietojärjestelmät. Näiden lisäksi sairaalaorganisaatiot käyttävät hallinnon tietojärjestelmiä (muun muassa talous- ja henkilöstöhallinto), asianhallinnan tietojärjestelmät (muun muassa tekstinkäsittely ja taulukkolaskenta), viestintäjärjestelmät (muun muassa sähköposti, hoitajakutsujärjestelmät), toiminnanohjausjärjestelmät, turvallisuusjärjestelmät (muun muassa kulunvalvonta, kameravalvonta, keskusvalvomo, äänievakuointi). Jotkut osat sairaalan järjestelmistä ovat sulautettuja järjestelmiä ja laitteita, joihin on ”upotettu” toimintaa ohjaavaa elektroniikkaa ja ohjelmistoa. (Saranto & Korpela, 1999, 296 - 297; Paloniemi, 2008, 10 - 11; Pekkarinen, 2016, 10.)

Martin C. Libicki on luonut kybermaailmaan rakenteen, jonka idea perustuu OSI-malliin (Open Systems Interconnection Reference Model) (Libicki, 2007, 89). OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. Kukin kerroksista käyttää alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs. OSI-malliin pohjautuvasta Libickin kybermaailman mallista on muokattu viisikerroksinen hierarkkinen rakennemalli, jossa kerroksina ovat fyysinen, syntaktinen, semanttinen, palvelut ja kognitiivinen. Mallia voidaan käyttää sairaalaympäristössä seuraavasti (Lehto, 2015, 21):

1. Fyysiseen kerrokseen kuuluvat tiedonsiirtoverkon fyysiset osat, kuten palvelimet, verkkolaitteet, kytkimet, reitittimet sekä kiinteät että langattomat yhteydet.
2. Syntaktinen kerros muodostuu erilaisista järjestelmien ohjaus- ja hallintaohjelmista, liityntäteknologioista sekä toiminnoista, joilla verkkoon kytketyt laitteet ovat vuorovaikutuksessa keskenään, kuten verkkoprotokollat, virheenkorjaus, kättely jne.
3. Semanttiseen kerrokseen kuuluu käyttäjien eri järjestelmissä oleva informaatio ja tietosisällöt sekä erilaiset käyttäjän hallinnassa olevien toimintojen ohjaus.
4. Palvelukerros sisältää sairaalan erilaiset hallinnolliset ja kliiniset palvelukokonaisuudet.
5. Kognitiivinen kerros kuvaa sairaalan päätöksentekijän ja toimijan informaation ongelmanratkaisu- ja tulkintaympäristöä, maailmaa, jossa informaatiota tulkitaan ja muodostetaan henkilökohtainen tilanneymmärrys.

Kuviossa 4 on esitetty kybertoimintaympäristön hierarkkinen rakennemalli.



KUVIO 4. Kybertoimintaympäristön hierarkkinen rakennemalli (Lehto, 2015, 21)

Kybertoimintaympäristön hierarkkista rakennemallia voidaan havainnollistaa oheisella käytännönläheisellä esimerkillä, jossa ihmisen identiteettiin kohdistuvat eri tekijät jakaantuvat rakennemallin kerroksille. (Sartonen, Huhtinen & Lehto, 2016, 1.) Esimerkki perustuu tosiseikkaan, jonka mukaan tämän päivän digitaalinen maailma on luonut ihmiselle erilaisia digitaalisia ja virtuaalisia identiteettejä. Digitaalinen maailma voidaan tällöin jakaa edellä kuvattuun viiteen kerrokseen, jotka ovat fyysinen-, syntaktinen-, semanttinen-, palvelu- ja kognitiivinen kerros. Näissä eri kerroksissa ihmisen digitaalinen identiteetti ilmenee eri tavoin. Fyysisessä kerroksessa ovat ihmisen digitaaliset päätelaitteet, kuten älypuhelin tai tietokone. Syntaktisessa kerroksessa käyttäjä ilmentyy IP-osoitteina, sähköpostiosoitteina, käyttäjätunnuksina ja useina virtuaali-identiteetteinä, joiden perusteella ihminen voidaan liittää tiettyyn fyysiseen laitteeseen tai käyttämäänsä palveluun. Semanttisessa kerroksessa sijaitsee meidän henkilökohtainen datamme ja informaatiomme, jotka voivat olla digitaalisia kuva-, teksti- ja äänitiedostoja. Palvelukerroksessa olemme jäseninä erilaisissa sosiaalisen median palveluiden verkostoissa, kuten Facebook- tai Twitter-ryhmissä, ystäväryhmissä, blogiverkostoissa jne. Virtuaalisen identiteettimme avulla voimme muodostaa erilaisia verkostoja, joissa toimimme kuhunkin verkostoon valitsemallamme identiteetillä. Kognitiivisessa kerroksessa ilmennymme inhimillisinä olentoina, joihin voidaan vaikuttaa kognitiivisin ja psykologisin menetelmin. Kognitiivisella tasolla ihmisellä on tietämiseen ja ymmärtämiseen liittyvää ajattelua, johon liittyvät sekä emootiot että rationaalisuus sekä kyky tehdä havaintoja ja päätöksiä.

Nämä digitaalisen maailman kerrokset muodostavat kokonaisuuden, jossa jokaisessa kerroksessa vaikuttavat omat sääntönsä ja lainalaisuutensa. Noustessa fyysisestä kerroksesta ylöspäin abstraktiotaso kasvaa ja ilmentymät laajentuvat. Näihin identiteetteihin liittyy yksityisyys, joka tarkoittaa luonnollisen henkilön oikeutta suojautua ulkopuoliselta puuttumiselta. Se tarkoittaa erityisesti kyberturvallisuuteen liittyvien riskien tunnistamista rakenteessa kerroksittain, jolloin lopputuloksena on järjestelmätasoinen tarkastelu. Viisikerroksista rakennemallia voidaan siten pitää järjestelmätason kuvauksena ja siten systeemikäsitteen viitekehyksenä organisaation digitaalisia rakenteita tarkastellessa.

3 Kyberhyökkäyksiä sairaalajärjestelmiin

3.1 Terveydenhuollossa todettuja kyberuhkia

Vuosi 2015 oli merkityksellinen terveydenhuollolle datamurtojen suhteen. Noin 300:sta Yhdysvaltain Office for Civil Rights (OCR) ilmoitetusta tapauksesta, 95 oli IT-järjestelmiin kohdistuneita hakkerointeja, ja 125 tapausta aiheutui luvattomasta pääsystä tai paljastumisesta. 58 tapauksessa kyse oli varastetuista laitteista tai tallenteista, lisäksi oli 16 häviämistapausta, ja seitsemän tapausta tietojen vääränlaisesta hävittämisestä. (Snell, 2016b.)

Haittaohjelmat leviävät etupäässä murrettujen verkkosivustojen ja verkkomainosten, sähköpostin ja sosiaalisen median välityksellä. Pelkkä vierailu sivustolla, jolle hyökkääjä on onnistunut ujuttamaan haittakoodia, voi saada haittaohjelman asentumaan vierailijan tietokoneelle. Työntekijän tietokoneelta haittaohjelma voi levitä edelleen muualle organisaation verkkoon. (Halonen, 2016, 26.)

Kun terveydenhuollon organisaatio joutuu kyberhyökkäyksen kohteeksi, sen vaikutukset ovat laaja-alaiset ja vaikutuksiltaan merkittävät. Ne ulottuvat:

1. Potilaiden turvallisuuteen
2. IT-ohjelmistojen saatavuuteen, joka voi estää potilaiden hoidon
3. Potilaiden ja työntekijöiden tietojen yksityisyyteen ja turvallisuuteen
4. Sairaalan maineeseen
5. Sairaalan talouteen

Yhdysvaltain FDA (Food and Drug Administration) on analysoinut kyberturvallisuushaavoittuvuuksia ja tapauksia, jotka voivat vaikuttaa suoraan lääkintälaitteisiin tai sairaalan verkon toimintaan. Analysoinnissa on tunnistettu seuraavat haavoittuvuusalueet:

- Verkkoon kytketyt/konfiguroidut lääkintälaitteet haittaohjelmien saastuttamina tai lamauttamina.
- Haittaohjelmat sairaaloiden tietokoneissa, älypuhelimissa ja tableteissa, kohdistuen mobiililaitteisiin käyttäen langattomia teknologioita päästäkseen käsiksi potilastietoihin, monitorointijärjestelmiin, ja implantoituihin potilaslaitteisiin.
- Kontrolloimaton salasanojen jakaminen, heikkojen salasanojen käyttö, (esim. hallinto-, tekninen-, tai huoltohenkilökunta).
- Turvallisuusohjelmistopäivityksien ja -paikkauksien epäonnistunut jakelu lääkintälaitteille ja tietoverkoille, sekä vanhojen lääkintälaitemallien (legacy) haavoittuvuuksien hoitamattomuus.
- Turvallisuushaavoittuvuudet suoraan kaupan hyllyiltä saatavissa ohjelmistoissa, jotka on suunniteltu suojaamaan luvaton laitteeseen tai verkkoon pääsy, mukaan lukien

selkokieliset tai vahvasti koodatut salasanat tai todennuksen puuttuminen, huoltomanuaalin dokumentoidut huoltotunnukset, tai heikko koodaus/SQL-injektio.

Terveydenhuolto on toimialana kiinnostava kyberhyökkäyksiä tekeville yksittäisille ihmisille tai organisaatioille muun muassa sen sensitiivisen tietosisällön vuoksi. Terveydenhuollon kyberturvallisuuden jatkuva parantaminen ja tietoisuuden lisääminen palvelee kaikkien kansalaisten etuja. Kyberturvallisuuden parantaminen vaatii vahvaa ymmärrystä tietoturvasta ja sekä terveydenhuollon toimintatavoista. Terveydenhuollon suurimmat kyberuhat liittyvät sairaalan lääketieteellisiin laitteisiin. Muita merkittäviä uhkia ovat muun muassa järjestelmien ja laitteiden ohjelmistojen haavoittuvuudet, niiden käyttötavat ja salasanakäytänteet, etähallittavat laitteet ja mobiililaitteet. (Halonen, 2016, 7.)

3.1.1 Lääketieteelliset laitteet ja niiden etähallinta

Lääketieteelliset laitteet ovat nykyään lähes poikkeuksetta verkkoon yhdistettäviä laitteita. Juuri tästä muodostuukin digitalisaation etu, jonka avulla tietoa voidaan hyödyntää koko organisaatiossa. Laitekanta tulee lisääntymään lähivuosina merkittävästi erityisesti siksi, että terveydenhuoltoa tuodaan koteihin aiempaa enemmän ja laitekanta lisääntyy niissä. Kodista on tulossa hyvää vauhtia sairaalan jatke. Se aiheuttaa suuria haasteita laitteiden, ohjelmistojen ja verkon toimivuudelle ja käytölle sekä siten myös koko alueen kyberturvallisuudelle.

Organisaatiotasolla lääketieteellisten laitteiden kyberturvan tasoa on aiemmin laskenut muun muassa se, että laitehankinta ja -hallinta on tehty organisaatioissa usein ohi tietohallinto-organisaation. Tietohallinto-organisaatiossa on kuitenkin yleensä paras tieto kyberturvallisuudesta ja heillä on myös yleensä päävastuu organisaation kyberturvallisuuspolitiikan jalkauttamisesta ja ylläpitämisessä. Kyberturvallisuus pitää nähdä tärkeänä osan potilaiden hoidon laatua. Määräys lääkintälaitteiden turvallisuudesta on vuodelta 2004 (Lääkelaitoksen julkaisusarja 1/2004) ja silloin ei ollut vielä näköpiirissä etäkäytettävien ja -hallittavien laitteiden markkinoille tulemisen suurta määrää.

Nykyään laitteiden ohjelmistotasoja päivitetään lähes poikkeuksetta etänä. Tämä tarkoittaa sitä, että laitteistotoimittajien kyberturvallisuuspolitiikka ja -käytänteet tulee auditoida myös, jotta varmistetaan kyberturvallisempi ympäristö.

3.1.2 Ohjelmistojen haavoittuvuudet

Missä tahansa ohjelmistossa voi olla virheitä, jotka altistavat ohjelman ja tiedon tietoturvaloukkauksille. Tällöin puhutaan haavoittuvuuksista, jotka saattavat mahdollistaa haittaohjelmien levityksen, pääsyn käsiksi salassa pidettäviin tietoihin tai vaikkapa ohjelmiston toiminnan estämisen. Ohjelmistohaavoittuvuuden hyväksikäyttö voi olla osa varsinaista haittaohjelman levittämis- tai aktivoitumismekanismia. Lisäksi alemman tason oikeuksilla aktivoitunut haittaohjelma voi hyväksikäyttää paikallista ohjelmistohaavoittuvuutta korkeamman

tason oikeuksien saamiseen. Tyypillisiä sähköpostin kautta leviävien haittaohjelmien hyväksikäyttämiä haavoittuvuuksia ovat sellaiset sähköpostiohjelmistojen tai selainten haavoittuvuudet, jotka mahdollistavat haittaohjelman aktivoitumisen ilman liitetiedoston avaamista. Hyvin tunnettuja ovat virukset, jotka ohjelmistohaavoittuvuutta hyväksikäyttämällä aktivoituvat jo sähköpostin esikatselutilassa. Lisäksi sähköpostin liitetiedostoina leviävät virukset voivat hyväksikäyttää lähes kaikkia liitetiedoston käsittelyyn käytettyjen sovellusohjelmistojen haavoittuvuuksia. Tällöin olennaista on pyrkiä hallitsemaan haavoittuvuuksia. Käytännössä organisaation on järjestettävä turvapäivityksien aktiivinen seuranta työasemissa ja palvelimissa, sekä ohjeistettava toimenpiteet löydettäessä haavoittuvuus. (Valtiovarainministeriö, 2009.)

3.1.3 Mobiililaitteet

Mobiililaitteita käytetään yhä useammin myös terveydenhuollossa. Laitteita voidaan käyttää missä vaan, jolloin ei olla välttämättä rakenteellisesti suojatussa tilassa. Laite voi myös jäädä ajoittain ilman valvontaa, jolloin riski sen joutumisesta varastetuksi kasvaa. Lisäksi kyberturvallisuus ei ole mobiililaitteissa niin hyvällä tasolla kuin perinteisissä tietokoneissa. Sairaalajärjestelmiin liittyvien mobiililaitteiden tulee kuulua tietohallinnon hallintaan, kuten kaikkien muidenkin tietoteknisten laitteiden ja ohjelmistojen. Mobiililaitteiden käyttöä kriittisissä toiminnoissa tulee harkita erityisesti siksi, että niiden tiedonsiirto ja puhe ovat riippuvaisia matkapuhelinverkoista.

3.1.4 Järjestelmien käyttötavat ja salasanakäytänteet

Merkittävänä kyberuhkana voidaan pitää myös henkilökunnan järjestelmien käyttötapoja ja salasanakäytänteitä. Käyttäjät voivat toimia kyberturvallisuuspolitiikan vastaisesti asettaessaan yhteiskäyttösalasanoja tai estääkseen vaikkapa aikalukituksen päälle menoa laitteessa. Tiedon jakamista ja kyberturvallisuuden merkityksen korostamista ei voi tehdä liikaa. Se on tuotava organisaation kulttuuriin ja työntekijöille sitä on painotettava säännöllisesti. Käyttäjät ovat helpoin kohde tietojen kalasteluun rikollisiin tarkoituksiin. (Siwicki, 2016.)

3.2 Sairaala hyökkäyskohteena

Kyberturvallisuudessa uhka, haavoittuvuus ja riski muodostavat toisiinsa liittyvän kokonaisuuden. Lähtökohtana on jokin arvoa sisältävä fyysinen esine, tieto, osaaminen tai muu immateriaalinen oikeus, joka halutaan suojata ja turvata. Uhka (threat) on jokin haitallinen kybermaailman tapahtuma, joka saattaa tapahtua. Uhan numeerinen arvo on todennäköisyys. Haavoittuvuus (vulnerability) on järjestelmässä oleva heikkous, joka lisää tapahtuman todennäköisyyttä tai kasvattaa sen aiheuttamia vahinkoja. Haavoittuvuus voidaan jakaa ihmisten toiminnassa (human factor), prosesseissa tai teknologiassa ilmentyviin haavoittuvuuksiin. Riski (risk) on vahingon odotusarvo. Se saadaan kertomalla tapahtuman todennäköisyys vahingon arvioidulla suuruudella.

3.2.1 Kyberhyökkäykset ja -tekniikat

ENISA käyttää oheisen taulukon 1 kyberuhkamallia, joka muodostuu hyökkäysmenetelmistä ja -tekniikoista, haittaohjelmista ja fyysisen maailman uhkista (ENISA, 2012,13 - 15):

TAULUKKO 1. Kyberhyökkäysmenetelmiä ja tekniikoita

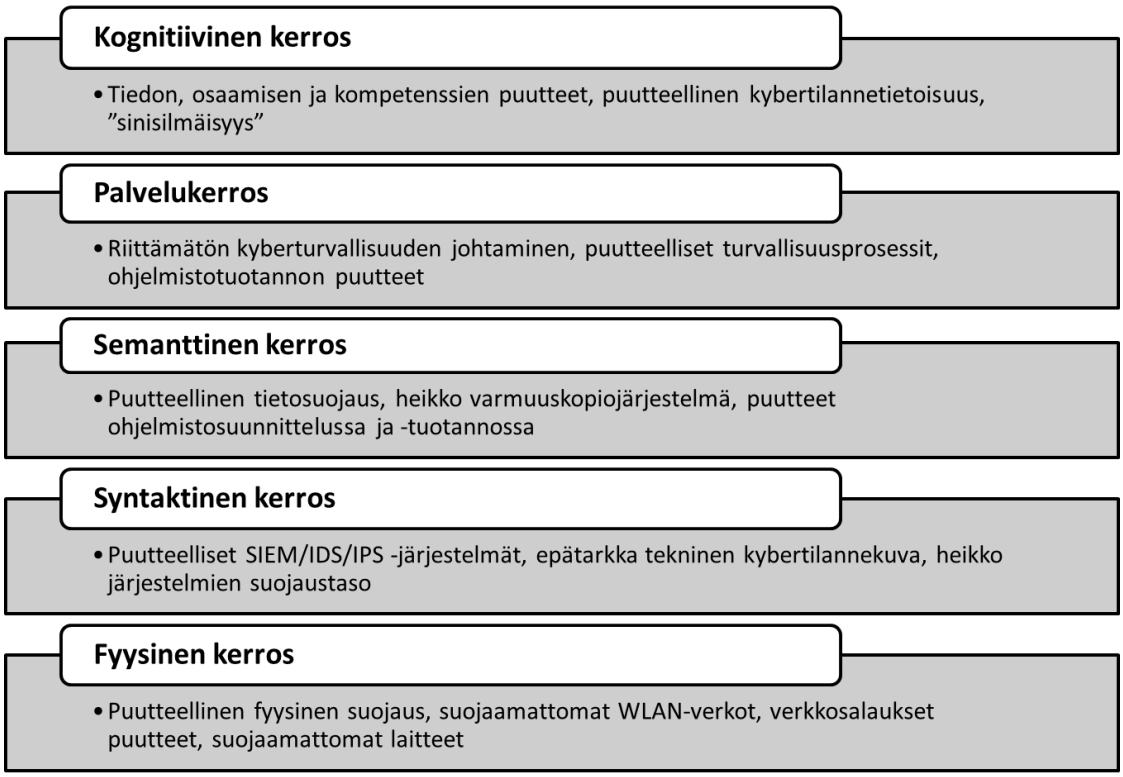
Kyberhyökkäykset ja tekniikat	Haittaohjelmat	Fyysiset uhat
• Drive-by Exploits • Code Injection Attacks • Botnets • Denial of service • Phishing • Compromising confidential information • Targeted Attacks • Identity Theft • Abuse of Information Leakage • Search Engine Poisoning	• Exploit Kits • Worms/Trojans • Rogueware/Scareware • Spam	• Physical Theft/Loss/Damage • Rogue certificates • Component corruption

3.2.2 Kybermaailman haavoittuvuudet

Hundley ja Anderson jakavat kybermaailman haavoittuvuudet seuraavasti (Hundley & Anderson, 1995, 237 - 238):

1. **Toimintoperustaisia**
    i. toimintajärjestelmät
    ii. prosessit
2. **Käyttäjäperustaisia**
    i. autentikointi
    ii. salasanat
3. **SW-perustaisia**
    i. takaovi
    ii. ohjelmistovirheet
    iii. asennusvirheet
4. **HW-perustaisia**
    i. suunnitteluvirheet
    ii. komponenttivirheet
5. **Verkkoperustaisia**
    i. TCP/IP

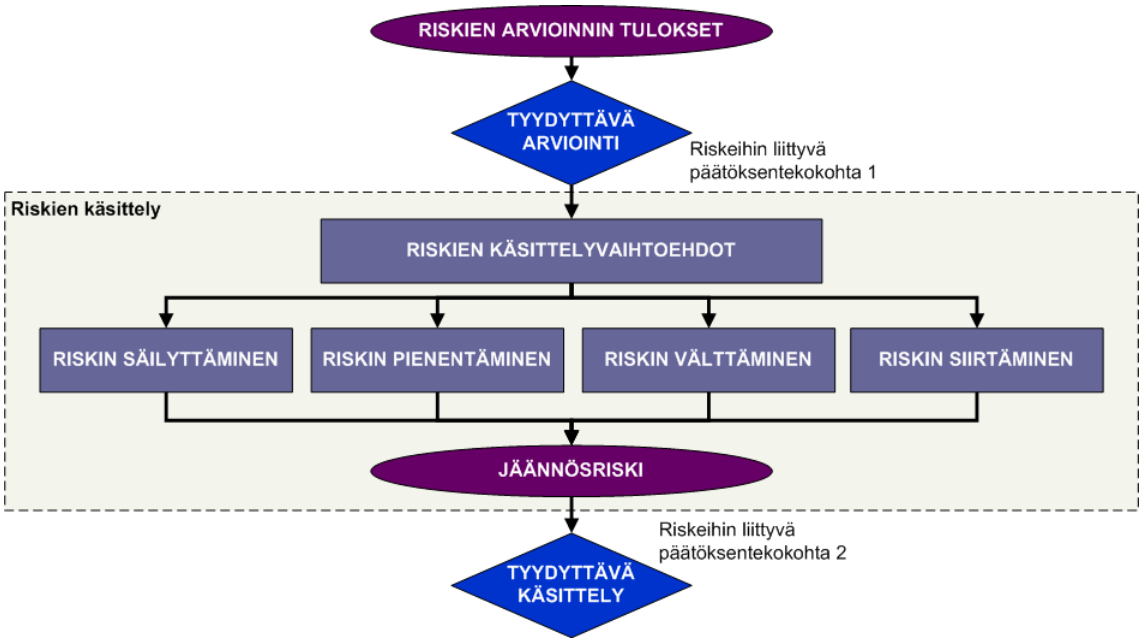
Yhteiskunta on yhä riippuvaisempi ohjelmistosta, tietokonelaitteistosta ja verkottuneesta toiminnasta ja siksi ICT-järjestelmät ja informaatioperustaiset järjestelmät ja toiminnat ovat kyberhyökkäysten kohteita. ICT-järjestelmien kompleksisuus tekee mahdottomaksi kokonaan eliminoida haavoittuvuudet sekä havaita ja jäljittää tunkeutumiset systeemin sisälle. Verkottuminen lisää tehokkuutta ja suorituskykyä, mutta samalla se lisää kyberturvallisuutta vaarantavia haavoittuvuuksia. Kuviossa 5 on esitetty tyypillisiä toimintaan liittyviä haavoittuvuuksia sijoitettuna aiemmin esitettyyn viisiportaiseen kyberrakennemalliin. (Lehto, 2014, 162.)



KUVIO 5. Kybertoimintaympäristön haavoittuvuuksia (Lehto, 2014, 168)

3.2.3 Toiminnan riskitarkastelu

Riskiä voidaan tarkastella sekä taloudellisen arvon että maineen menettämisen kannalta. Riskien arvioinnin tuloksista tulee johtaa päätösprosessi esimerkiksi kuvion 6 mukaisesti. Riskien käsittelyvaihtoehdot ulottuvat halitusta riskein säilyttämisestä riskien pienentämiseen, välttämiseen tai siirtämiseen mm. vakuuttamalla toimintaa niin, että jäännösrikit ovat organisaatiossa hyväksyttävällä tasolla. Riskejä voidaan pienentää tai joiltakin osin jopa välttää sääntelytoimenpitein, kehittämällä organisaation prosesseja ja yhteisöllisyyttä sekä kehittämällä teknologisia ratkaisuja.



KUVIO 6. ISO27005: Riskien käsittely (SFS-käsikirja, 2012, 205)

3.2.4 Tyypillisiä kyberhyökkäysmalleja

Haitan aiheuttaja toteuttaa kyberhyökkäyksiä kybermaailman eri rakenteisiin. Kyberrakenteen fyysiseen kerroksen voidaan kohdistaa sekä kineettistä että ei-kineettistä vaikutusta. Kineettisellä asevaikutuksella voidaan tuhota fyysisiä verkkoja, järjestelmiä ja niiden osia sekä tietovarastoja (Data Warehouse). Fyysisen maailman uhkia ovat myös laitejärjestelmien komponenteissa olevat haittaohjelmat ja takaportit.

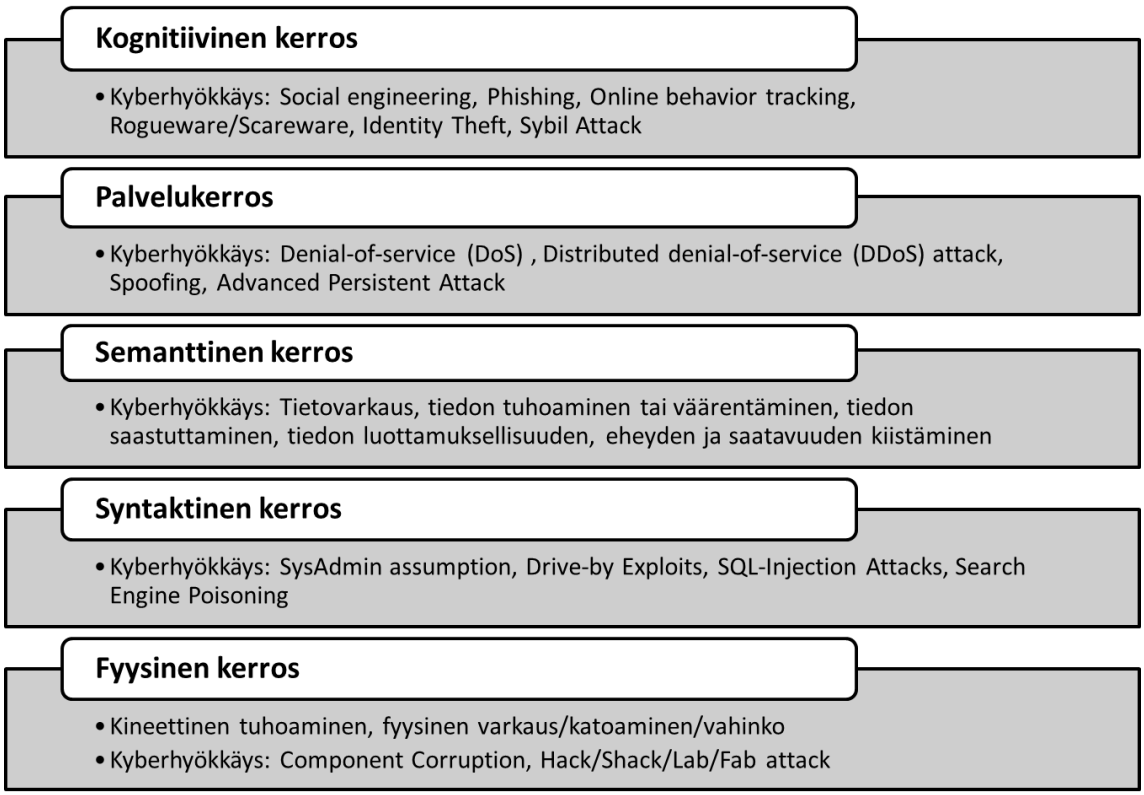
Hyökkäyksellä syntaktista kerrosta vastaan tavoitellaan järjestelmän tai sen osien saamista hallintaan. Hyökkäyksillä voidaan häiritä organisaation verkon toimintaa tai avata mahdollisuuksia hyökkäyksille muita kerroksia vastaan.

Kyberhyökkäyksen kohteena semanttista kerrosta vastaan on informaatio. Kybervakoilu voidaan määritellä toimeksi, jolla hankitaan salaisia tietoja (sensitiivinen, yksityisoikeudellinen tai turvaluokiteltu) yksityisiltä ihmisiltä, kilpailijoilta tai eri ryhmiltä poliittisen tai taloudellisen edun saavuttamiseksi käyttäen laittomia menetelmiä internetissä, verkoissa, ohjelmistoissa tai tietokoneissa. (Liaropoulos, 2010, 181 - 182.)

Hyökkäyksellä palvelukerrosta vastaan pyritään lamauttamaan verkkopalveluiden toiminta. Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston tarkoitettu käyttö.

Hyökkäys kognitiivista kerrosta vastaan voi kohdistua hyökkäyksenä johtoa tai muita päätöksentekijöitä kohtaan, tai vaikutusyrityksenä jollekin asiantuntijatasolle tai hyökkäyksenä kaikkia järjestelmien käyttäjiä vastaan. Hyökkäyksillä pyritään estämään esimerkiksi toiminnan

oikeanlaisen tilannetietoisuuden syntyminen. Kuviossa 7 on esitetty erilaisia hyökkäysmalleja ja -vektoreita kybermaailman eri kerroksia vastaan. (Lehto, 2014, 167 - 168.)



KUVIO 7. Hyökkäysvektoreita kybertoimintaympäristön eri tasoille (Lehto, 2014, 167 - 168)

3.2.5 Terveydenhuoltoon kohdistuneita kyberhyökkäyksiä

Tämän tutkimuksen tausta-aineistoksi tutkittiin pääosin vuosien 2013-2017 aikana tapahtunutta yli kuuttakymmentä (65 kpl) hyökkäystä terveydenhuoltoa vastaan. Tarkasteluun on otettu tapauksia Suomesta, muualta Euroopasta ja Pohjois-Amerikasta. Aineiston mukaan terveydenhuoltoa kohtaan tapahtuu perinteisiä hyökkäyksiä kuten hakkerointeja, kiristys- ja virushyökkäyksiä, laitteiden varastamista sekä hajautettuja palvelunestohyökkäyksiä (DDoS). Näillä hyökkäyksillä on ollut merkittäviä vaikutuksia terveydenhuollossa, koska toiminnan yhteydessä on usein päästy häiritsemään reaaliaikaisia palveluja, kuten potilastietojärjestelmiin tai sähköisiin resepteihin liittyviä palveluja. Huolestuttavaa on, että usein hyökkäyksiä ei huomata ennen kuin pitkän aikaa on kulunut tapahtuman alkamisesta ja usean aikaa on voinut kulua jopa kuukausia, jolloin tutkinta on vaikeaa ja isoja määriä tietoja on jo voinut päätyä rikollisten käyttöön. Kiristyshaittaohjelmahyökkäyksissä tartunta selviää nopeasti, mutta niissäkin tapauksissa palveluiden palauttaminen normaalitilaan voi kestää useita päiviä riippuen järjestelmän koosta, tartunnan laajuudesta ja varmuuskopiojärjestelyistä.

Tarkasteltaessa kyberhyökkäyksiä terveydenhoitoa kohtaan, nousevat kiristyshaittaohjelmat ja hakkerointi yleisimmiksi tapauksiksi. Aineisto jakaantuu hyökkäysvektoreiden perusteella seuraavasti:

1. Kiristyshaittaohjelma, 18
2. Hakkerointi ja tietomurto, 24
3. Muut tapaukset, yhteensä, 23
    a. Tietokoneen (vast.) varkaus, 9
    b. Virushyökkäys, 5
    c. DDos, 4
    d. Muu, 5

4 Sairaalan kyberturvallisuus

4.1 Parhaat käytännöt

Kansalliset standardointijärjestöt laativat kansallisia standardeja ja osallistuvat kansainvälisten standardien laadintaan, jolloin niissä on huomioitu parhaat käytänteet. Suomen kansallinen toimija tällä alueella on Suomen standardisoimisliitto ry (SFS). Suomessa on hajautettu standardisointijärjestelmä, jossa SFS toimii keskusjärjestönä ja laatii standardit yhdessä toimialayhteisöjensä kanssa. SFS toteaa standardien tarkoituksesta seuraavaa: Standardisointi on yhteisten toimintatapojen laatimista. Sen tarkoitus on helpottaa viranomaisten, elinkeinoelämän ja kuluttajien elämää. Standardisoinnilla lisätään tuotteiden yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa. (Suomen Standardisoimisliitto SFS ry.)

Organisaatiot käyttävät standardeja ja muita erilaisia ohjeita ja suosituksia vapaaehtoisesti. Niistä ilmenevät parhaat käytänteet ja tavoitteet liittyvät yleensä toiminnan kehittämiseen, jotka ovat parhaimmillaan ennakoivia menettelyjä. Kybermaailmassa ne avustavat käyttäjäänsä parannettaessa organisaation toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tällöin toiminnot saattavat olla esimerkiksi kyberturvallisuuden johtamisen ja hallinnoinnin tai teknillistä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa tai käyttöä.

Monien organisaatioiden kyberturvallisuuteen liittyvää toimintaa leimaa edelleen häiriötilanteisiin reagoiva toimintatapa, jossa sairaalat eivät tee poikkeusta. Reagoiva toimintatapa tarkoittaa, että häiriötilanteissa ollaan tapahtuneen tosiasian edessä ja toimintaa leimaa nopeat päätelmät ja kiireelliset toimenpiteet. Kyberturvallisuuden kehittäminen parhaita käytänteitä hyödyntäen luo edellytyksiä organisaatiossa erityisesti proaktiiviseen toimintaan reagoivan toiminnan sijasta.

NIST-standardin Kyberturvallisuuden viitekehys (Framework for Improving Critical Infrastructure Cybersecurity) tarjoaa organisaation kyberturvallisuuden kehittämiselle yhteisen kielen, ymmärryksen, ja hallinnan sisäisille ja ulkoisille sidosryhmille. Sen avulla voidaan tunnistaa ja priorisoida toimia kyberturvallisuuden riskien vähentämiseksi, luoda toimintapolitiikka ja yhdenmukaistaa tekniset lähestymistavat liiketoiminnan suojaamiseksi. Sitä voidaan soveltaa sekä oman organisaation proaktiivisen toiminnan kehittämiseen, että laajentaa tarvittaessa koskemaan myös organisaation kriittisten palvelujen toimittajia. Toiminnallinen viitekehys tarjoaa loogisesti etenevän joukon toimia kyberturvallisuuden kehittämiseksi. Lisäksi viitekehyksen jokainen toimenpide koostuu neljästä elementistä, jotka ovat toiminta ja sen kategoria, alakategoria ja niihin liittyvät informatiiviset viitteet. Oheiseen luetteloon on koottu viitekehyksen toimenpiteet ja niiden sisällöt (National Institute of Standards and Technology, 2018, 14 - 15.):

- **Tunnista** - Kehitä organisaation ymmärtämistä hallitsemaan kyberturvallisuus riskejä järjestelmissä, varoissa, datassa ja ominaisuuksissa.
- **Suojaa** - Kehitä ja toteuta asianmukaiset suojatoimet kriittisten infrastruktuuripalvelujen toimittamisen varmistamiseksi.
- **Havaitse** - Kehitä ja toteuta asianmukaiset toiminnot kyberturvallisuustapahtumien havaitsemiseksi.
- **Vastaa** - Kehitä ja toteuta asianmukaiset toiminnot toteutettavaksi havaittuihin kyberturvallisuustapahtumiin.
- **Palaudu** - Kehitä ja toteuta asianmukaiset toiminnot, joilla ylläpidetään sietokykyä koskevat suunnitelmat ja palauta kaikki kyvykkyydet tai palvelut, jotka olivat heikentyneet kyberturvallisuustapahtuman vuoksi.

Kategoriat ovat päätoimintojen osa-alueita, jotka ovat jaettavissa kyberturvallisuuden tarkasteluryhmiin, kuten esimerkiksi ”pääsyn hallinta” tai ”tunnistusprosessit". Alakategoriat jakaantuvat edelleen teknillisiin kohtiin ja / tai hallintatoimintaa. Informatiiviset viitteet ovat standardien, ohjeiden ja käytäntöjen osia, jotka ovat parhaita käytänteitä kyseseisin kohdan tarkasteluun.

Terveydenhuollon kyseessä ollen edellä mainitun kyberturvallisuuden viitekehyksen tarkastelussa voidaan hyödyntää seuraavissa kohdissa esitettäviä parhaita käytänteitä.

Terveydenhuollon sektorin kyberturvallisuus työryhmä (HCIC) on määritellyt kuusi korkean tason vaatimusta suositusten ja toimintatapojen järjestämiseksi. Kun suositukset on otettu käyttöön, ne auttavat lisäämään tilannetietoisuutta, vähentämään riskejä ja haavoittuvuuksia sekä toteuttamaan suojauksia. Vaatimukset toimenpiteiksi ovat (Csulak, Meadows, Cormane, DeCesarea, Finn, Jarrett, Laybourn, McNeil, McWHorter, Mellinger, Monson, Ramadoss, Rice, Sardanopoli, Suarez, Stine, Sublett, Thompson, Ting & Trotter, 2017, 24 - 44.):

1. Tehosta johtajuutta ja hallintotapaa sekä määritä selkeitä tavoitteita terveydenhuollon kyberturvallisuudelle.
2. Lisää lääkinnällisten laitteiden ja terveydenhuollon tietoturvaa ja organisaation häiriötilanteiden sietokykyä.
3. Kehitä terveydenhuollon henkilöstön osaamisalueita, jotka ovat tarpeen kyberturvallisuustietoisuuden ja teknisten valmiuksien priorisoimiseksi ja varmistamiseksi.
4. Kasvata terveydenhuollon sektorin toimintavalmiutta parantamalla kyberturvallisuustietoisuutta ja -koulutusta.
5. Tunnista mekanismit tutkimus- ja kehitystoiminnan sekä tiedollisen omaisuuden suojelemiseksi.
6. Paranna tiedonvaihtoa alan kyberturvallisuuden uhista, riskeistä ja suojaustoimenpiteistä.

Lääkinnällisten laitteiden ja potilastietojärjestelmän osalta on syytä tunnistaa erityisesti niitä kyberturvallisuuteen liittyviä haasteita, jotka muodostuvat mm. vanhoista käyttöjärjestelmistä, turvallisuuden kehittämisen eri elinkaarivaiheista, vahvan todentamisen haasteet, sekä sairaalaverkon strategiset ja arkkitehtuuriset lähestymistavat tuotteen käyttöönottoon, hallintaan ja ylläpitoon liittyen. (Csulak ym., 2017, 22 - 23.)

Kyberturvallisuuden kehittyessä on myöskin mahdollisuus toteuttaa huipputeknisiä turvallisuusratkaisuja, mutta korkean turvallisuustason aikaansaaminen merkitsee myöskin korkeita kustannuksia. Tämä tosiasia saattaa joissain tapauksissa rajoittaa yhteistyötä terveydenhuollossa tai sen palveluntarjoajien kanssa. Jossakin vaiheessa turvallisuuden rakentamisessa tuleekin vastaan tilanne, jossa organisaation on hyväksyttävä jäljelle jäävät tietoturvariskit. Tämä vuoksi sairaaloiden onkin suunniteltava, toteutettava ja ylläpidettävä yhtenäisiä toimintatapoja, prosesseja ja järjestelmiä riskien hallitsemiseksi.

Tärkeimpien turvatoimenpiteiden toteuttamiseen kuuluvat (ENISA, 2016, 10 - 11.):

- Verkon segmentointi (älykkäät palomuurit),
- Verkon valvonta ja tunkeutumisen havaitseminen,
- Vankka salaus,
- Kulunvalvonta,
- Käytön autentikointi ja valtuutus.

Kliinisessä työssä toimiva sairaalahenkilöstö käyttävät useita eri tietokoneita ympäri laitosta jatkuvasti (jopa 70 kertaa / vuoro) hoitotyössä. Toimijoiden tulee todentaa henkilöllisyytensä, jotta he voivat suorittaa näitä tehtäviään (esim. päästä potilastietoihin, tilata diagnostiikkatestit, määrätä lääkkeitä jne.). Tunnistautuminen tapahtuu tyypillisesti henkilökohtaisella käyttäjänimellä ja salasanalla. Menetelmä on altis kyberhyökkäyksille, sillä käytössä olevat salasanat ovat usein varsin heikkoja. NIST SP 800 - 663 antaa vaihtoehtoja salasanojen käytölle käyttäjän todentamiseen, mukaan lukien käyttäjän hallussa olevat esineet (esimerkiksi etäluettava kortti tai tunnisteväline) tai biometriikka. Myös hoidossa käytettävien lääkinnällisten laitteiden toimivuus on varmistettava kyberturvallisuuden näkökulmasta. Laitetta käyttävä organisaatio on todennettava ja valtuutettava käyttämään kyseistä laitetta hoitotyössä. Lisäksi laitteen ja muiden terveydenhuollon teknologioiden väliset yhteydet on todennettava. Toisin sanoen laitteista pitäisi tietää, minkä teknologian kanssa ne kommunikoivat, ja että niiden tulee voida pitää yhteyttä vain tekniikalla, joka sisältää tarvittavat tunnisteet. (Csulak ym., 2017, 32.)

Sairaaloiden tulisi lisäksi kiinnittää erityistä huomiota konkreettinen häiriötilanteiden toiminta- ja palautumissuunnitelmiin. Toimenpiteitä ovat mm. seuraavat (ENISA, 2016, 53.):

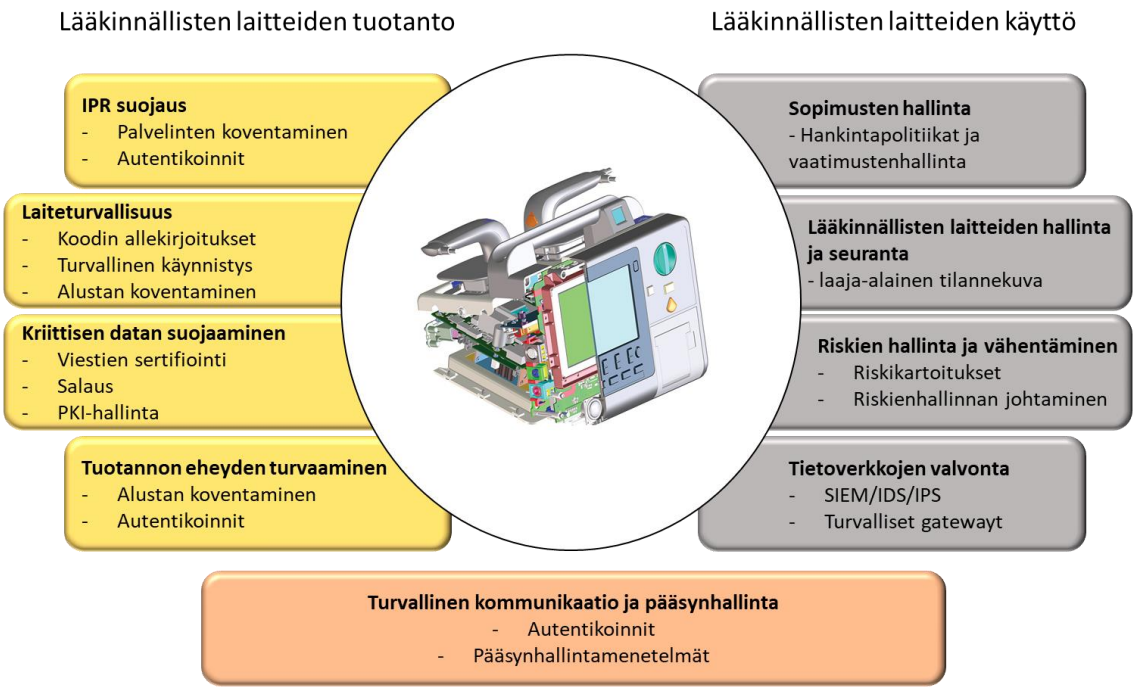
- Laaditaan kustannus-hyötyanalyysi sairaalan tärkeimmistä IoT-komponenteista. Älykkään sairaalan toteutus on kallista ja sille on asetettava riittävät kyberturvallisuutta edistävät suojaukset.
- Luodaan älykkäille sairaalalaitteille selkeä tietoturvastrategia, jossa roolit ja vastuut sekä säännöllinen koulutus ja tietoisuuden lisääminen ovat keskeisiä tekijöitä ennakoivan lähestymistavan aikaansaamiseksi tietoturvaan.
- Luodaan mobiililaitteiden ja omien laitteiden (BYOD) käytölle selkeät toimintaperiaatteet, koska nämä laitteet ovat usein osana älykkään sairaalan ekosysteemiä. Toimenpiteet tällä alueella ovat näin ollen ensisijaisen tärkeitä.
- Tunnistetaan laitteet ja miten ne liittyvät toisiinsa (tai ovat yhteydessä internetiin). Joidenkin järjestelmien osalta paras vaihtoehto turvallisuudelle ja sietokyvylle on, että valmistaja kieltää sisäänrakennetut verkko-ominaisuudet laitteeseen.
- Määritellään ja toteutetaan turvallisuusperusteet kaikille tärkeimmille käyttöjärjestelmille.

Toimintamenetelmien ja erilaisten teknillisten ratkaisujen lisäksi terveydenhuollon kyberturvallisuutta tulee lisätä kehittämällä henkilöstön toimintavalmiuksia. Hyvinä käytänteinä tässä yhteydessä toimivat erilaiset työpajat, kokoukset, konferenssit ja harjoitukset. Lisäksi terveydenhuollon sektorien on annettava potilaille tietoa siitä, miten hallinnoida terveystietoja. Lisäksi terveydenhuollon eri sektorien on kehitettävä kyberosaamisohjelmia kouluttaakseen toimintaketjujensa päätöksentekijöitä. (Csulak ym., 2017, 40.)

4.2 Lääkinnällisten laitteiden kyberturvallisuus

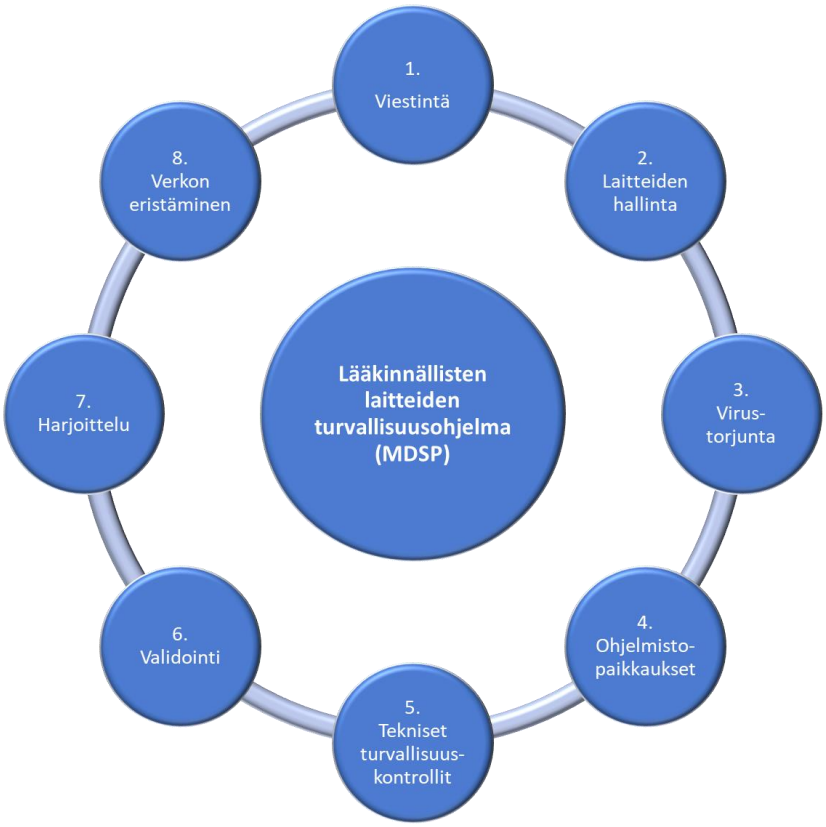
Yleinen käsitys on, että organisaatioiden kyberturvallisuuden kehittämisessä monitahoisella yhteistyöllä ja tiedonvaihdolla on keskeinen merkitys. Sitä tarvitaan erityisesti lääkinnällisten laitteiden ja järjestelmien osalta, kun otetaan huomioon, että verkkorikollisuuden riskienhallinta muodostuu laajasta joukosta sidosryhmiä. Vain sidosryhmien yhdessä muodostamalla vastuulla voidaan saavuttaa todellisia parannuksia tilanteeseen. Sidosryhmiin kuuluvat laitevalmistajat, laitteiden käyttäjät, järjestelmäintegraattorit ja terveydenhuollon ICT-kehittäjät.

Kuviossa 8 on vastuutoimenpiteitä hahmoteltu laitevalmistajan ja käyttäjäorganisaation kesken.



KUVIO 8. Lääkinnällisten laitteiden kyberturvallisuus – Jaettu vastuu (Symantec Corporatio, 2016, 2)

Lääkinnällisten laitteiden turvallisuusohjelma (kts. kuvio 9) antaa suuntaviivoja yhdessä muodostettavan jaetun vastuun toteuttamiseksi. Siinä toimenpiteet on kuvattu suunniteltaviksi siten, että ne ovat toistettavissa kahdeksan vaiheisessa prosessissa. Samalla se muodostaa ennaltaehkäisevän toiminnan mallin terveydenhuoltoon. Mallin avulla järjestelmä- ja laitetoimituksiin liittyvät eri osapuolet kykenevät arvioimaan, toteuttamaan ja viestimään lääkinnällisiin laitteisiin liittyvistä turvallisuusriskeistä. Ohjelma tuo yhteen tärkeitä sidosryhmiä, kuten kliinisen tekniikan, informaatioteknologian, tietoturvan ja vaatimustenmukaisuuden, laillisuuden, koulutuksen ja hankintaosastot, käsittelemään lääkinnällisten laitteiden kyberturvallisuuteen liittyviä haasteita. (Meditology Services LLC, 2017, 10.)



KUVIO 9. Lääkinnällisten laitteiden turvallisuusohjelma (Meditology Services LLC, 2017, 10)

Palveluntarjoajien tulee määritellä luokitukset ja prioriteetit lääkinnällisiin laitteisiin riskin/laitteen tyypin mukaan. Luokitukset voivat vaihdella organisaation painopisteiden perusteella, mutta ne voivat seurata esimerkin mukaista mallia (kts. taulukko 2 ja taulukko 3). (Meditology Services LLC, 2017, 10.)

TAULUKKO 2. Lääkinnällisten laitteiden prioriteettitasot (Meditology Services LLC, 2017, 10)

Prioriteettitaso	Kuvaus
1	Elintärkeä (defibrillaattori, sydämentahdistin, hengityskone)
2	Parantava/Terapeuttinen (infuusiopumppu, painekammio, dialyysi)
3	Potilasdiagnostiikka (sydänsähkökäyrä, ultraääni, röntgen, laboratoriolaitteet)
4	Analytiikka (sikiömonitori, potilasmonitori)
5	Sekalaiset (lääkekaapit, autoklaavi, vaaka)

TAULUKKO 3. Lääkinnällisten laitteiden turvallisuusluokitukset (Meditology Services LLC, 2017, 14)

Turvallisuusluokitus	Kuvaus
A	Yli 100,000 merkintää tallennettu, lähetetty tai käsitelty
B	10,001 – 99,999 merkintää tallennettu, lähetetty tai käsitelty
C	Alle 10,000 merkintää tallennettu, lähetetty tai käsitelty
D	Laite ei tallenna, lähetä tai käsittele terveystietoja

Lääkinnällisten laitteiden kyberturvallisuustoimenpiteiden luokittelemiseksi edellä esitetyistä laitteiden prioriteettitasoista ja turvallisuusluokituksesta voidaan muodostaa luettelo, jonka perusteella laitteiden suojaustoimenpiteille voidaan kohdistaa vaatimuksia ja toimenpiteitä voidaan toteuttaa optimaalisesti turvallisuusohjelman eri vaiheissa.

4.3 Uudet teknologiat

Uusi käynnissä oleva teknologinen vallankumous - Teollisuus 4.0 (Industrial 4.0) - muuttaa erityisesti valmistavan teollisuuden toimintaa. PricewaterhouseCoopersin (PwC) selvityksen mukaan valmistavan teollisuuden yritykset aikovat investoida noin 5 % vuosittaisesta liikevaihdostaan digitalisaatioon. Yli 80 % yrityksistä uskoo data-analytiikalla olevan viiden vuoden kuluessa merkittävä vaikutus päätöksentekoon ja operatiiviseen toimintaan. Datan ammattimainen käsittely tarjoaa muun muassa arvokasta tietoa tuotteiden käytöstä, laitteiden toiminnasta ja auttaa ylläpitämään pitkäkestoisia asiakassuhteita. Analytiikan avulla tuotteita voidaan kehittää asiakastarpeen mukaan ja niiden oheen voidaan tuoda personoituja palveluita. (PricewaterhouseCooper, 2016, 23.)

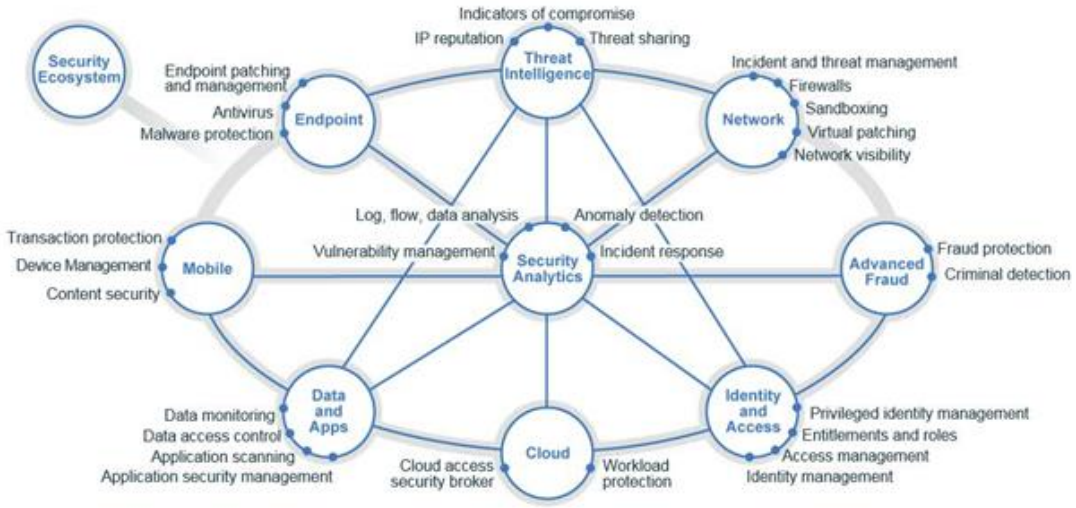
Kyberfyysinen järjestelmä on määritelty järjestelmäksi, jossa yhteen liitetyt ohjelmistot kontrolloivat fyysisiä laitteita. Kyberfyysiset järjestelmät ovatkin siten ohjelmistoalustoja, joilla valvotaan, ohjataan ja suojataan toimintaprosesseja. (Sadeghi, Wachsmann & Waidner, 2015, 1 - 2.)

Nämä ohjelmistoalustat tarvitsevat myös palvelimia ja muita laitteistoja, jolloin kokonaisuudesta muodostuu eräänlainen digitaalinen toiminta-alusta, jonka kehitystä sanelee edellä mainittu teollinen vallankumous – Teollisuus 4.0.

Nykyään on jo hyvin tarjolla erilaisia kyberturvallisuusratkaisuja ja -työkaluja organisaatioiden tarpeisiin. Haasteena ovat ratkaisujen ja työkalujen fragmentaarisuus sekä uusien systeemien implementaation ja ylläpidon ongelmat, mitkä aiheuttavat koko järjestelmään sekä monimukaisuutta että myös jopa kompleksisuutta, ja sitä kautta kokonaisuuden hallinnan vaikeutta. Systeemien monimutkaisuus ja kompleksisuus edellyttävät integroitujen kyberturvallisuusjärjestelmien kehittämistä, joissa on tunnistettu sekä ulkoiset että sisäiset uhat ja joihin on rakennettu kokonaisvaltainen turvallisuusjärjestelmä älykkään kyberturvallisuusarkkitehtuurin kautta (kts. kuvio 11).

Kyberturvallisuusjärjestelmän ja siten arkkitehtuurin teknillisen osan tulee sisältää älykkäitä analyysiratkaisuja organisaation koko ICT-infrastruktuurin alueella. Järjestelmällä tulee olla kyvykkyys nähdä sekä organisaation sisälle, että ulkopuoliseen maailmaan, joista uhat tulevat. ICT-infrastruktuurin tulee sisältää itsessään tarvittavat teknilliset turvallisuuskyvykkyydet. Uusia keinoja uhkien paljastamiseen tarvitaan, sillä organisaatio saattaa kohdata jopa 200 000 tietoturvatapahtumaa päivässä. Tapahtumien kattava tarkistaminen ihmistyönä on mahdotonta. Tarkistustyöhön tarvitaan myös tekoälyyn perustuvia ratkaisuja. Lisäksi tekoälyn kyvykkyys tulee esille erityisesti alkuvaiheen analyyseissä ja havaintojen läpikäynnissä. Tekoäly kykenee käsittelemään ja vertaamaan hetkessä satoja tuhansia asiakirjoja ja tietolähteitä ongelman ratkaisemiseksi. Tekoälyavusteisilla integroiduilla ratkaisuilla tavoitellaan aikaisempaa parempaa näkyvyyttä ICT-infrastruktuurin eri tasoille, jolloin suojautuminen ja torjunta voidaan toteuttaa kokonaisuutena eikä yksittäisinä toimenpiteinä. Tekoälyratkaisuja ja kognitiivista tietojenkäsittelyä voidaankin soveltaa kyberhyökkäysten havaitsemiseen, torjuntaan ja selvittämiseen.

Oheisessa kuviossa 10 on esitetty esimerkkinä IBM:n konsepti integroidusta kyberturvallisuusratkaisusta, jossa analytiikkakyvykkyys on asetettu ratkaisun keskiöön.



KUVIO 10. IBM:n integroitu kyberturvallisuuskonsepti (Falco, 2016)

MIT:n tutkijoiden ja koneoppimiseen erikoistuneen PatternExin yhteistyössä kehittämä tekoälyalusta AI2 ennustaa kyberhyökkäykset paremmin kuin mikään muu olemassa oleva järjestelmä. AI2 ei luota pelkkään automatiikkaan, vaan yhdistää automaattisiin löydöksiin ihmisasiantuntijoiden panoksen. Järjestelmä tunnistaa 85 prosenttia alkavista hyökkäyksistä, mikä on noin kolme kertaa enemmän kuin tämän hetken parhaiden järjestelmien kyky. Tutkijat ovat samalla onnistuneet vähentämään niin sanottujen väärien hälytysten (false positive) määrää huomattavasti. (Conner-Simons, 2016; Veeramachaneni, Arnaldo, Cuesta-Infante, Korrapati, Bassias & Li, 2016, 49.)

Tekoälyn ohella mielenkiitoinen tekniikka-alue on virtualisointi. Virtualisointitekniikan avulla voimme suojautua tai puolustautua hyökkääjiä vastaan käyttämällä osoitealueita, joita käyttöjärjestelmässä ei ole käytettävissä. Lähtökohtaisesti virtualisointi on kehitetty ratkaisemaan tietokonetekniikan resurssiongelmaa. Tietokoneiden arkkitehtuurista johtuen ne on suunniteltu suorittamaan vain yhtä käyttöjärjestelmää ja sovellusta kerrallaan. Virtualisointi mahdollistaa useiden käyttöjärjestelmien ja sovellusten toiminnan yhdellä fyysisellä palvelimella tai "isännällä". Jokainen itsenäinen "virtuaalikone", joka sisältää vieraskäyttöjärjestelmän ja -sovelluksen, on eristetty muista toiminnoista. Virtualisoinnissa hyödynnetään virtualisointikomentoja, joilla käyttöjärjestelmä siirretään virtuaalikoneeksi (on-the-fly) ja lisäksi luodaan hypervisori, joka ohjaa laitteita. Hypervisori voidaan määrittää tarttumaan "mielenkiintoisiin" tapahtumiin. (Zaidenberg, 2017, 135, 137 - 138.)

Tulevaisuuden Teollisuus 4.0 ympäristössä liikkuu valtava määrä dataa sen eri osien välillä. Tietojen on oltava salassa mm. siksi, että suojaustoimenpiteillä varmistetaan organisaation sijoituksen tai aineettoman omaisuuden suojaaminen sekä tiedon luottamuksellisuus, käytettävyys ja eheys. Kyseeseen tulevat kryptograafiset ratkaisut ja niiden algoritmien siirtäminen integroidun alustan toiminnoiksi. Tällöin tulee ratkaistavaksi ongelma siitä, että miten voimme käyttää salaisia tietoja ja varmistaa niiden salassa pidettävyys tietojenkäsittelyn aikana. Asiaan liittyy ainakin seuraavia lähestymistapoja ja ominaisuuksia (Heitmann, 2017, 11):

- Alkuperäisten tietojen muuttaminen
  - anonymisointi ja sekoittaminen - runsaasti hyötyjä ja vähän suojaa
- Alkuperäisten tietojen peittäminen ennen käsittelyä
  - käytettävyyden menettäminen - vaikea hyödyntää monenkeskisesti
- Salaisen tiedon käyttäminen sellaisenaan laskennassa (ilman salauksen purkamista)
  - pieni käytettävyyden menetys - hidas käsittely laskennassa (monimutkainen)
- Lohkoketju
  - tarjoaa laajassa mitassa luotettavuutta

Data suojausta tutkittaessa ja tehokkaita lähestymistapoja kehitettäessä on datan käsittelyyn osallistuvien käyttäjäosapuolten suojaamiseksi toimintaprosessissa huomioitava seuraavia toimenpiteitä (Heitmann, 2017, 33):

- Toimintamallit luodaan salatun datan käsittelyyn, esimerkiksi koneoppimiseen.
- Toimintamallit salataan ja jaetaan muille osallistujaosapuolille.
- Osallistujaosapuolet käyttävät salattua toimintamallia omassa toiminnassaan.
- Toimintamallien kehittäminen suojataan.
- Toimintamalleja ei anneta ulkopuolisten käyttöön.

Yritysten verkottuminen on laajentunut muun muassa ulkoistettujen toimintojen kautta (muun muassa ICT-palvelut) ja voivat parhaimmillaan muodostaa jo globaaleja ketjuja. Tämän johdosta minkä tahansa verkon linkin ongelma voi aiheuttaa suuria häiriöitä koko ketjussa. Toimitusketjuihin liittyvät kyberturvallisuuden riskit kohdistuvat hankintaan, toimittajien hallintaan, kuljetusvarmuuteen ja moniin muihin toimintoihin ja prosesseihin koko toimitusketjussa. Verkottuneessa toiminnassa toimitusketjun riski eivät rajoitu vain tavaroiden fyysiseen tuotantoon tai jakeluun, vaan toteutuessaan hyökkäykset voivat aiheuttaa häiriöitä ketjun tietovirroissa. Yleisesti ottaen datan käsittelyyn tarvitaan korkeita turvatakuita yhteistyötä tekevien eri osapuolten väleille. Algoritmit tarjoaisivat paremman tietoturvan, jos kaikki käsiteltävät tiedot voidaan pitää vähintään muuttumattomina. Lohkoketju on tekniikka, jolla ICT-infrastruktuurin toimijat voivat yhdessä tuottaa ja ylläpitää luotettavia tietoja hajautetusti. Tekniikassa jokainen uusi lohko sisältää edeltävän lohkon tiivisteen, joka muodostaa lohkoketjun muuttumattoman historian. Lohkoketjuteknologia mahdollistaa hajautetusti ja luotettavasti tuotettuna muun muassa digitaaliset älykkäät sopimukset, sähköiset omaisuusrekisterit, identiteettirekisterit, laitteiden väliset tiedot ja autonomiset organisaatiot.

Nykyään voidaan jo tunnistaa tekoälyyn perustuvien haittaohjelmistojen aiheuttamia hyökkäyksiä ICT-infrastruktuuria vastaan. Ne ovat aiempia hyökkäysmuotoja epäsymmetrisempiä verrattuna kyberpuolustukseen, joten tulevaisuuden haasteet liittyvät siihen, miten voimme kehittää vastaavasti tekoälyyn pohjautuvia suojausmenetelmiä esimerkiksi turvallisen kyberfyysisen järjestelmäalustan aikaansaamiseksi. Näin ollen edelleen pätevät suojaustoimintoina henkilöstön hyvä koulutus (käyttäjät, ICT-henkilöstö) sekä se, että sovelletaan kehittyneimpiä ja parannettuja turvallisuusmenetelmiä (ml. politiikka), parannetaan lähdekoodin laatua ja läpinäkyvyyttä ja huolehditaan ohjelmistopäivityksistä. Henkilöstön osaamisessa tulee huomioida Teollisuus 4.0 tekniikoiden muodostama toimintaympäristö. (Destre, 2017, 36 - 37.)

Teollisuus 4.0 ympäristössä esiintyvistä erilaisista digitaalisignaaleista voidaan muodostaa niihin perustuva kunnonvalvonta, jota voidaan hyödyntää myös kyberhyökkäysten havainnoinnissa. Siinä prosessimallin kuvaus muuttujineen ja analyysitietojen redundanssi muodostavat johtopäätösten perustan. Älykkäässä alustassa tulee huomioida erityisesti langattomiin yhteyksiin pohjautuvien liikkuvien robottien anturin mittauksen vianilmaisu ja mallinnukseen perustuva vianhavaitsemisjärjestelmän täysimääräinen hyödyntäminen. Antureissa ja toimilaitteissa muodostavat perustiedot tekoälyratkaisujen vikadiagnosointiin kyberhyökkäyksiä vastaan. (Dai, 2017, 37.)

5 Sairaalan kyberturvallisuusarkkitehtuuri

5.1 Kyberturvallisuusarkkitehtuurin tarve ja rakenne

Teollisuus 4.0 kehityksen myötä organisaation ICT-infrastruktuuri muodostuu yhä tiiviimmästä kokonaisuudesta, joka on laitteiden, ohjelmistojen ja ihmisten muodostama yhteenliittymä. Se kehittyy monimutkaisuuden kautta yhä kompleksisempaan suuntaa eri osien sisältämien keskinäisten vuorovaikutusten vuoksi. Kehityskulku asettaa uusia vaatimuksia järjestelmien perinteisen syvyyssuuntaisen suojausstrategian kehittämiseen.

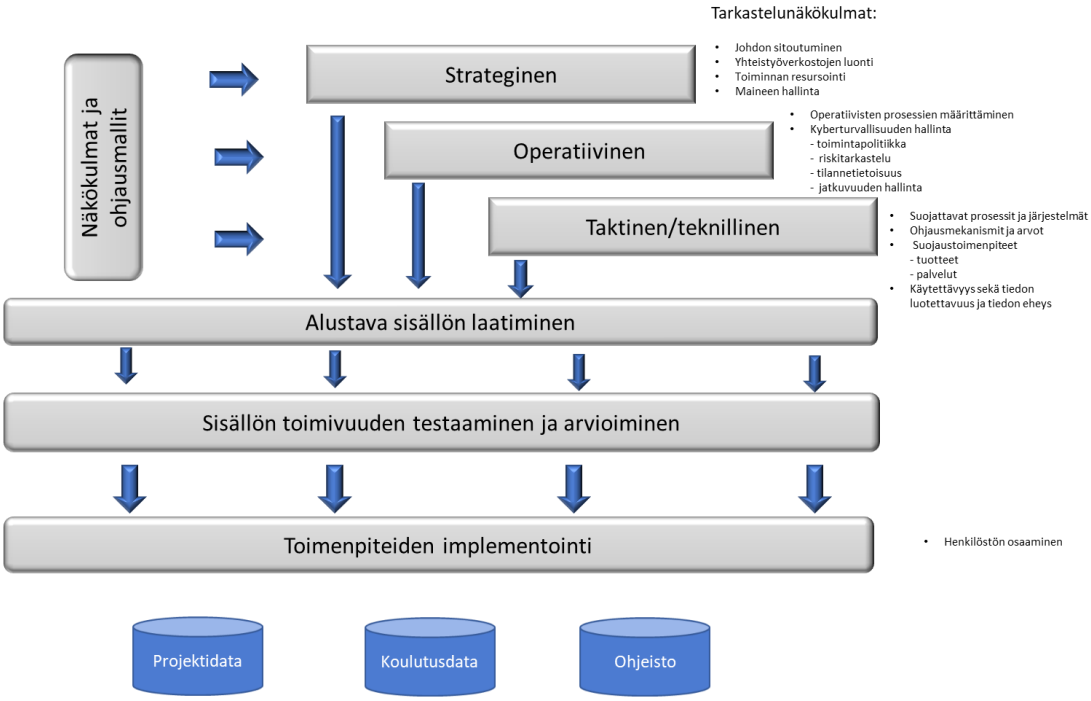
Tällä hetkellä useita kyberturvallisuusratkaisuja ja -työkaluja on tarjolla organisaatioiden tarpeisiin. Haasteena ovat ratkaisujen ja työkalujen fragmentaarisuus sekä uusien systeemien implementaation ja ylläpidon ongelmat, mitkä aiheuttavat koko järjestelmän kompleksisuuden kasvun ja hallinnan vaikeudet. Systeemien kompleksisuus edellyttää integroitujen järjestelmien kehittämistä, joissa on tunnistettu sekä ulkoiset että sisäiset uhat ja rakennettu kokonaisvaltainen kyberturvallisuusjärjestelmä.

Organisaation ICT-infrastruktuurin perinteiseen kuorisuojaukseen integroiduilla uuden teknologian ratkaisuilla parannetaan näkyvyyttä järjestelmätasoilla. Tällöin uhkilta suojautumista voidaan kehittää kokonaisuutena ja siten täydentää yksittäisinä toimenpiteinä toteutettuja ratkaisuja. Tekoälyn kyvykkyyttä voidaan hyödyntää tapahtumien analyyseissä ja havaintojen läpikäynnissä. Tekoäly kykenee käsittelemään hetkessä satoja tuhansia asiakirjoja ja tietolähteitä. Esimerkiksi tällä hetkellä julkaistaan päivittäin lähes 8 000 kyberturvallisuutta käsittelevää artikkelia, joiden käsittelyyn ja hyödyntämiseen tarvitaan älykästä konetta.

Hyökkääjä voi käyttää hyväkseen organisaatioiden siiloutuneita turvallisuusratkaisuja, joilla kullakin on vaikuttavuutta organisaation koko ICT-järjestelmään. Perinteiset suojauskehiin perustuvat turvallisuusratkaisut haastetaan tämän päivän kehittyneillä hyökkäysmenetelmillä, jotka kohdistuvat organisaatioon sekä sen ulkopuolelta, että sisäpuolella. Integroidussa turvallisuusjärjestelmässä on tavoitteena luoda vahva tietoverkon suojaus, päätelaitteiden hallinta ja turvallisuus, datavirtojen aktiivinen monitorointi, havaintokyvykkyyden kehittäminen ja erilaisten hyökkäysvektoreiden torjunta. Järjestelmä edellyttää kyvykkyyttä ymmärtää alati muuttuvaa hyökkäysalaa ja uusia hyökkäysvektoreita. Tavoitteena voitaneen pitää älykkäistä kyberturvallisuusratkaisuista yhdessä perinteisten menetelmien kanssa muodostettava alusta. Se mahdollistaisi laajan ekosysteemin integroituja turvallisuusratkaisuja. Alustaratkaisu voisi mahdollistaa tehokkaan kyberturvallisuuden asiantuntijaverkoston ja tekoälysovelluksen yhteistyön, jossa tekoäly toimii avustavan asiantuntijan roolissa toteuttamalla toimintaympäristössä tarvittavia toimenpiteitä ja samalla tuottamalla jalostettua informaatiota päätöksenteon pohjaksi.

Kehittäminen voi tapahtua muodostamalla älykäs järjestelmäalusta. Älykäs järjestelmäalusta vastaa kyberturvallisuusarkkitehtuurissa kysymykseen: miten IT-infrastruktuurin suojaustoimenpiteet on suoritettava? Se liittyy organisaation toimintatasolla teknillis-taktiseen näkökulmaan. Muut organisaation näkökulmat kyberturvallisuuden arkkitehtuurissa ovat strateginen ja operatiivinen näkökulma. Edellinen vastaa kysymykseen miksi suojaustoimia tarvitaan ja jälkimmäinen vastaa kysymykseen mitä pitää erityisesti suojata.

Tässä tutkimuksessa on päädytty laatimaan organisaation kyberturvallisuuden kokonaisarkkitehtuuri, jota voidaan esittää oheisella kuviolla 11. Siitä ilmenevät sekä eri näkökulmat pääasiallisine sisältöineen, että sen toteutusprosessi vaiheineen.



KUVIO 11. Sairaalan kyberturvallisuusarkkitehtuuri

Sairaalajärjestelmien sisältämien tietosisältöjen (datan) suojaaminen mahdollistaa tiedon käytettävyyden (saatavuuden), luotettavuuden ja eheyden varmistamisen perinteisten tietoturvallisuuden edellyttämin keinoin. Kyberfyysisten järjestelmien osalta datan suojaamisen lisäksi on erityistä huomiota kiinnitettävä koko kybertoimintaympäristöön. Kuvion 11 kyberturvallisuusarkkitehtuuri ohjaa huomion kiinnittämisen tarkastelunäkökulmien kautta koko sairaalaorganisaation toimenpiteisiin. Johdon sitoutuminen ja siten koko toiminnan resursointi on onnistuneen kyberturvallisuuden edellyttämän toiminnan lähtökohta.

Myös operatiivisten prosessien tunnistaminen, priorisointi ja jatkuvuuden hallinnan tunnistamiset johdattavat tarkastelun teknillisen tason ratkaisujen muodostamiseen. Teknillisellä tasolla kyberfyysisten järjestelmäalustojen kyberhyökkäysten torjunta edellyttää, että järjestelmäalustaan ja sen toimintaan kehitetään joustavia ominaisuuksia, jotka parantavat erityisesti suojausmenetelmiä, uudelleenkonfigurointia ja vikadiagnostiikkaa sen automaatio- ja logistiikkamoduuleissa. Toiminta voi perustua tulevaisuudessa yhä enemmän älykkäisiin moduuleihin, jotka voivat tunnistaa kriittisten ja potentiaalisten kyberhäiriöiden oireet jo ennalta ja toipua häiriöistä nopeasti.

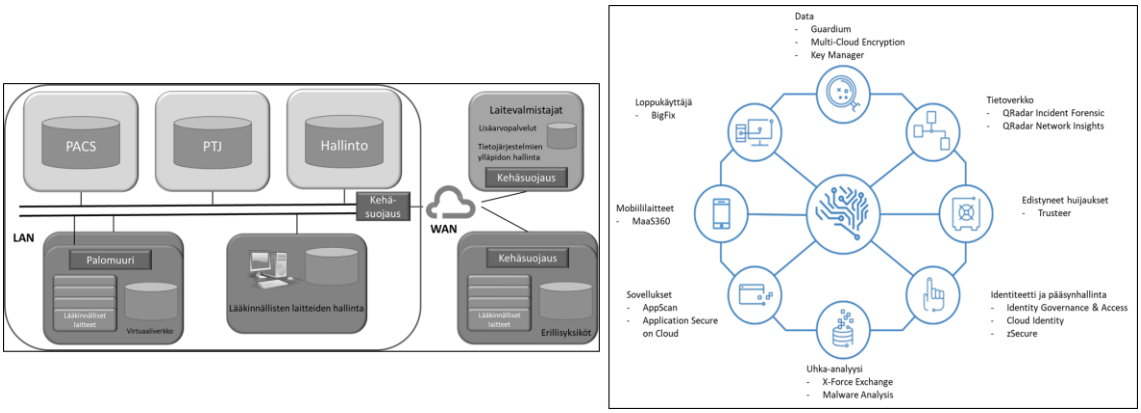
Tällöin käyttöön voidaan hahmotella mm. seuraavia menetelmiä ja toimenpiteitä, jotka ovat Teollisuus 4.0 päivitettyjä:

- Älykkäitä häiriöiden tunnistamisella ja vikadiagnostiikoille kehitettyjä tekoälymenetelmiä.
- Virtualisoinnin hyödyntämistä, jolloin hypervisori voidaan kehittää tarttumaan poikkeaviin tapahtumiin.
- Keitetään edelleen suojaustoimintoina henkilöstön koulutusta (käyttäjät, IT-henkilöstö), sovelletaan kehittyneimpiä ja jatkuvasti päivitettäviä turvallisuusmenetelmiä ja -tekniikoita, parannetaan lähdekoodin laatua ja läpinäkyvyyttä ja huolehditaan ohjelmistopäivityksistä.
- Kehitetään kyberturvallisia komponentteja (Hardware) järjestelmien eri osiin, parannetaan järjestelmien kehittämistä, hallintaa ja käyttöä kaikilta osiltaan.
- Kehitetään salassapidon ja yksityisyyden suojaa tiedonhankinnassa, tietojen analysoinnissa ja jakamisessa. Tähän lohkoketjutekniikka tarjoaa laajassa mitassa luotettavuutta.

5.2 IBM Security-kyberturvallisuuskonsepti

5.2.1 Vyöhykesuojaus ja älykkäät suojausratkaisut

Älykkään kyberturvallisuusarkkitehtuurin avulla voidaan kehittää kyberfyysisten järjestelmäalustojen turvallisuutta kaikilta osiltaan yhdistämällä perinteiseen vyöhykesuojausstrategiaan uuden teknologian avulla integroituja ratkaisuja. Kehittämisen seurauksena kokonaisuudesta muodostuu älykäs järjestelmäalusta. Kuviossa 12 vasemmalla on sairaalajärjestelmä, joka pitää sisällään vyöhykesuojauksen menetelmiä ja oikealla on IBM:n integroitu kyberturvallisuuskonsepti. (Falco, 2015; Integrating the Healthcare Enterprise, 2015, 9 - 10.)



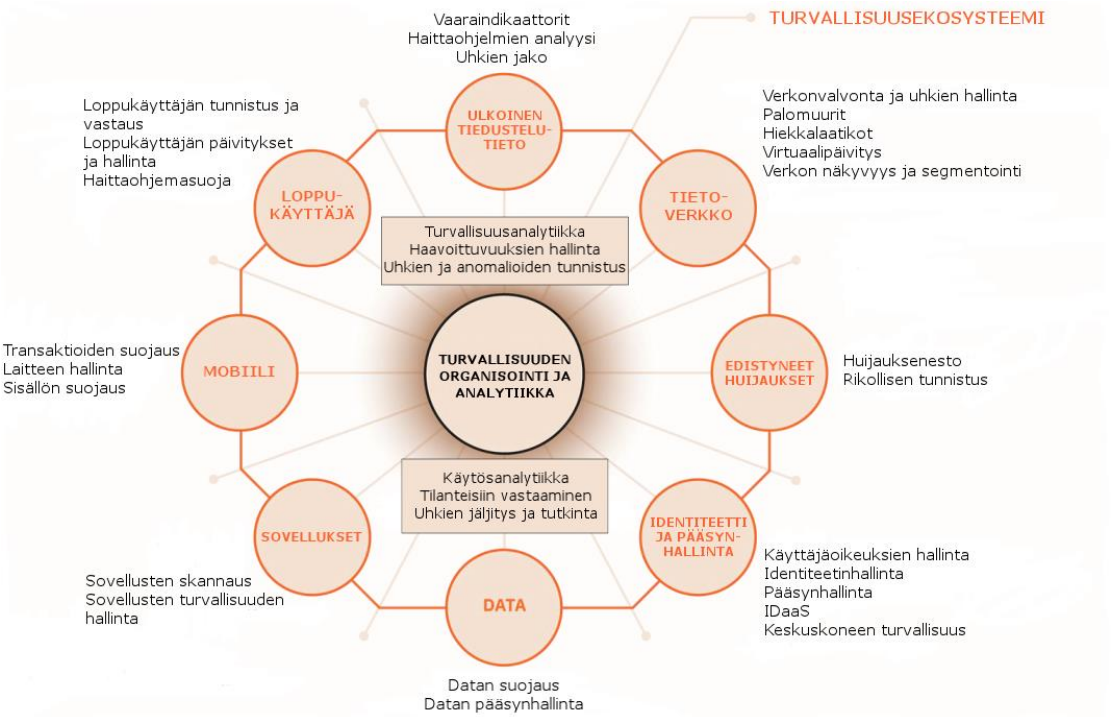
KUVIO 12. Sairaalajärjestelmä ja IBM:n integroitu kyberturvallisuuskonsepti

Kuviossa 12 sairaalajärjestelmä on jaettu vyöhykkeisiin suojausvaatimusten ja -tason mukaisesti (Perimeter Security). Vyöhykkeiden välillä on tyypillisesti sekä fyysisiä että tietoteknisiä suojamuureja (esimerkiksi palomuurit). Vyöhykesuojauksessa eri tietoturvan tasoa vaativat järjestelmät on sijoitettu suojattuihin segmentteihin ja jatkuvuuskriittiset tietojärjestelmät sijaitsevat verkkoarkkitehtuurissa parhaiten suojatulla alueella. Näin saavutetaan monikerroksittainen suojaus, joka on tyypillinen tämän päivän tietoteknillisissä arkkitehtuureissa.

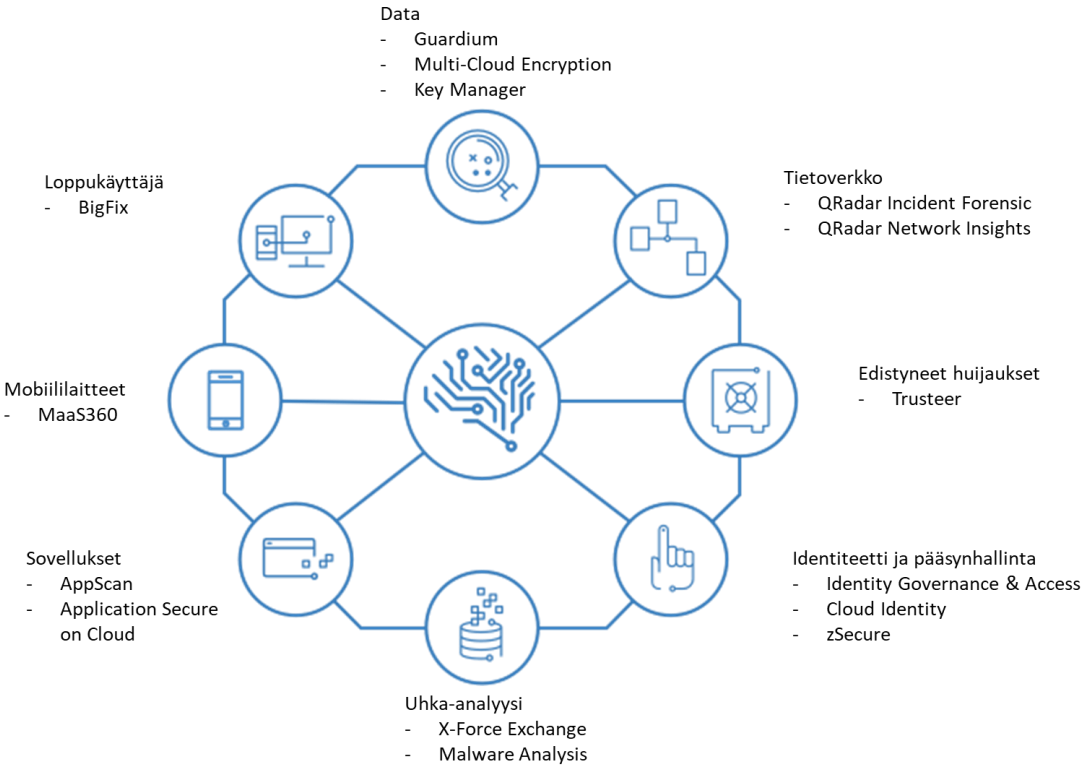
IBM kyberturvallisuuskonsepti puolestaan koostuu kahdeksasta osasta, jotka ovat ulkoinen tiedustelutieto (Threat Inteligence), tietoverkko (Network), edistyneet huijaukset (Advanced Fraud), identiteetti ja pääsynhallinta (Identity & Access), tietovarannot (Data), sovellukset (Apps), mobiili (Mobile) ja loppukäyttäjä (Endpoint). Konseptin tarkoituksena on olla kokonaisvaltainen ratkaisu, jonka avulla koko organisaation tietoturvaa voidaan edistää monialaisesti. Vuonna 2017 Watson for Cyber Securityn kognitiiviset teknologiat integroitiin osaksi uutta IBM Cognitive SOC -alustaa (Security Operations Consulting), joka mahdollistaa älykkäisiin moduuleihin pohjautuvan kyberturvallisuuden järjestelmäalusta-ajattelun kehittämisen. Seuraavaksi selvitetään edellä mainittuihin moduuleihin pohjautuvien Watson-kyberturvallisuusratkaisujen liittämismahdollisuuksia nykyisen sairaalajärjestelmän vyöhykeperusteisen turvallisuusratkaisun tueksi. Aluksi tarkastelussa käydään läpi IBM:n konseptin ominaisuuksia ja sen jälkeen tarkastellaan niiden soveltuvuutta viisikerroksisen kyberturvallisuuden rakenteen suojaukseen (kts. kuvio 12).

5.2.2 IBM konsepti

IBM:n konseptin ja sen sovellustason ratkaisujen (kuviot 13 ja 14) keskeisenä kyberturvallisuutta analysoivana ja toimenpiteiden ohjausta avustavana sovelluksena on IBM QRadar Watson Advisor, joka hyödyntää kerättyä tietovarantoa. IBM QRadar Watson Advisor ja sen sisältämät kognitiiviset kyvykkyydet ovat hyödynnettävissä IBM QRadar Security Intelligence Platformin kautta. Potentiaalisten uhkien tunnistamisessa voidaan hyödyntää Watsonin luonnollisen kielen ymmärtämisen kyvykkyyksiä, jolloin mahdollistuu muun muassa blogien, verkkosivujen, tutkimusraporttien ja QRadarin tarjoaman datan läpikäynti. Prosessin tarkoituksena on nopeuttaa uhkiin reagointia. IBM SOC -alusta kykenee lisäksi hyödyntämään IBM:n i2-analytiikkatyökalua ja IBM X-Force Exchange-tietokantaa.



KUVIO 13. IBM Security - integroitu kyberturvallisuuskonsepti



KUVIO 14. IBM:n integroitu kyberturvallisuuskonsepti ja sen sovellukset

IBM i2 Enterprise Insight Analysis (EIA) käyttää olemassa olevaa tietoturvainfrastruktuuria, muuta dataa ja avoimien lähteitä hyödyntävien järjestelmien tarjoamaa dataa. Häiriötilanteessa tapahtuman tutkiminen perustuu näiden tietolähteiden hyödyntämiseen. Ratkaisu käyttää myös sosiaalisesta mediasta saatua tietoa erityisesti häiriön aiheuttajan tai aiheuttajien tunnistamiseksi. Näihin tietoihin perustuen organisaatio voi kehittää suojautumisen toimintastrategioitaan ja -mallejaan.

EIA:n on avoin ja modulaarinen arkkitehtuuri, joka on skaalautuva ja lisäksi räätälöitävissä kolmannen osapuolen sovelluksien ja niiden tarjoamien ominaisuuksien kanssa. Tällöin tulee kyseeseen mm. luonnollisen kielen prosessointi ja analytiikka taktisella, operationaalisella ja strategisella tasolla. Avoin malli mahdollistaa myös tilannetiedon jakamisen tietoturvauhkista sekä omassa organisaatiossa että kumppaneiden, asiakkaiden ja muiden organisaatioiden kanssa.

5.2.3 Tietoturvauhat (Threat Intelligence)

Tietoturvauhkiin keskittyviä analyysi ja tietämystosio perustuvat relevantin datan ja informaation tunnistamiseen, keräämiseen ja rikastamiseen. Alustan tietoturvauhkien analyysimenetelmät käyttävät pohjana dataa haitantekijöistä hunaja-ansoja, roskapostiansoja ja pimeää verkkoa hyväksi käyttäen. Alusta sisältää uhkatiedusteluun liittyvä elementtejä ja siten kykenee analysoimaan häiriöistä saatavia indikaattoreita jatkuvasti. Osioon kuuluu uhkatietopankki, jota pidetään yllä päivittäisistä tietoturvatapahtumaista kerättävällä tiedolla. Tiedot voidaan kategorisoida maantieteellisen sijainnin ja vaarallisuuden mukaan. Alusta sisältää tällä hetkellä yli 700 teratavua dataa sekä reaaliaikaista tietoa tietoturvahyökkäyksistä. Sovellustasolla tähän ulkoisen tiedustelutiedon hallintaan on tarjolla X-Force Exchange-alusta. X-Force Exchange on yhteistyöalusta, joka tuo uhkien analytiikkapalveluita- ja teknologioita pilvipalveluun SaaS (Software as a Service) palveluna. Palvelu on tietoturvallisuusuhkia koskevan informaation jakamiseen keskittynyt alusta, joka mahdollistaa nopean globaaleihin tietoturvallisuusuhkiin keskittyvien tutkimuksien läpikäymisen, tietämyksen kokoamisen yhteen paikkaan, asiantuntijakonsultaatiot ja yhteistyön muiden tietoturvauhkiin keskittyvien tahojen kanssa. Alustan avulla organisaatiot voivat tehdä yhteistyötä tietoturvauhkien vastaisessa taistelussa ja jakaa tietoa keskenään.

5.2.4 Tietoverkko (Network)

Tietoverkon osa-alueeseen kuuluvat QRadar Incident Forensics, QRadar Network Insights, Management Network Security ja Secure SD-Wan toiminnot. QRadar Incident Forensics mahdollistaa askel askeleelta jäljittää oletettavan hyökkääjän tai hyökkääjien toimia ja tutkia epäilyjä aiheuttavia tietoverkkotapahtumia. Se myös nopeuttaa QRadarin keräämän informaation tutkimista, jota QRadar Network Insights analysoi tietoverkossa liikkuvasta datasta reaaliajassa. Se seuloo dataa paljastaakseen hyökkääjän ”jalanjäljet” tai paljastaakseen piilossa olevia tietoturvauhkia, kuten haittaohjelmia, ennen kuin ne vahingoittavat organisaatiota. Managed Network Security Services mahdollistaa monitorointi-, hälytys-, ja verkon

tietoturvateknologiapalveluita osana kokonaiskonseptia. Secure SD-WAN liittyy laajakaista- ja WAN-verkon hallintaa tarkoituksena tunnistaa käyttäjien identiteettejä ja sovelluksia koskevat asiat.

5.2.5 Loppukäyttäjä (Endpoint)

Loppukäyttäjäosio sisältää BigFix-toiminallisuuden (Endpoint Manager), joka on kehitetty järjestelmähallintaa varten. Sen avulla on mahdollista hallita suuria ryhmiä tietokoneita, joiden käyttöjärjestelminä ovat esimerkiksi Windows, Mac OS X, VMaware ESX, Linux ja Unix sekä erilaiset mobiilikäyttöjärjestelmät, kuten Windows Phone, Symbian, iOS ja Android. BigFix tarjoaa järjestelmän ylläpitäjille työkalut etähallintaan, laitepäivitykseen, ohjelmistojen jakeluun, käyttöjärjestelmien kehitykseen, tietoverkkojen tietoturvan ylläpitämiseen ja laitteistojen sekä ohjelmistojen luetteloimiseen.

BigFix:n alusta jakautuu ICT-toimintoihin ja tietoturvaan sekä edelleen osiin, jotka sisältävät laitehallinnan (Endpoint Management) ja loppukäyttäjän tietoturvan (Endpoint Security). Laitehallinta puolestaan koostuu kolmesta osasta, jotka liittyvät havainnointiin (Discovery and Patching), elinkaarihallintaan (Lifestyle Management) sekä ohjelmistojen yhdenmukaisuuteen ja käytettävyyteen (Software Compliance and Usage). Loppukäyttäjän tietoturva sisältää myös kolme osaa, jotka ovat toiminnan jatkuvuuden hallinta (Continuous Monitoring), uhkilta suojautuminen (Threat Protection) ja tapahtumiin reagointi (Incident Response).

Havainnointiin (Discovery Patchin) liittyvä osa-alue tarjoaa yhden konsolin hallintajärjestelmän useiden laitteiden ja niiden ominaisuuksien tunnistamiseen, ylläpitoon ja raportointiin. Hallintajärjestelmän avulla voidaan tehostaa laitteiden päivitysprosessin onnistumisessa ja saada tietoa päivitysten tilasta. Elinkaarihallintaan liittyvä osio (Lifestyle Management) auttaa etsimään ja korjaamaan ongelmia kaikilla organisaation IT-infastruktuurin alueilla, kuten mobiiliympäristössä, fyysisessä ympäristössä tai virtuaalisessa ympäristössä. Ohjelmistojen yhdenmukaisuuteen ja käytettävyyteen (Software Compliance and Usage) liittyvä osa-alue auttaa tunnistamaan asennettuja ohjelmia ja niiden käyttöä. Toiminnon avulla voidaan löytää kaikki lisensioidut ja lisensioimattomat ohjelmistot. Toiminto auttaa myös tunnistamaan käyttämättömiä tai tarpeettomia ohjelmistoja. Jatkuvuuden hallintaosio (Continuous Monitoring) tarjoaa ominaisuuksia haavoittuvuuksien etsimiseen ja toiminnan sisäiseen valvontaan. Uhkilta suojautumisen osio (Threat Protection) mahdollistaa reaaliaikaisen hyökkäyksien tunnistuksen ja järjestelmän puolustuksen hyökkäyksien aikana. Hyökkäyksien jo tapahduttua tapahtumiin reagointiosio (Incident Response) mahdollistaa asettaa saastuneita laitteita karanteeniin ja auttaa hyökkäyksistä saastuneiden laitteiden tunnistamisessa.

BigFix- ja QRadar-ohjelmistoja voidaan käyttää yhdessä siten, että QRadar generoi havaitsemiaan tietoturvauhkiin liittyviä hälytyksiä BigFix:n korjattavaksi ja BigFix avustaa organisaation IT-tukea korjaamaan haavoittuvuudet. Prosessi mahdollistaa tietoturvauhkien ja haavoittuvuuksien priorisoinnin, riskien arvioinnin ja raportoinnin.

5.2.6 Mobiililaitteiden hallinta (Mobile)

Mobiililaitteiden hallintasovellus, MaaS360, mahdollistaa organisaation henkilökohtaisten mobiililaitteiden, sovelluksien ja sisällön hallinnan tietoturva huomioiden. Tietoturvallinen ympäristö mahdollistaa sensitiivisten tiedostojen erottamisen mobiililaitteisiin asennetuista sovelluksista. Hallintasovellus hyödyntää Watsonin analytiikkaominaisuuksia tuottaa relevanttia informaatiota organisaation datasta, joka voi olla sekä rakenteellisesta että rakenteettomasta. Siihen liittyy myös ominaisuus hyödyntää mobiililaitteiden tietoturvaindeksiä ja pilvipohjaista datan suorituskykytestiä.

5.2.7 Identiteetti ja pääsynhallinta (Identity, Access)

Identiteetti ja pääsynhallintaosioon lukeutuva ZSecure-ratkaisu on suunniteltu auttamaan loppukäyttäjiä hallitsemaan palvelimien tietoturvallisuutta, monitoroimaan tietoturvauhkia, valvomaan käyttöä ja konfigurointeja sekä valvomaan toimintaan liittyvien sääntöjen noudattamista. Ratkaisun avulla voidaan toteuttaa myös kattavia data-analyysejä, joiden avulla voidaan tunnistaa piilossa olevia ja monimutkaisia riskejä, tehdä hälytyksiä ja räätälöityjä raportteja. ZSecure-ratkaisuun kuuluu oleellisena osana RACF (Resource Access Control Facility) tietoturvajärjestelmä, joka mahdollistaa hallita käyttöoikeuksia ja käyttöprofiileita sekä luoda lokitiedostoja. Toiminnon pääominaisuudet muodostuvat autentikoinnista, järjestelmäresurssien identifioinnista, luokittelusta ja suojaamisesta sekä suojattujen järjestelmien ja resurssien käyttöä valvonnasta.

zSecure Administration koostuu zSecure Admin ja zSecure Visual-työkaluista. Admin automatisoi myös toistuvia tietoturvatehtäviä, kuten salasanojen hallintaa ja käyttäjien sekä käyttäjäryhmien ID-informointia. Admin kykenee myös yhdistämään turvallisuussäännöstöjä erilaisista tietokannoista sekä pitämään useat eri RACF-tietokannat synkronoituina. Lisäksi Adminin kyvykkyyksiin kuuluu tietokantojen siivoaminen ja käskyjen muodostaminen tehtävän suorittamiseksi. Visual-käyttöliittymä puolestaan mahdollistaa kriittisen informaation tarkastelun ja optimoi resursseja hajauttamalla RACF:n ylläpidon siten, että se voidaan toteuttaa osastotasoittain.

5.2.8 Ohjelmisto, sovellukset (Apps)

Organisaation IT-infrastruktuurin ohjelmistojen (Apps) tietoturvan testauksen ja riskien hallinnan osa-alueelle on käytettävissä Appscan-sovellus. Se tukee ohjelmistoihin kohdistuvien riskien arviointia hyödyntäen tietoturvatestausta, jonka avulla voidaan tunnistaa ja eliminoida niiden haavoittuvuuksia. Sovellus auttaa myös kontrolloimaan ohjelmistojen kehittämistä ja käyttöönottoja tunnistamalla haavoittuvuuksia ja virheitä jo aikaisessa prosessin vaiheessa. Sovelluksen ominaisuuksiin kuuluu myös monitorointikyky, jolla voidaan seurata ohjelmistoihin liittyvien tietoturvaohjelmien edistymistä ja hallinnoimaan sääntelyvaatimuksia, jotka on kehitetty suojaamaan WEB-sovellusten prosessoimaa sensitiivistä dataa. Sovelluksen avulla mahdollistetaan koko ohjelmistokehityksen elinkaaren aikana tapahtuva tietoturvatestaus. Tietoturvatestejä voidaan toteuttaa osana ohjelmistokehityksen rutiineita ja laaduntarkastusprosesseja yhtäaikaisesti

ohjelmistokehityksessä ja tuotannossa olevien sovellusten kanssa. Ominaisuuden avulla pyritään varmistamaan se, että kaikki ohjelmistokehityksessä olleet sovellukset tarkastetaan ennen julkaisua ja kaikki tuotannossa olevat sovellukset voidaan säännöllisesti tarkastaa tietoturvauhkien ja haavoittuvuuksien varalta. Toiminta vaatii tietoturva-, ohjelmistokehitys- ja testausryhmien toimivaa yhteistyötä ja toimivaa alustaa tähän tarkoitukseen.

5.2.9 Tietovarannot (Data)

Tietovaranto-osioon liittyy Guardium-alusta, joka on suunniteltu suojaamaan kriittistä dataa sen paikasta riippumatta. Alusta avustaa käyttäjiä automaattisesti analysoimaan tietojärjestelmäympäristön tapahtumia. Tällöin on mahdollista minimoida riskejä sekä suojella sensitiivistä dataa sisäisiltä ja ulkoisilta uhkilta. Alustaan liittyy graafinen käyttöliittymä, jonka avulla käyttäjät voivat tunnistaa ja korjata sensitiiviseen dataan kohdistuvia riskejä. Alusta kykenee käsittelemään rakenteetonta ja rakenteellista dataa sekä relaatiotietokantoja, tietovarastoja erilaisine tietokantoineen. Monikerroksinen alustaratkaisu mahdollistaa automatisoidun tietoturvauhka-analyysien tekemisen, dynaamisen datan suojauksen ja koko organisaation laajuisen tietovarantojen analysoinnin. Alustan keskeisimmät ominaisuudet yhteenvetona ovat; datan etsintä ja riskiluokittelu, datan käsittelijän tunnistaminen, poikkeavuuksien havainnointi analytiikan ja koneoppimisen menetelmin, uhkien tunnistaminen ja tietomurtojen pysäyttäminen.

5.2.10 Edistyneet huijaukset (Advanced Fraud)

Edistyneet huijaukset osion Trusteer-ominaisuus mahdollistaa toteuttaa organisaation asiakasrajapintaan luottamuksellisen identiteetin tarkastusmenetelmän. Se hyödyntää pilvipohjaisia älykkäitä ratkaisuja. Trusteer-ominaisuuksia ovat jatkuva digitaalinen identiteetin suojaus ja pilvipalvelu, joka tarjoaa reaaliaikaisia arvioita uhkista.

Trusteer Pinpoint Detect auttaa suojaamaan liiketoiminnan käyttötilejä ja havaitsemaan korkean riskin haittaohjelmien tartunnan saaneita loppukäyttäjälaitteita. Trusteer Pinpoint Assure on suunniteltu havaitsemaan ja ennustamaan riskit, jotka liittyvät asiakassuhteeseen jo sen käynnistämisvaiheessa. Trusteer Mobile SDK auttaa havaitsemaan reaaliaikaiset laitteiden ja istuntojen riskit ylläpitämällä niissä käytettävien sovellusten eheyttä analysoimalla laiteriskejä. Myös muita indikaattoreita, kuten käyttäytymishäiriöitä, navigointieroja ja tietojenkalastelua, voidaan hyödyntää. Trusteer Mobile Browser tarjoaa mobiililaiteeseen tietoturvaa silloin, kun käytetään suojattua verkkosivustoja. Laitteeseen tehdään riskiperusteinen analyysi havaitsemaan muun muassa väärennetyt pankkisivut ja man-in-the-middle-hyökkäykset. Trusteer Rapport on suojausratkaisu loppukäyttäjille, jonka tarkoituksena on suojata käyttäjiä haittaohjelmilta ja phishing-hyökkäyksiltä. Sen avulla voidaan havaita MitB-hyökkäyksiä (Man-in-the-Browser), poistaa haittaohjelmia päätelaitteista ja estää ulkopuolisten tahojen pääsyn tietojenkalastelualueisiin.

6 Toimenpiteet sairaalan kyberturvallisuuden edistämiseksi

6.1 Kyberturvallisuusarkkitehtuurin huomioiminen

Sairaalan kyberturvallisuusarkkitehtuurin lähtökohdat voidaan muodostaa hyödyntämällä terveydenhuollon kyberturvallisuustyöryhmän (HCIC) määrittelyjä ja suosituksia toimintatapojen järjestämiseksi. (Csulak ym., 2017, 1.) Ne liittyvät organisaation johtajuuteen ja hallintoon, häiriötilanteiden sietokykyyn, henkilöstön osaamiseen sekä tutkimukseen ja tiedonvaihtoon. Toimenpiteissä tulee myös tunnistaa kyberturvallisuuteen liittyvät haasteet, jotka muodostuvat erityisesti laitteiden erilaisista elinkaarivaiheista ja heijastuvat järjestelmätasolla uusien tuotteiden käyttöönottoon, hallintaan ja ylläpitoon.

Älykkäitä sairaaloita kehitettäessä ENISA painottaa uudistuksissa tietoturvastrategioiden ja kustannus-hyötyanalyysien merkitystä strategisella päätöksentekotasolla päätettävistä riittävistä kyberturvallisuutta edistävistä suojausratkaisuista (ENISA, 2016, 11). Suosituksissa operatiivisen tason tehtävänä on luoda toimintapolitiikka, joka huomio erityisesti mobiililaitteiden ja henkilökunnan omien laitteiden (BYOD) käytölle selkeät periaatteet. Teknis-taktisella tasolla tulee tunnistaa käytettävät laitteet ja miten ne liittyvät toisiinsa (tai ovat yhteydessä Internetiin) sekä määrittää ja toteutetaan turvallisuusperusteet kaikille tärkeimmille järjestelmille. Kaikilla päätöksentekotasoilla roolit ja vastuut sekä säännöllinen koulutus ja tietoisuuden lisääminen ovat keskeisiä tekijöitä ennakoivan lähestymistavan aikaansaamiseksi tietoturvaan.

Toimintamenetelmien ja erilaisten teknillisten ratkaisujen lisäksi terveydenhuollon kyberturvallisuutta tulee lisätä kehittämällä henkilöstön toimintavalmiuksia. Hyvinä käytänteinä tässä yhteydessä toimivat erilaiset työpajat, kokoukset, konferenssit ja harjoitukset. Lisäksi terveydenhuollon sektorien on annettava potilaille tietoa siitä, miten hallinnoida terveystietoja.

Sairaalan, kuten yleensäkin organisaatioiden, kyberturvallisuuden kehittämisen perusteet alkaa visiointi- ja strategiatyön tasoilta. Johdon laatima visiointi toimintansa kehittämiseksi muutetaan strategisiksi tavoitteiksi, operatiivisen tason toimenpiteiksi, ohjeiksi ja toteutuspolitiikaksi. Teknis-taktisella tasolla toteutetaan strategiasta johdettuja käytännön toimenpiteitä. Toimenpiteiden onnistumisen mahdollistavat organisaation kyvykkyystekijät.

6.1.1 Strateginen näkökulma

Terveydenhuolto on tärkeä osa kansallista infrastruktuuria, mikä antaa selkeän perusten kunkin sairaalan strategiatyölle. Painotuksen voi tällöin kohdistaa kyberluottamuksen jatkuvaan kehittämiseen ja ylläpitämiseen osana kansallista kriittistä infrastruktuuria. Strategiset valinnat liittyvät luontevasti terveydenhuoltovastuun, organisaatiomaineen, sairaalatoiminnan ja sen jatkuvuuden varmistamiseen. Johdolta edellytetään konkreettisia strategisia valintoja sekä valittujen toimenpiteiden suorittamisen tukemista ja ohjaamista läpi koko organisaation. Johdon

tärkeänä tehtävänä on huolehtia toimenpiteiden riittävästä resursoinnista sekä uudistuksissa tietoturvastrategioiden ja laitevalintojen kustannus-hyötyanalyysien huomioimisesta päätöksenteosta. Valituista toimenpiteitä tulee viestittää kattavasti organisaation henkilöstölle ja muille sidosryhmille.

6.1.2 Operatiivinen näkökulma

Operatiivisen tason toimenpiteillä edistetään strategisia tavoitteita. Kattavat turvallisuutta ja luottamusta lisäävät toimenpiteet edellyttävät kokonaisvaltaista kyberturvallisuuden hallintaa. Sen lähtökohtana tulee olla kohteen riskiarviointi ja arvioinnin perusteella tehtävät toimenpideanalyysit. Organisaation on myös tärkeää julistaa ja viestittää politiikka, jolla johto sitoutuu hallinnan kehittämisen edellyttämiin toimenpiteisiin. Kyberturvallisuuden varmistavan politiikan julistaminen ja toimintatapojen kehittäminen tulee yhdistää organisaation yleiseen toimintapolitiikkaan. Organisaation ylimmän tason tehtävänä on linjata hyväksyttävät riskitasot ja riskien pienentämiseen liittyvät toimenpiteet politiikan avulla. (Johnson, Dempsey, Ross, Gupta & Bailey, 2011, 1.) Operatiivisen tason konkreettiset käytännön toimenpiteet tulee kohdistaa tietoturvaratkaisujen varmistamiseen sekä organisaation toiminnan jatkuvuus- ja toipumissuunnitelmien laadintaan. (Suomen Standardisoimisliitto SFS ry, 2012, 211 - 212). Sairaalaympäristössä käytettävien erilaisten laitteiden (ml. mobiililaitteet ja henkilöstön omat laitteet, BYOD) hallinnan ja käytön tilannetietoisuuden ylläpitäminen on toiminnan jatkuvuuden varmistamisessa avainkysymys. Tavoitteena tulee olla toimintaprosessien käytettävyyden jatkuva seuranta ja päätöksenteon tuenta analysointia ja päätöksiä edellyttävissä häiriötilanteissa.

6.1.3 Taktinen- ja teknillinen näkökulma

Taktisen- ja teknillisen näkökulman voi katsoa painottuvan kiinteästi käytännön laiteiden ja järjestelmien sekä niiden käytön suojaukseen. Myös turvallisen toiminnan ohjausmekanismit, kuten salasanakäytännöt ja laitteista huolehtiminen, yhdessä toimintakulttuurin kehittämisen ja toiminnan arvopohjan huomioimisen kanssa ovat keskeisiä tekijöitä toiminnan käytettävyysvaateiden sekä tiedon luotettavuus- ja tiedon eheysvaateiden osilta.

NIST-organisaation (National Institute of Standards and Technology) ohjetta Framework for Improving Critical Infrastructure Cybersecurity noudattaen voidaan painottaa alla olevaan menettelyä myös sairaalan tapauksessa (National Institute of Standards and Technology, 2018, 1). Lähtökohtana on tällöin sairaalan suojattavien prosessien ja sitä kautta laitteiden ja järjestelmien tunnistaminen. Tähän liittyy erityisesti organisaation kyky ymmärtää ja hallita kyberturvallisuusriskejä niissä (kts. liitteet 1 ja 2). Suojaustoimenpiteitä voidaan kehittää ja toteuttaa tämän jälkeen asianmukaisilla kyberturvallisuustuotteilla ja -palveluilla, jotka vastaavat erityisesti laiteriskeihin. Edellä mainitut toimenpiteet mahdollistavat toimintaan liittyvien riskien ja häiriöiden havaitsemisen perustan. Toisaalta tilannekuva ja sitä kautta syntyvä havaintokyky ja tilannetietoisuus ovat parhaimmillaan huomattavasti laajempi asia. Suomalainen vahvuus on

julkisen ja yksityisen sektorin yhteistyö (Public and Private Partnership, PPP) ja muu organisaatioiden välinen yhteistyö. (Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen, 2018, 62.)

Tilannetietoisuuden hyödyntämissuunnitelmat tulee laatia erikseen ja kouluttaa henkilökunta toimimaan niiden mukaisesti havaittuihin kyberturvallisuustapahtumiin vastaamiseksi. Myös tapahtumista palautumisen ratkaisee kokonaisuus, jossa henkilöstöä, palveluja ja tekniikkaa hyödynnetään tapauskohtaisesti ja suunnitellusti. Palautumisen liittyy merkittävänä tehtävänä siitä oppiminen ja toiminnan kehittäminen.

Tyypilliset vyöhykesuojauksen kyberturvallisuustuotteet ja -palvelut liittyvät verkon segmentointiin (muun muassa älykkäät palomuurit), valvontaan ja tunkeutumisen havainnointiin, salaukseen, kulunvalvontaan sekä käytön autentikointiin ja valtuutukseen (ENISA, 2016, 35). Vyöhykesuojausta voidaan pitää yhdistelmänä erilaisia teknillisiä ratkaisuja, joilla organisaation ICT-järjestelmien laitetasot pyritään suojaamaan häiriön aiheuttajilta (kts. kuvio 14).

Sairaalan ICT-järjestelmistä ja niiden laitteista muodostuva teknillinen kokonaisuus on systeemiajatuksen mukaan terveydenhuollon osajärjestelmä. Sitä voidaan hyvin kutsua sairaalan ICT-alustaksi. Tällöin systeemitason näkökulmasta katsottuna tuleekin huolehtia siitä, että kaikilla terveydenhuollon toimijoilla on riittävät kyberturvallisuusvalmiudet ja parhaat käytännöt organisaation koosta tai sijaintimaasta riippumatta. Näin voidaan yhdessä toimien ennalta ehkäistä laajojen kyberhäiriötilanteen syntyminen. Organisaatiotason ICT-järjestelmien ja -laitteiden vyöhykesuojauksen täydentämistä toimenpiteillä, jotka kohdistuvat niiden kyberrakenteeseen kaikilla tasoilla, voisi nimittää systeemitason suojaukseksi taktisella tasolla. Taktiselle tasolle kehitettävää systeemitason kybersuojausta on kuvattu seuraavassa luvussa.

6.2 Systeemitason suojauksen teknillinen kehittäminen

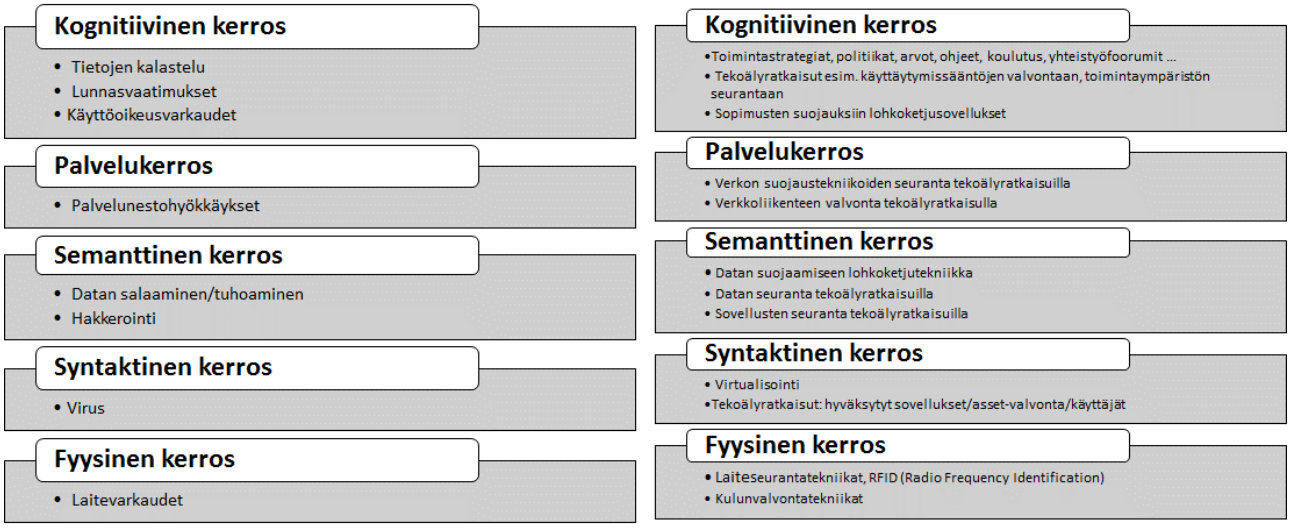
6.2.1 Systeemitason suojauksen kehitystä edistävät tekniikat

Kyberfyysisissä järjestelmissä verkon avulla yhteen liitetyt laitteet ohjelmistoineen kontrolloivat fyysisiä prosesseja. Sairaalan toimintaan liittyy merkittävä määrä teknillisiä laitteita ja niistä koostuvia toiminnallisia kokonaisuuksia – järjestelmiä, jotka ovat kyberfyysisiä järjestelmiä. Sairaala on teknillisessä mielessä järjestelmistä koostuva järjestelmä ja on puolestaan osa isoa terveydenhuollon kokonaisuutta. Toimintoja verkottuu siten monella tasolla terveydenhuollossa.

Teollisuus 4.0 kehityskulku mahdollistaa nykyistä älykkäämmän sairaalan suunnittelun ja toteutuksen edistyksellistä teknologiaa, kuten tekoälyä, robotiikkaa, IoT:tä ja uusia potilastietojärjestelmiä hyödyntäen. Asiaan liittyy myös ajatukset etähoidon ja -diagnostiikan sekä ns. oman datan käytön hyödyntämisestä.

Perinteiset organisaation ICT-infrastruktuurin syvyyssuuntaisiin vyöhykkeisiin suojauskehiin perustuvat turvallisuusratkaisut eivät vastaa enää riittävästi tämän päivän kehittyneisiin uhkiin, jotka tulevat laajalta alueelta joko organisaation ulkoa tai sisältä. Näin ollen integroidussa turvallisuusjärjestelmässä tulee voida teknillisillä ratkaisuilla luoda vyöhykkeisiä suojauskehiä täydentävä vahva käyttäjä-, tietoverkko- ja datavarantojen suojaus, päätelaitteiden hallinta ja turvallisuus, datavirtojen aktiivinen monitorointi, havaintokyvykkyyden luominen ja erilaisten hyökkäysvektoreiden torjunta. Järjestelmä edellyttää kyvykkyyttä ymmärtää alati muuttuvaa hyökkäysalaa ja uusia hyökkäysvektoreita. Älykkäästä kyberturvallisuusarkkitehtuurista voidaan muodostaa kyberturvallisuuteen alustoja, jotka tarjoavat laajan kohdennetun ekosysteemin integroituja turvallisuusratkaisuja. Alustaratkaisut mahdollistavat tehokkaan kyberturvallisuusasiantuntijoiden ja tekoälysovelluksen yhteistyön, jossa tekoäly toimii avustavassa roolissa toteuttamalla tarvittavia suojaustoimenpiteitä ja samalla tuottamalla analyysin kautta jalostettua informaatiota päätöksenteon pohjaksi. Lisäksi virtualisointi antaa mahdollisuuksia ICT-prosessien valvontaa, lohkoketjutekniikka sopimusten ja datan suojaukseen sekä RFID-tekniikka (Radio Frequency Identification) laiteseurantaan. Älykkään kyberturvallisuusarkkitehtuurin mukaisen alustaratkaisun tulee sisältää joustavasti ja kattavasti sovellettuna Teollisuus 4.0-kehityksen mukanaan tuovia muita ratkaisuja. (Suomen Automaatioseura ry Turvallisuusjaosto, 2010, 69 - 70.)

Oheisessa kuviossa 15 on terveydenhuoltoon viime vuosina kohdistuneita hyökkäyksiä, jotka on koottu tämän tutkimuksen tausta-aineistosta (liite 3). Ne on sijoitettu tyypilliseen organisaation ICT-rakenteeseen, jota sairaalan järjestelmät myös edustavat. Kuvaan on myös hahmoteltu uuden teknologian mahdollistavia suojausideoita (kts. luku 4.3). Ratkaisut voidaan rakenteessa kohdistaa sen eri kerroksille, jolloin niiden yhteisvaikutuksella ns. systeemitason teknillistä suojausta voidaan tavoitella.



KUVIO 15. Sairaalajärjestelmien uhkakuvat ja uudet suojaustekniikat

Systeemitason suojausta voidaan pyrkiä kehittämään soveltamalla uusien tekniikoiden avulla ratkaisuja kyberrakenteen jokaiselle tasolle.

Systeemitason ajattelussa kognitiiviselle kerrokselle liittyvät organisaation visiot toiminnasta ja siitä johdetut toimintastrategiat ja politiikat. Organisaation arvot, toimintaohjeet, henkilöstön koulutus ja muut henkilöstön kompetenssia kehittävät tapahtumat, kuten kyberturvallisuuden yhteistyöfoorumit ja muut vastaavat tapahtumat, muodostavat yhdessä edistyksellisten suojaustekniikoiden ja palvelujen kanssa toiminnan jatkuvuuden varmistamiseen hyvän perustan. Tekoälyratkaisut voivat soveltua käyttäytymissääntöjen valvontaan, toimintaympäristön seurantaan ja esimerkiksi käyttöoikeuksien hallintaan laajasti eri laitteissa ja järjestelmissä. Kognitiivisella tasolla verkottuneessa toiminnassa organisaation riskit liittyvät myös organisaation tietovirtoihin. Lisäksi datan käsittelyyn tarvitaan luotettavia menettelyjä yhteistyötä tekevien osapuolten väleille. Lohkoketjutekniikan soveltaminen mahdollistaa hajautetusti ja luotettavasti erilaisissa tietovirroissa ja -varannoissa suojaamisen organisaatioiden kesken. Lohkoketjutekniikalla voidaan suojata myös osapuolten välisiä kaupallisia ja muita vastaavia sopimuksia.

Palvelukerros pitää sisällään julkisen tiedonhaun, julkiset ja kaupalliset verkkopalvelut, kansalaisen palvelut, operatiiviset palvelut ja viestinnälliset palvelut. Tekoälyratkaisuja kehittämällä verkkoliikenteestä voidaan seuloa dataa ja siten paljastaa normaalista poikkeavia ilmiöitä, kuten haittaohjelmia. Verkon suojaustekniikoiden seuranta tekoälyratkaisuilla mahdollistanee esimerkiksi verkon käyttäjien ja sovellusten tunnistamisen.

Semanttinen kerros pitää sisällään systeemitasolla kaiken sen datan, jota muodostetaan rakenteen eri kerroksilla ja kootaan toiminnan edellyttämällä tavalla. Sen suojaaminen tulee entisestään korostumaan, koska älykkäät alustaratkaisut tuottavat koko ajan aiempaa enemmän dataa ja koko järjestelmän toiminta tulee perustumaan myös aiempaa enemmän datan käyttöön. Datan saatavuus, luotettavuus ja eheys korostuvat. Tämän päivän tekoälyratkaisut kykenevät käsittelemään rakenteetonta ja rakenteellista dataa sekä relaatiotietokantoja, tietovarastoja erilaisine tietokantoineen. Ne mahdollistavat siten organisaation laajuisen tietovarantojen tietoturva-analyysien tekemisen. Lisäksi eräänä ajatuksena voisi olla tekoälyratkaisuilla tapahtuva dataa tuottavien sovellusten seuranta. Yhteenvetoina voisivat olla datan riskiluokittelu, datan käsittelijän tunnistaminen, poikkeavuuksien havainnointi, uhkien tunnistaminen ja tietomurtojen pysäyttäminen. Lohkoketjutekniikkaa voidaan soveltaa datan suojaamiseen. Tekniikka voitaneen soveltaa myös kyberrakenteen semanttisen kerroksen datan suojaamiseen.

Syntaktinen kerros on teknillinen järjestelmätaso, joka pitää sisällään järjestelmien ja laitteiden ohjaus- ja hallintaohjelmat, niiden lankayhteydet ja langattomat yhteydet sekä verkkojen verkkoprotokollat, liikenteen virheenkorjaus- ja kättelymenettelyt. Oletuksena on, että jatkossa tekoälytekniikalla voidaan erilaisista digitaalisignaaleista muodostaa niihin perustuva laitteiden toiminnan kunnonvalvonta, joka palvelee myös kyberhyökkäysten havainnoinnissa. Sairaalan älykkäässä alustassa tulee huomioida erityisesti langattomiin yhteyksiin pohjautuvien laitteiden

vianilmaisu ja niiden käytön mallinnukseen perustuva vianhavaitsemisjärjestelmä. Virtualisointitekniikan avulla voitaneen suojautua tai puolustautua hyökkääjiä vastaan käyttämällä osoitealueita, joita käyttöjärjestelmässä ei ole käytettävissä. Virtualisointi mahdollistaa useiden käyttöjärjestelmien ja sovellusten toiminnan yhdellä fyysisellä palvelimella, jolloin vieraskäyttöjärjestelmä ja -sovellukset ovat eristetty muista toiminnoista. Virtualisoinnissa hyödynnetään virtualisointikomentoja, joilla käyttöjärjestelmä siirretään virtuaalikoneeksi (on-the-fly) ja lisäksi luodaan hypervisori, joka ohjaa toimintaa. Hypervisoria voidaan hyödyntää tarttumaan poikkeaviin tapahtumiin.

Fyysinen kerros pitää sisällään teknillisen laitetason, joka koostuu muun muassa sairaalalaitteista, verkkolaitteista, kuten kytkimistä ja reitittimistä, sekä niin fyysisetä kaapeloinnista kuin langattomien yhteyksien laitteista. Kerrokseen liittyvät laitetilojen suojaustarpeet sekä yksittäisten laitteiden paikantamisen ja liikuttamisen seurantatarpeet. Laitetiloja voidaan suojata kehittyneillä kulunvalvontaratkaisuilla ja laitteiden liikuttelua voidaan valvoa RFID-tekniikkaa hyödyntämällä.

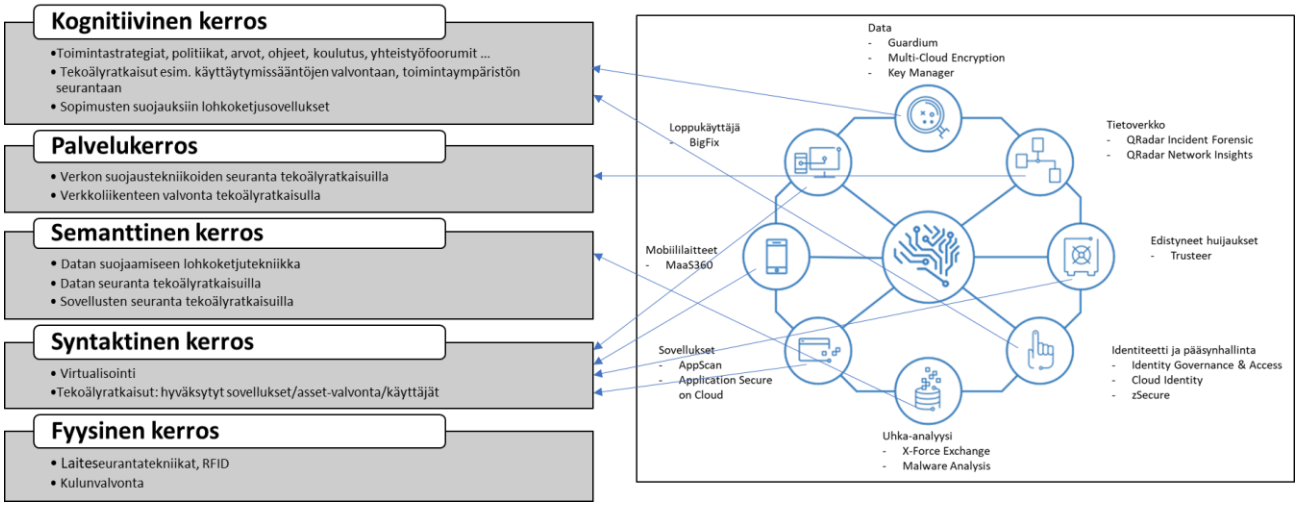
6.2.2 IBM Watson systeemitasolla

IBM kyberturvallisuuskonseptin kahdeksan eri osaa voidaan liittää viisikerroksiseen ICT-rakenteeseen oheisen kuvion 16 mukaisesti. Systeemitason tilannetietoisuus muodostuu kaikilta tasoilta saatavaan tilannekuvaan SOC:n (Security Operations Center) kautta ja on siten tärkeä osa kyberhäiriöiden torjunnassa.

Watsonin kyvykkyyksiä ovat ulkoinen tiedustelutieto (Threat Inteligence), tietoverkko (Network), edistyneet huijaukset (Advanced Fraud), identiteetti ja pääsynhallinta (Identity & Access), tietovarannot (Data), sovellukset (Apps), mobiili (Mobile) ja loppukäyttäjä (Endpoint).

Watson-ratkaisussa AI-kyvykkyyttä edustavat tietoverkkotasolla toimiva QRadar-sovellus, edistyneitä huijauksia torjumassa Trusteer-sovellus, tietovarantojen osalta Guardum-sovellus ja mobiililaitteiden hallinnassa ja suojauksessa MaaS360-ratkaisu.

Muilla osa-alueilla, ulkoinen tiedustelutieto, identiteetti ja pääsynhallinta, sovellukset ja loppukäyttäjä, ratkaisut perustuvat alueille kehitettyihin perinteisiin sujausmenetelmiin.



KUVIO 16. Suojaustekniikat ja niihin liittyvät IBM kyberturvallisuuskonseptin osat

6.3 Systeemitason suojauksen yhteenveto

Systeemitason suojauksen lähtökohtana on yhdistelmä strategisen päätöksentekotason toimenpiteitä, jotka täyttävät arkkitehtuurin (kuvio 11) vastaavan tason näkökulmien vaateet ja siten vastaavat kysymykseen ”Miksi kyberturvallisuutta on organisaatiossa edistettävä?” Samalla tapahtuu organisaation ylimmän johdon sitoutuminen kyberturvallisuuden edistämiseen. Sitoutuminen puolestaan mahdollistaa toimenpiteiden resursoinnin.

Operatiivisella päätöksentekotasolla päätöksien tarkoituksena tulee olla sairaalan toimintaprosessien jatkuvuuden varmistaminen. Tällöin tulee etsiä vastausta kysymykseen ”Mitä pitää suojata?”. Tehtävät liittyvät toiminnan ohjaukseen, jossa ensisijaisena tarpeena on linjata hyväksyttävät riskitasot ja riskien pienentämiseen liittyvät toimenpiteet niin kumppaneiden kuin oma organisaation sidosryhmien kesken. Oman organisaation toimenpiteet liittyvät toimintapolitiikkaan ja -ohjaukseen. Lääkinnällisten laitteiden turvallisuusohjelma (kts. kuvio 9) antaa suuntaviivoja yhdessä muodostettavan jaetun vastuun toteuttamiseksi. Lääkinnällisiin laitteisiin liittyvät tämän hetkiset riskit voidaan määrittää laitteen tyypin mukaan ja ne voivat vaihdella organisaation painopisteiden perusteella (kts. taulukko 2 ja taulukko 3). Laitekohtaisia hakkerointiuhkia ja niiden vaikutuksia on kuvattu liitteessä 2.

Taktisen päätöksentekotason näkökulman voi katsoa painottuvan käytännön laiteiden ja järjestelmien sekä niiden käytön suojaukseen. Tähän liittyy kysymys ”Miten suojaudutaan?”. Lähtökohtana voidaan pitää tällöin sairaalan suojattavien prosessien ja sitä kautta laitteiden ja järjestelmien tunnistamista sekä kykyä ymmärtää ja hallita niiden kyberturvallisuusriskejä. Toimenpiteet liittyvät suojaustekniikkaan ja -palveluihin. Henkilöstön kyky toimia taktisella tasolla on myös suojautumisessa ratkaisevan tärkeää. ICT-järjestelmien ja -laitteiden vyöhykesuojauksen täydentäminen uusilla teknillisillä ratkaisuilla, jotka ulottuvat niiden kyberrakenteen kaikille tasoille, edistää systeemitason suojausta taktisella tasolla.

Systeemitason kyberturvallisuuden aikaansaaminen tapahtuu parhaiten perinteistä vyöhykkeistä suojausta täydentämällä kuvion 11 arkkitehtuurin näkökulmia ja toteutusprosessin vaiheita seuraamalla tässä tutkimuksessa esille tuotujen toimenpiteiden avulla. Systeemitason tilannekuva ja sitä kautta syntyvä havaintokyky ja tilannetietoisuus muodostuu eri päätöksentekotasojen yhteisvaikutuksesta. Organisaation kyberturvallisuuden kyvykkyys ratkaisee tilannetietoisuuden muodostamisen ja hyödyntämisen.

LÄHTEET

Amir, U. 2015. U.S. Based Medical Software Company Breach Expose 4 Million People. HACKREAD:n internetsivusto. Saatavilla: 7.2.2019 https://www.hackread.com/us-medical-software-company-breach/

ASC COMMUNICATION. 2019a. Ariz. pain clinic breach affects nearly 900k patients, employees. Becker's healthcaren internetsivusto. Saatavilla: 7.2.2019 http://www.beckershospitalreview.com/healthcare-information-technology/ariz-pain-clinic-breach-affects-nearly-900k-patients-employees-providers.html

ASC COMMUNICATIONS. 2019b. Central Ohio urology group cyberattack affects 300,000 patients. Becker's healthcaren internetsivusto. Saatavilla: 7.2.2019 https://www.beckershospitalreview.com/healthcare-information-technology/central-ohio-urology-group-cyberattack-affects-300-000-patients.html

ASC COMMUNICATIONS. 2019c. Community health plan of Washington data breach affects nearly 400k. Becker's healthcaren internetsivusto. Saatavilla: 7.2.2019 https://www.beckershospitalreview.com/healthcare-information-technology/community-health-plan-of-washington-data-breach-affects-nearly-400k.html

ASC COMMUNICATIONS. 2019d. Company issuing health plan ID cards hit with data breach affecting 3.3.M. Becker's healthcaren internetsivusto. Saatavilla: 7.2.2019 https://www.beckershospitalreview.com/healthcare-information-technology/company-issuing-health-plan-id-cards-hit-with-data-breach-affecting-3-3m.html

Ayala, L. 2016. Cybersecurity for Hospitals and Healthcare Facilities – A Guide to Detection and Prevention. USA: Apress.

BBC. 2017. NHS cyber-attack: GPs and hospitals hit by ransomware. BBC:n internetsivusto. Saatavilla: 6.2.2019 http://www.bbc.com/news/health-39899646

Bisson, D. 2017. Health IT Vendor Restores EHR Access Following Ransomware Attack. Tripwire, Inc:n internetsivusto. Saatavilla: 6.2.2019 https://www.tripwire.com/state-of-security/latest-security-news/health-vendor-restores-ehr-access-following-ransomware-attack/

Bowman, D. 2016a. Feds reach $2.14 HIPAA settlement with California health system. Questexin internetsivusto. Saatavilla: 6.2.2019 https://www.fiercehealthcare.com/regulatory/ocr-reaches-2-14m-hipaa-settlement-california-health-system

Bowman, D. 2016b. Hacked hospital can't afford victim credit monitoring. Questexin internetsivusto. Saatavilla: 6.2.2019 https://www.fiercehealthcare.com/privacy-security/hacked-hospital-can-t-pay-for-victim-credit-monitoring

Bryant, M. 2016. Data for 655,000 Bon Secours patients exposed online Industry Diven internetsivusto. Saatavilla: 6.2.2019 http://www.healthcaredive.com/news/data-for-655000-bon-secours-patients-exposed-online/424480/

Černiauskas, Š. 2017. Lithuania: Cybercriminals Blackmail Plastic Surgery Clinic with Stolen Photos. OCCRP:n internetsivusto. Saatavilla: 6.2.2019 https://www.occrp.org/en/daily/6387-lithuania-cybercriminals-blackmail-plas

Conner-Simons, A. 2016. System predicts 85 percent of cyber-attacks using input from human experts. MIT Newsin internetsivusto. Saatavilla: 6.2.2019 http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

Csulak, E., Meadows, T., Corman, J., DeCesare, G., Fernando, A., Finn, D., Jarrett, M., Laybourn, L., McNeil, M., McWhorte, D., Mellinger, R., Monson, J., Radadoos, R., Rice, T., Sardanopoli, V., Suarez, R., Stine, K., Sublett, C., Thompson, L., Ting, D. & Trotter, F. 2017. Report on improving cybersecurity in the health care industry. Health care industry cybersecurity task force-raportti. Saatavilla: 6.2.2019 https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

Daim, X. 2017. From model, signal to knowledge data-driven condition monitoring and attack detection in 4G Industrial Systems, SPS NATO PROJECT G5172. Northumbria University Newcastle, UK. Julkaisematon konferenssiesitelmä 19.10.2017.

DataBreaches.net. 2016. Baltimore addiction treatment clinic hacked; patients' info up for sale on dark web (UPDATED). DataBreaches.netin internetsivusto. Saatavilla: 6.2.2019 https://www.databreaches.net/baltimore-addiction-treatment-clinic-hacked-patients-info-up-for-sale-on-dark-web/

DataBreaches.net. 2017a. Attackers claim to have hacked MEDHOST (UPDATED). DataBreaches.netin internetsivusto. Saatavilla: 6.2.2019 https://www.databreaches.net/attackers-claim-to-have-hacked-medhost/

DataBreaches.net. 2017b. Chase Brexton Health Care notifies more than 16,000 patients after phishing incident. DataBreaches.netin internetsivusto. Saatavilla: 6.2.2019 www.databreaches.net/chase-brexton-health-care-notifies-more-than-16000-patients-after-phishing-incident/

DataBreaches.net. 2017c. Washington Health System Greene notifies 4,145 patients after hard drive with PHI was discovered stolen. DataBreaches.netin internetsivusto. Saatavilla: 6.2.2019 https://www.databreaches.net/washington-health-system-greene-notifies-4145-patients-after-hard-drive-with-phi-was-discovered-stolen/

Davis, J. 2016. Cyberattack at Appalachian Regional Healthcare keeping EHR down after six days. Healthcare IT Newsin internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareitnews.com/news/cyberattack-appalachian-regional-healthcare-keeping-ehr-down-after-six-days

Davis, J. 2017. Urology Austin ransomware attack may have exposed more than 279,000 patient records. Healthcare IT Newsin internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareitnews.com/news/urology-austin-ransomware-attack-may-have-exposed-more-279000-patient-records

Davis, J. 2018. Allscripts sued over ransomware attack, accused of 'wanton' disregard. Healthcare IT Newsin internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareitnews.com/news/allscripts-sued-over-ransomware-attack-accused-wanton-disregard

Destre, E. 2018. Risks and Advantages in using Artificial Intelligence on Cyber Defence and Cyber Attack. Cyber Defence in Industry 4.0 Systems and Related Logistics an IT Infrastructures. *The NATO Science for Peace and Security Series. D: Information and Communication Security 51.*

ENISA. 2012. ENISA Threat Landscape Responding to the Evolving Threat Environment-raportti. European Network and Information Security Agency.

ENISA. 2016. Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures. ENISA:n raportti. Saatavilla: 6.2.2019 https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Falco, C. 2016. Unleashing the Immune System: How to Boost Your Security Hygiene. IBM:n internetivusto. Saatavilla: 6.2.2019 https://securityintelligence.com/news/unleashing-the-immune-system-how-to-boost-your-security-hygiene/

Finnish News Network. 2017. Denial-of-service attacks snap Kela services. Finnish News Networkin internetsivusto. Saatavilla: 6.2.2019 http://www.dailyfinland.fi/national/966/Denial-of-service-attacks-snap-Kela-services

FireEye. 2016. Mandiant Consulting - M-Trends 2016. Special report 2016. Saatavilla: 6.2.2019 https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf

Gold, A. 2013. Stolen computers risks info for 4 million patients. Questexin internetsivusto. Saatavilla: 6.2.2019 http://www.fiercehealthcare.com/it/stolen-computers-risk-info-for-4-million-patients

Goud, N. 2019. Cyber Attack on Emory Healthcare compromises 80K patient records. Cybersecurity Insidersin internetsivusto. Saatavilla: 6.2.2019 http://www.cybersecurity-insiders.com/cyber-attack-on-emory-healthcare-compromises-80k-patient-records/

Grimes, S. T. 2016. Part 1 of 3: Best Practices for Medical Device Cybersecurity Management. *CE-IT Collaboration Town Hall Series 23 - 24*. Saatavilla: 6.2.2019 https://docplayer.net/35473652-Part-1-of-3-best-practices-for-medical-device-cybersecurity-management.html

Groden, C. 2015. This big U.S. health insurer just got hacked. Cybersecurityn internetsivusto. Saatavilla: 6.2.2019 http://fortune.com/2015/09/10/hack-health-insurer-bluecross/

HACKREAD. 2015. Massive US Healthcare Company Hacked, 1.1 million customers affected. HACKREAD:n internetsivusta. Saatavilla: 6.2.2019 https://www.hackread.com/us-healthcare-company-hacked/

HACKREAD. 2016. Central Ohio Urology Group Hacked; 223GB of Crucial Data Leaked (Updated). HACKREAD:n internetsivusta. Saatavilla: 6.2.2019 https://www.hackread.com/central-ohio-urology-group-hacked/

Halonen, P. 2016. Kyberturvallisuus terveydenhuollossa. Viestintäviraston kyberturvallisuuskeskuksen PowerPoint-esitys. Saatavilla: 6.2.2019 https://docplayer.fi/25743256-Kyberturvallisuus-terveydenhuollossa-perttu-halonen-helsinki.html

Heitmann, B. 2017. Secure Multi-Party Computation (SMPC) on Secret Data. SPS NATO PROJECT G5172. Fraunhofer FIT, RWTH Aachen University, Germany. Julkaisematon konferenssiesitelmä 18.10.2017.

HHS. 2017. Lack of timely action risks security and costs money. HHS:n internetsivusto. Saatavilla: 6.2.2019 https://www.hhs.gov/about/news/2017/02/01/lack-timely-action-risks-security-and-costs-money.html

Homewood, B. 2017. IAAF says medical records compromised by Fancy Bear hacking group. Reutersin internetsivusto. Saatavilla: 6.2.2019 http://in.reuters.com/article/us-sport-doping-iaaf-idINKBN1750ZM

Hundley, R. 0. & Anderson, R. H. 1995. Emerging Challenge: Security - and Safety in Cyberspace. *IEEE Technology and Society,* 19 - 28. Saatavilla: 6.2.2019 https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch10.pdf

Hunt, R. 2016. The Red Cross Blood Service: Australia's largest ever leak of personal data. Troy Huntin blogi. Saatavilla: 6.2.2019 https://www.troyhunt.com/the-red-cross-blood-service-australias-largest-ever-leak-of-personal-data/

IBM Security. 2017. IBM X-Force Threat Intelligence Index 2017 - The year of the mega breach. IBM X-Force Threat Intelligence Index 2017.n PowerPoint-esitys.

Integrating the Healthcare Enterprise. 2015. IHE Patient Care Device (PCD) White Paper 10 Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide. Integrating the Healthcare Enterprisen raportti. Saatavilla: 6.2.2019 http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf

Johnson, A., Dempsey, K., Ross, R., Sarbari, G., S. & Bailey, D. 2011. Guide for Security-Focused Configuration Management of Information Systems. National Institute of Standards and Technologyn Information security -raportti. Saatavilla: 6.2.2019 https://www.govinfo.gov/content/pkg/GOVPUB-C13-63e84ab7af43b36228f10e4f0b5f8c38/pdf/GOVPUB-C13-63e84ab7af43b36228f10e4f0b5f8c38.pdf

Kallio, H. 2016. Sairaalalaitteiden turvallisuus. Julkaisematon raportti. Cyber trust- projekti.

KnowBe4. Social Engineering Causes Seattle Hospital 90K Databreach. KnowBe4:n internetsivusto. Saataville: 6.2.2019 https://blog.knowbe4.com/bid/356162/Social-Engineering-Causes-Seattle-Hospital-90K-Databreach

Krishnan, R. 2016. Ransomware attacks on Hospitals put Patients at Risk. Hacker Newsin internetsivusto. Saatavilla: 6.2.2019 http://thehackernews.com/2016/04/hospital-ransomware.html

Kumar, M. 2016. Hundreds Of Operations Canceled After Malware Hacks Hospitals Systems. The Hacker Newsin internetsivusto. Saatavilla: 6.2.2019 http://thehackernews.com/2016/11/hospital-cyber-attack-virus.html

Landi, H. 2017. Media Reports: Virus Shuts Down Erie County Medical Center's Computer System. Cybersecurityn internetsivusto. Saatavilla: 6.2.2019 https://www.healthcare-informatics.com/news-item/cybersecurity/media-reports-virus-shuts-down-erie-county-medical-center-s-computer-system

LaPointe, J. 2016a. Bizmatics healthcare data breach affects another 22k patients. Xtelligent Healthcare Media, LLC:n internetsivusto. Saatavilla: 6.2.2019 http://healthitsecurity.com/news/bizmatics-healthcare-data-breach-affects-another-22k-patients

LaPointe, J. 2016b. Hackers Access EHR Data in Potential Healthcare Data Breach. Xtelligent Healthcare Media, LLC:n internetsivusto. Saatavilla: 6.2.2019 https://healthitsecurity.com/news/hackers-access-ehr-data-in-potential-healthcare-data-breach

Lehto, M. 2014. Kybertaistelu ilmavoimaympäristössä. Teoksessa T. Kuusisto (toim.), *Kybertaistelu 2020, (157 - 178).* Taktiikan laitos Julkaisusarja 2, No. 1/2014. Helsinki: Maanpuolustuskorkeakoulu.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, P., Rusi, T. & Salminen, M. 2017. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017.

Lehto, M. Phenomena in the Cyber World. 2015. Teoksessa M. Lehto & P. Neittaanmäki. *Cyber Security: Analytics, Technology and Automation, (3 - 29)*. USA: Springer.

Liaropoulos, A. 2010. War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory. *Proceedings of the 9th European Conference on Information Warfare and Security, the Department of Applied Informatics University of Macedonia Thessaloniki Greece 1 - 2,* (177 - 182).

Libicki, M. C. 2007. Conquest in Cyberspace – National Security and Information Warfare. New York: Cambridge University Press.

McGee, M.K. 2016. Cancer Center Chain Faces Multiple Breach Lawsuits. Information Security Media Group, Corp:n internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareinfosecurity.com/cancer-center-chain-faces-multiple-breach-lawsuits-a-9007

Meditology Services LLC. 2017. Hijacking Your Life Support: Medical Device Security. Saatavilla: 6.2.2019 https://www.meditologyservices.com/fullpanel/uploads/files/whitepaper-medical-device-security-2017.pdf

Miliard, M. 2016. Flint hospital hit with cyber attack after hacker group Anonymous promises action on water crisis. Healthcare IT Newsin internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareitnews.com/news/flint-hospital-hit-cyber-attack-after-hacker-group-anonymous-promises-action-water-crisis

Monegain, B. 2016a. Hackers hit two California hospitals with ransomware. Healthcare IT Newsin internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareitnews.com/news/hackers-hit-two-california-hospitals-ransomware

Monegain, B. 2016b. Methodist Hospital recovering from five day ransomware attack, claims it did not pay up. Healthcare IT Newsin internetsivusto. Saatavilla: 6.2.2019 http://www.healthcareitnews.com/news/methodist-hospital-recovering-five-day-ransomware-attack-claims-it-did-not-pay

Morley, N. 2017. Hackers have stolen data from a cosmetic surgery clinic used by the rich and famous. Associated Newspapers Limitedin internetsivusto. Saatavilla: 6.2.2019 https://metro.co.uk/2017/10/24/hackers-have-stolen-data-from-a-cosmetic-surgery-clinic-used-by-the-rich-and-famous-7023893/

MTV Uutiset. 2016. Palvelunestohyökkäys lamautti Kanta-palvelut: "Vakava häiriö". MTV Uutisten internetsivusto. Saatavilla: 6.2.2019 http://www.mtv.fi/uutiset/kotimaa/artikkeli/palvelunestohyokkays-lamautti-kanta-palvelut-vakava-hairio/6119086

Murawski, J. 2017. 24,000 UNC Health Care patients affected by potential security breach. The News & Observerin internetsivusto. Saatavilla: 6.2.2019 https://www.newsobserver.com/news/business/article188757969.html

National Institute of Standards and Technology. 2018. Framework for Improving Critical Infrastructure Cybersecurity version 1.1. Saatavilla: 6.2.2019 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Pagliery, J. 2014. Hospital network hacked, 4.5 million records stolen. Cable News Networkin internetsivusto. Saatavilla: 6.2.2019 http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/

Pagliery, J. 2015. UCLA Health hacked, 4.5 million victims. Cable News Networkin internetsivusto. Saatavilla: 6.2.2019 http://money.cnn.com/2015/07/17/technology/ucla-health-hack/index.html

Palmer, D. 2017. 'Previously unseen' malware behind cyberattack against UK's biggest hospital group. Saatavilla: 7.2.2019 http://www.zdnet.com/article/previously-unseen-malware-behind-cyberattack-against-uks-biggest-hospital-group/

Paloniemi, S.2008. Tietojärjestelmien käytön ongelmia suomalaisessa terveydenhuollon työssä. Tietojenkäsittelytieteen kandidaatintutkielma. Jyväskylän yliopisto. Saatavilla: 6.2.2019 https://jyx.jyu.fi/bitstream/handle/123456789/20051/Satu.Paloniemi.pdf?sequ

Pekkarinen, T. 2016. Kyberturvallisuus sairaaloiden eri toimialoilla. Pohjois-Savon sairaanhoitopiiri Sairaanhoitopiirien kyberturvallisuusseminaari, 19.10.2016. Saatavilla: 7.2.2019 http://ssty.fi/download/valmiusseminaari19102016/Pekkarinen_kybertuvallisuus_sairaalan_eri_toimialoilla.pdf

Piggin, R. 2017. Cybersecurity of medical devices - Addressing patient safety and the security of patient health information. BSI:n raportti. Saatavilla: https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf

Pilieci, V. 2016. Ottawa Hospital hit with Ransomware, information on four computers locked down. Postmedia Network Inc:n internetsivusto. Saatavilla: 7.2.2019 http://www.ottawasun.com/2016/03/13/ottawa-hospital-hit-with-ransomware-information-on-four-computers-locked-down

Pirkkalainen, S. Virtuaalivaluuttaa louhiva haittaohjelma saastutti Lahden kaupungin tietojärjestelmän – terveyskeskukset ruuhkautuivat. Ylen internetsivusto. Saatavilla: 7.2.2019 https://yle.fi/uutiset/3-10066289

PricewaterhouseCoopersin (PwC). 2016. Industry 4.0: Building the digital enterprise. PwC:n raportti. Saatavilla: 7.2.2019 https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf

Radware Ltd. 2018. DDoS Case Study: DDoS Attack Mitigation Boston Children's Hospital. Radware Ltd:n internetsivusto. Saatavilla: 6.2.2019 https://security.radware.com/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/

Rissanen, J. & Koivuranta, E. 2016. Verkkorikolliset tunkeutuvat sairaalan verkkoon, lukitsevat tiedostoja ja vaativat rahaa – Ovatko tietoni turvassa?. Ylen internetsivusto. Saatavilla: 6.2.2019 http://yle.fi/uutiset/3-8904018

Ruohan, L. 2016. Info of 200,000 babies leaked, causes panic among parents. Global Timesin internetsivusto. Saatavilla: 6.2.2019 http://www.globaltimes.cn/content/977702.shtml

Sadeghi, A. R., Wachsmann, C. & Waidner, M. 2015. Security and privacy challenges in industrial internet of things. *Proceedings DAC '15 Proceedings of the 52nd Annual Design Automation Conference, 54* (1 - 6).

Saranto, K. & Korpela, M. (toim.) 1999. Tietotekniikka ja tiedonhallinta sosiaali- ja terveydenhuollossa. Helsinki: Sanoma Pro Oy.

Sartonen, M., Huhtinen, A-M. & Lehto, M. 2016. Rhizomatic Target Audiences of the Cyber Domain. *Journal of Information Warfare, 15(4),* 1 - 13. Saatavilla: 6.2.2019 https://toinformistoinfluence.com/2016/12/31/journal-of-information-warfare-volume-14-issue-4-fall-16-is-out/

Savolainen, J. 2017. TYKS joutui kyberhyökkäyksen kohteeksi - tietohallintojohtaja: "Järjestäytynyttä rikollisuutta". Iltalehden internetsivusto. Saatavilla: 6.2.2019 http://www.iltalehti.fi/digi/20170609220019698 8_du.shtml

Siwicki, B. 2016. Healthcare staff lacking in basic security awareness, putting medical infrastructure at risk. HIMSS Median internetsivusto. Saatavilla: 6.2.2019 https://www.healthcareitnews.com/news/study-healthcare-staff-lacking-basic-security-awareness-putting-medical-infrastructure-risk

Snell, E. 2016a. Banner Health Data Breach Affects 3.7M Records. Xtelligent Healthcare Media, LLC:n internetsivusto. Saatavilla: 6.2.2019 http://healthitsecurity.com/news/banner-health-data-breach-affects-3.7m-records

Snell, E. 2016b. Cybersecurity Attacks Leading 2016 Data Breach Cause. Xtelligent Healthcare Media, LLC:n internetsivusto. Saatavilla: 6.2.2019 https://healthitsecurity.com/news/cybersecurity-attacks-leading-2016-data-breach-cause

Ms. Smith. 2016. Kansas heart hospital hit with ransomware; attackers demand two ransoms. IDG Communications, Inc:n internetsivusto. Saatavilla: 6.2.2019 https://www.csoonline.com/article/3073495/data-protection/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html

State of California. 2019. California correctional health care services (CCHCS). State of Californian internetsivusto. Saatavilla: 6.2.2019 http://www.cphcs.ca.gov/docs/press/Release%20-%20Potential%20Breach%20PHI.pdf

Steffen, S. 2016. Hackers hold German hospital data hostage. Deutsche Wellen internetsivusto. Saatavilla: 6.2.2019 http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030

Storm, D. 2015. MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. IDG Communications, Inc:n internetsivusto. Saatavilla: 6.2.2019 http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

Suomen Automaatioseura ry turvallisuusjaosto. 2010. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. 1. painos. Saatavilla: 6.2.2019 https://zapdoc.site/queue/teollisuusautomaation-tietoturva-verkottumisen-riskit-ja-nii.html

Suomen Standardisoimisliitto SFS ry. 2012. SFS-käsikirja 327. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Helsinki: SFS ry.

Suomen Standardisoimisliitto SFS ry. Standardi tutuksi. Standardisoimisliitto SFS ry:n internetsivusto. Saatavilla: 6.2.2019 http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi

Symantec Corporatio. 2016. Symantec, Industry Focus: Medical Device Security. Symantec Corporation internetsivusto. Saatavilla: 6.2.2019 https://www.symantec.com/content/dam/symantec/docs/data-sheets/symc-med-device-security-en.pdf

Terhune, C. 2015. Anthem hack exposes data on 80 million; experts warn of identity theft. Los Angeles Timesin internetsivusto. Saatavilla: 6.2.2019 http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html

The Farber Law Group. 2013. Confidential data of 90,000 UW Medicine patients compromised. The Farber Law Groupin internetsivusto. Saatavilla: 6.2.2019 https://www.washingtoninjuryattorneyblog.com/2013/12/confidential_data_of_90000_uw.html

The Deloitte Center for Health Solutions. 2013. Issue Brief: Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives. Deloitten internetsivusto. Saatavilla: 6.2.2019 https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-networked-medical-device.pdf

Valtiovarainministeriö. 2009. 5 Kuinka välttää tartunta. Varainministeriön internetsivusto. Saatavilla: 6.2.2019 www.vahtiohje.fi/web/guest/kuinka-valttaa-tartunta

Varsinais-Suomen sairaanhoitopiiri. 2015. Tietokonevirus torjuttu sairaanhoitopiirin tietoverkossa. Varsinais-Suomen sairaanhoitopiirin internetsivusto. Saatavilla: 6.2.2019 http://www.vsshp.fi/fi/sairaanhoitopiiri/media-tiedotteet-viestinta/tiedotteet/Sivut/tietokonevirus-torjuttu.aspx

Veeramachaneni, K., Arnaldo, I., Cuesta-Infante, A., Korrapati, V., Bassias, C. & Ke, L. 2016. AI2: Training a big data machine to defend. *Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference,* 9 - 10.

Vinton, K. 2015. Premera Blue Cross Breach May Have Exposed 11 Million Customers' Medical And Financial Data. Forbesin internetsivusto. Saatavilla: 6.2.2019 https://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach

World Health Organization. 2011. Core Medical Equipment. World Health Organization internetsivusto. Saatavilla: 6.2.2019 https://apps.who.int/iris/bitstream/handle/10665/95788/WHO_HSS_EHT_DIM_11.03_eng.pdf?sequence=1

Zaidenberg, N. J. 2018. Hardware rooted security in Industry 4.0 systems. Cyber Defence in Industry 4.0 Systems and Related Logistics an IT Infrastructures. *The NATO Science for Peace and Security Series. D: Information and Communication Security 51.*

Zhang, Y., Qui, M., Chun-Wei, T., Hassan, M. M. & Alamri, A. 2017. Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. *IEEE Systems Journal, 1* (88 - 95).

LIITE 1: Lääkintälaitteet

Analyzer, Laboratory, Hematology, Blood Grouping, Automated
Anesthesia Unit
Apnea Monitors
Aspirator
Auditory Function Screening Device, Newborn
Bilirubinometer
Blood Gas/pH/Chemistry Point of Care Analyzer
Blood pressure monitor
Bronchoscope
Cataract Extraction Units
Clinical Chemistry Analyzer
Colonoscope
Cryosurgical Unit
Cytometer
Defibrillator, External, Automated; Semi-automated
Defibrillator, External, Manual
Densitometer, Bone
Electrocardiograph, ECG
Electrosurgical Unit
Fetal Heart Detector, Ultrasonic
Fetal monitor
Glucose Analyzer
Hematology Point of Care Analyzer
Hemodialysis Unit
Immunoassay Analyzer
Incubator, Infant
Information
Laser, CO2
Laser, Ophthalmic
Mammography unit
Monitor, Bedside, Electroencephalography
Monitor, Central Station
Monitoring System, Physiologic
Monitor, Telemetric, Physiologic
Peritoneal Dialysis Unit
Pulmonary function analyzer
Radiographic, Fluoroscopic System
Radiotherapy Planning System

Radiotherapy Systems
Remote-afterloading brachytherapy system
Scanning System, CT
Scanning System, Magnetic Resonance Imaging, Full-Body
Scanning System, Ultrasonic
Transcutaneous Blood Gas Monitor
Ventilator, Intensive Care
Ventilator, Intensive Care, Neonatal/Pediatric
Ventilator, Portable
Videoconferencing system, Telemedicine
Warming Unit, Radiant, Infant
Whole Blood Coagulation Analyzer

(World Health Organization, 2011, 1 - 2.)

LIITE 2: Lääkintälaitteiden kyberominaisuuksia

Cyber Trust tutkimushankkeen yhteydessä Keski-Suomen sairaanhoitopiirille tehdyssä sairaalalaitteiden turvallisuuskatsauksessa kerättiin sairaalalaitteiden turvallisuuskatsauksessa tietoa 18:n laitteen hyökkäysvektoreista ja mahdollisista suojausjärjestelmistä, kuten salauksista. Hyökkäysvektori on väylä, jonka kautta hyökkääjä voi saada yhteyden laitteeseen ja mahdollisesti saada sen haltuunsa. Tutkimuksen erityisenä kiinnostuksen kohteena oli verkkoliitynnät, paikallinen verkottuminen, muut laitteiden liitynnät ja WLAN-yhteys hyökkäysvektoreina. Liitynnöistä ehkä tärkeimmän hyökkäysvektorin muodostaa USB-portti. Saastuneella muistitikulla voi halutun viruksen saada laitteeseen väliaikaisellakin yhdistämisellä. Lisäksi tutkimuksessa mainitaan hyökkäysvektorina SD-muistikortin käyttö. Langattomien laitteiden murtaminen tai niiden toiminnan häiritseminen ei välttämättä vaadi samassa tilassa olemista, joten hyökkääjä voi toimia verrattain salassa. Lisäksi WLAN-verkon kuuntelemiseen ja sen kautta hyökkäämiseen on valmiita työkaluja, jotka madaltavat kynnystä hyökkäyskokeiluihin. Langattoman verkon avulla voidaan esimerkiksi salakuunnella potilastietoja tai tehdä Man in the Middle -hyökkäys, jossa hyökkääjä välittää kaiken datan kohteen ja sen käyttämän tukiaseman välillä ja mahdollisesti muuttaa viestejä tarpeensa mukaan. Lisäksi laitteeseen voidaan saada yhteys, jonka avulla sitä voidaan hallita. Sammuttaminen, järjestelmän tekeminen toimintakyvyttömäksi tai järjestelmän hallittu käskyttäminen ovat mahdollisia hakkeroinnin tuloksia. Haltuun ottamisen helppouteen vaikuttaa edellä mainittujen hyökkäysvektoreiden lisäksi laitteen tietojärjestelmän rakenne. Jos käytössä on yleinen käyttöjärjestelmä, on hyökkääjän helpompi hyödyntää aikaisempaa kokemusta ja valmiita työkaluja muodostaakseen niistä hyökkäysvektorin käyttöjärjestelmään. Toisaalta on kuitenkin hyödyllistä muistaa, että valmiissa käyttöjärjestelmissä tietoturvaa on todennäköisesti koeteltu ja paranneltu enemmän kuin alusta alkaen laitteelle räätälöidyssä järjestelmissä. (Kallio, 2016.)

Tutkimuksessa mainitaan eräänä laitteiden liityntöihin liittyvistä esimerkkilaitteista EKG-piirturit (GE, 3500), jotka pitävät sisältää SD-muistikorttipaikkoja. Em. laitetyypissä ohjelmistopäivitykset asennetaan kortin avulla, jolloin vaikkapa uuden ohjelmiston asentaminen korttia vaihtamalla on maininnan arvoinen reitti laitteen tietojärjestelmiin myös hyökkäystarkoituksissa. Korttipaikka on laitteen näytön takana ja helposti saavutettavissa. Esimerkkitapauksessa hyökkäysvektorin avulla voi saada haltuunsa potilastietoja. (Kallio, 2016.)

Kaikissa tutkituista laitteissa ei ole WLAN-yhteyttä, mutta joissakin niistä voidaan käyttää erilaisia adaptereita tämän ominaisuuden saamiseksi. Tutkituista laitteista vain kolmen laitteen WLAN-salauksesta löytyi käsikirjatietoa. Niistä löytyi laite (Drägerin Infinity Delta), jonka kaikki versiot tukevat salaamatonta liikennettä tai WEP-salausta. WEP-salauskin on helposti murrettavissa ja, jotta laite käyttäisi turvallista WPA2-salausta, tulee laitteessa olla asennettuna erillinen ohjelma (nimeltä VR8). Vastaava esimerkki löytyy eräästä EKG-piirturilaitteesta (Schillerin Cardiovit AT-102+), jossa langaton verkkoyhteys on valinnainen ominaisuus. Turvallinen valinta tulee osata tehdä useiden turvallisuusominaisuuksiltaan erilaisten salausmenetelmien välillä (WEP, WPA, WPA2).

Joissain tapauksissa laitteita voidaan yhdistää langattomaan verkkoon erillisillä hyvää salausta tukevilla adaptereilla (Silex), jolloin adapterilla voidaan hoitaa sekä liikenteen salaus, että autentikointi kattavasti. (Kallio, 2016.)

Viitetutkimuksessa mukana olleissa kahdessa ultraäänilaitteessa (GE Healthcare:n LOGIQ P9 ja Philipsin EPIQ 5c) oli WLAN-valmius, mutta kummankaan laitteen ohjekirjasta ei löydy tietoa niiden liikenteen salauksista. Philipsin valmistama laite sisältää kuitenkin palomuurin ja virustentorjuntaohjelman. Lisäksi laitteessa on potilastietojen salausmahdollisuus. Tämän päivä IoT-laitteiden tavoin laitteeseen voidaan muodostaa etäyhteys valmistajan tukipalveluista. Tukipalveluiden tarpeellisuuden ohessa etäyhteys voi myös sisältää hyökkäysvektorinmahdollisuuden. Yleisesti ottaen etäyhteys, jonka ulkopuolinen voi helposti muodostaa, on todella houkutteleva ominaisuus hyökkääjälle. Ultraäänilaitteissa on myös USB-portteja, joita voidaan hyödyntää hyökkäysvektoreina. (Kallio, 2016.)

Verkkoliityntään tai paikalliseen verkottumiseen tutkimuksessa mukana olleista laitteista löytyvät esimerkit mm. potilasmonitorista. Ne sisältävät useita mahdollisuuksia hyökkäysvektoreille. Verkkoliityntään käytettävä Ethernet-portti löytyy Philipsin potilasmonitorista (Intellivie MX800). Sen muina ulkoisina liityntöinä ovat viisi USB porttia ja WLAN-yhteys. WLAN-yhteydestä ei ole saatavilla tarkempaa tietoa, joten se voi olla erikseen tilattava lisäominaisuus. Em. esimerkkilaitteen käyttöjärjestelmä voi olla joko Windows 7 tai XP. Toisessa esimerkkimonitorissa (GE:n potilasmonitori Carescape B850) on Linux-käyttöjärjestelmä, LAN-yhteyteen kahden portin kautta, USB-porttia ja kaksi sarjaporttia. Näiden kahden esimerkkilaitteen haavoittuvuudet liittyvät käyttöjärjestelmiin ja ulkoisiin liityntöihin. Kolmas esimerkkimonitori (Drägerin Infinity Deltan) pitää sisällään haavoittuvuuden suojaustasoltaan puutteellisen WLAN-yhteyden kautta (WEP-salaus, VR8-ohjelmistoa) ja lisäksi laite pystyy muodostamaan yhteyden erittäin moneen muuhun laitteeseen erilaisten liittymiensä ansiosta. Monet yhdistettävistä laitteista ovat laitevalmistajan omia tuotteita. Näistä hyvänä esimerkkinä toimii telemetrialähetin (TelesSmart M300), joka voi muodostaa langattoman yhteyden erilliseen keskusyksikköön (Infinity). Keskusyksiköstä voidaan lähettää päälaitteelle (TeleSmart) käsky pitää ääntä, jotta se voidaan paikallistaa. Paikallistamisäänen pyyntö voi toimia hyökkäysvektorina laitteelle, jolloin sen toimintaa voidaan häiritä ja hämmentää käyttäjiä. (Kallio, 2016.)

Muista tutkimuksessa olleista laitteista voidaan todeta seuraavaa (Kallio, 2016):

- Liikuteltavia röntgenlaitteita (Ziehman RFD ja Fuji FDR Go) voidaan myös yhdistää langattomaan verkkoon erillisillä adaptereilla, mutta tutkimuksessa mukana olleista laitteiden salausmenetelmistä ei ollut käytettävissä ohjekirjatietoa.
- Radiometerin verikaasuanalysaattori (ABL90 FLEX) ei yhdisty langattomaan verkkoon, mutta LAN verkkoon kylläkin. Lisäksi siinä on kolme USB-porttia ja sarjaportteja. Sen käyttöohjeissa todetaan, että laitteen tiedot voi varmuuskopioida CD-levylle tai USB-massamuistilaitteelle, mutta muuta mainintaa levynlukijasta ei ole. Analysaattori ei ole

tutkimuksen ainut esimerkkilaite, josta puuttuvat käytön ja erityisesti kyberturvallisuuden kannalta katsoen tärkeät ohjekirjatiedot.

- Ruiskupumpputelakka (Injectomat MC Agilia) ei sisällä valmiuksia kommunikointiin minkään muun kuin erillisen verkkokommunikointiin tarkoitetun Link+-yksikön kautta. Laitteita voidaan laittaa useita tähän yhteen yksikköön ja se kommunikoi infrapunan avulla ruiskupumpputelakoiden kanssa. Link+ puolestaan muodostaa verkkoyhteydessä muuhun maailmaan. Link+-yksikköön voi olla yhteydessä mini USB-, sarja- tai Ethernet-portin kautta. Kaikki vaativat hyökkääjältä fyysistä yhteyttä laitteeseen. Lisähuoli voi olla uudelleenkäynnistyspainikkeesta, jonka kyllä kerrotaan olevan suojattu. Laitteen uudelleenkäynnistys on kuitenkin huomionarvoinen häirinnän keino.
- Kuvalevyjen lukulaitteet (Agfan CR 85-X, Soredexin Digora Optime, Fujin Capsula XL) eivät voi liittyä langattomaan verkkoon, mutta kaksi ensimmäistä esimerkkilaitetta (Agfan CR 85-X ja Soredexin Digora Optime) sisältävät Ethernet-portin. Jälkimmäisin esimerkkilaite välittää kuvansa erilliselle konsolille, josta kuvia voi tarkastella ja mahdollisesti lähettää eteenpäin mm. tulostimille tai palvelimille (DICOM-muotoisena, Digital Imaging and Communications in Medicine). Keskimmäisen esimerkkilaitteen käyttöohje kehottaa käyttämään palomuuria ja virustentorjuntaohjelmaa.

Kuvantaminen (MRI)

Yleisin uhka MRI-kuvantamislaitteen turvallisuudelle realisoituu, kun staattinen magneettikenttä vetää metalliesinettä puoleensa. Yleisesti ottaen MRI-laitteita pidetään hyvin turvallisina, mutta mikäli hakkeri kykenee peukaloimaan MRI-kuvantamislaitteen kontrolleja, voi henkilö joutua törmäys- tai loukkaantumisriskeihin, jotka voivat johtua esimerkiksi jonkinlaisen metalliesineen puoleensa vetämisestä. MRI-kuvantamislaite voi myös vahingoittua esimerkiksi nopeasti kiihtyvien esineiden vaikutuksesta ja nämä hyvin vahvan magneettikentän aiheuttamat onnettomuudet, jossa laitteen magneettikentän keskus vetää puoleensa ferromagneettisia esineitä puoleensa, ovat aiheuttaneet loukkaantumisia ja kuolemantapauksia. Eräässä tapauksessa kuusivuotias poika kuoli MRI-kuvantamisen aikana, laitteen vetäessä happisäiliötä puoleensa huoneen toiselta puolelta ja iskien sen voimalla kohti pojan päätä. MRI voi irrottaa asennettuja laitteita, lämmittää laitteita radiotaajuuksien avulla tai sumentaa kuvantamisen aikana kuvattuja kuvia. Tästä johtuen kaikki passiiviset implantit on merkitty tietynlaisella informaatiolla koskien niiden käyttöä magneettikuvausympäristössä. Peukaloimalla kuvantamisparametreja, kuten toistoaika (Repetition Time eli TR) ja kaikuaika (Echo Time eli TE), viipaleiden lukumäärät ja paksuudet, kääntökulmat tai vokseleiden koko, hakkeri voi saattaa kuvantamislaitteen epäluotettavaan tilaan ja mahdollisesti aiheuttaa potilaiden loukkaantumisia. (Ayala, 2016, 21 - 22.)

Taulukossa 4 havainnollistuvat mahdolliset MRI-laitteeseen kohdistuvat kyber-fyysiset hyökkäykset:

TAULUKKO 4 Mahdollisia MRI-kuvantamislaitteeseen kohdistuvia hyökkäyksiä (Ayala, 2016, 21)

Haitallinen hakkeritoiminta	Seuraukset
Huijata MRI-kuvantamislaitetta siten, että se sammuttaa magneettikentän	MRI-kuvantamislaite lakkaa toimimasta kentän sammuessa
Ohittaa MRI-kuvantamislaitteen magneettikentän vahvuus	Potilaat voivat kärsiä kudoksien lämpenemisestä tai palovammoista. Lisäksi vahingot laitteelle ovat mahdollisia
Saada laite siirtämään enemmän virtaa kuin ydin on suunniteltu kestämään	MRI-laitteen tai muiden elektroniset laitteiden vahingot tai tuho mahdollinen
Hiljentää kaikki hälytykset	Tekniset asiantuntijat eivät ole tietoisia vaarallisista tilanteista
MRI-laitteen kytkeminen pois päältä, sisäisten tiedostojen salaaminen	Häiritsee MRI-kuvantamisoperaatioita. Lunnaita MRI-laitteen avaamiseksi voidaan vaatia
Vaihtaa näytön informaatiota	Aiheuttaa sekaannusta protokollan suhteen
Saa MRI:n hälyttämään satunnaisesti	Häiritsee MRI-kuvantamisoperaatiota
Uudelleen käynnistää laitteen	Pyyhkii pois konfiguraatioasetukset
Yhdistää jonkun potilaan kuvantamistiedosto toisen potilaan vastaavaan	Diagnoosi toimitetaan väärälle potilaalle

PET-tomografia

PET-laite on ydinlääketieteen funktionaalinen kuvantamisteknologia, jota käytetään potilaiden metabolisten prosessien tarkkailemiseen. PET-kuvantamista käytetään muun muassa neurologiassa, jossa sillä mitataan aivojen toiminnan aktiivisuutta, joka voidaan havaita aivojen aktiivisten osien verenkierron vilkastumisesta ja glukoosin käytön kasvusta. PET-kuvausta hyödynnetään myös syöpätautien alueella etsittäessä elimistössä olevaa syöpää tai sen lähettämiä etäpesäkkeitä. PET-kuvausta hyödynnetään lisäksi tietokonetomografian kanssa, jolloin voidaan tarkentaa sairastunut alue elimessä. PET-tomografian etuna on, että sen avulla on mahdollista huomata sairastuminen jo sen alkuvaiheessa, jolloin tilanteeseen voidaan puuttua ja löytää tehokas hoitokeino. (Ayala, 2016, 21.)

PET-kuvantamisjärjestelmä tunnistaa gammasädepareja, jotka emittoituvat epäsuorasti positroneja emittoivista radionuklideista (merkkiaine), jota ruiskutetaan kehon sisälle. Kehossa olevan merkkiainekonsentraation perusteella rakennetaan kolmiulotteisia malleja tietokoneanalyysin avulla. PET-skannaus sisältää altistuksen ionisoivalle säteilylle. Standardi PET-tomografiassa käytetty radiolähetin lähettää tehokasta 14 mSv:n suuruista säteilyä. Vertailun vuoksi muiden lääketieteellisten toimenpiteiden säteilyannos on välillä 0.02 mSv rinnan alueen röntgenkuvaukseen ja 6.5-8 mSv rinnan CT-kuvaukseen. PET-CT-kuvaukseen säteilyaltistus voi olla 23-26 mSv. (Ayala, 2016, 21.) Esimerkkejä potentiaalisista PET-skannerin hakkeroinneista on esitelty taulukossa 5.

TAULUKKO 5 Potentiaaliset PET-skannerin hakkerointimahdollisuudet (Ayala, 2016, 21 - 22)

Haitallinen hakkeritoiminta	Seuraukset
Hiljentää kaikki hälytykset	Hoitaja ei ole tietoinen, milloin PET-järjestelmän toiminta pettää
PET-laitteen kytkeminen pois päältä, sisäisten tiedostojen salaaminen	Häiritsee PET-kuvantamisoperaatioita. Lunnaita PET-laitteen avaamiseksi voidaan vaatia
Muuttaa varastoituja protokollia PET:n muistissa	Vääränlainen diagnostiikka
Saa PET:n hälyttämään satunnaisesti	Häiritsee PET-kuvantamisoperaatiota
Uudelleen käynnistää laitteen	Pyyhkii pois konfiguraatioasetukset
Yhdistää jonkun potilaan kuvantamistiedosto toisen potilaan vastaavaan	Diagnoosi toimitetaan väärälle potilaalle

Röntgengeneraattori

Lääketieteellisiä röntgenlaitteita käytetään ottamaan kuvia tiheistä kudoksista. Röntgenlaitteiden säteily on erittäin penetroivaa, ionisoivaa säteilyä, jolloin se voi olla hyvin vaarallista. Röntgensäteet imeytyvät hyvin pehmytkudokseen ja vakavat palovammat voivat aiheutua käsien, käsivarsien, ihon tai silmien altistumisesta primäärille tai diffraktoituneelle säteelle. Yleisin ja nopeimmin palautuva muutos on punoituksen muodostuminen. Mikäli säteilyannostus ja energia ovat riittävän matalalla tasolla, punoitusta tapahtuu, jonka jälkeen se katoaa ilman sivuvaikutuksia. Toinen muutos on hiusten tai karvoituksen menettäminen. Pienellä annostuksen määrällä hiukset alkavat kasvaa uudelleen ajan kanssa, eikä pysyviä vaikutuksia jää. Kolmas väliaikainen vaikutus on talirauhasten talin tuoton väliaikainen häiriö, jolloin rauhaset eivät tuota normaalia määrää talia. (Ayala, 2016, 21.)

Mikäli hakkeri kykenee kasvattamaan säteilyannosta tai altistusta, potilas voi vastaanottaa liiallisen määrän säteilyä, joka johtaa pysyvään hiusten, hikirauhasten tai ihon tuhoutumiseen arpia aiheuttaen. Akuutissa altistuksessa on kyse kertaluonteisesta tapahtumasta, jossa potilas saa suuren määrän säteilyä (esimerkiksi 1 Sievert) ja oireet ilmaantuvat nopeasti päivien tai viikkojen kuluessa. Krooniset altistukset ovat pitkäaikaisia altistuksia matalalla säteilymäärällä. Altistuksen vaikutukset näkyvät usein kertaluonteisena tapahtumana, jossa säteilyannostuksen määrä on korkea. Krooniset altistukset ovat pitkäaikaisia altistumisia matalalle säteilyn määrälle ja vaikutukset ilmaantuvat hitaasti 20 - 30 vuoden kuluessa altistumisesta. Kroonisten altistumisten seuraukset ilmaantuvat hitaasti, sillä keholla on aikaa parantaa itseään altistumisen jälkeen. (Ayala, 2016, 21.)

Säteilystä aiheutuneet palovammat voivat olla akuutteja lokaaleja altistuksia, jotka ovat seurausta suoralle primäärille säteilylle altistumisesta. Korkeaenergiset röntgensäteet penetroivat ihon ulkoisia kerroksia, jotka sisältävät eniten hermopäätteitä, jolloin potilas ei välttämättä tunne, että hän on saanut yliannoksen röntgensäteilyä, ennen kuin vahinko on jo tapahtunut. Ääritapaukset vaativat ihosiirrännäisiä tai sormien amputaatioita. Annostuksen vaarallisuus riippuu

vastaanotetusta annoksesta, altistuksen suuruudesta, röntgensäteiden energiamäärästä sekä potilaan herkkyydestä. Palovammoja voi syntyä 300 rem (Röntgen Equivalent Man) säteilymäärillä, mutta useimmiten niiden syntyminen vaatii 600 rem säteilyn. Säteilysairautta voivat aiheuttaa koko kehoon suuntautuvat useamman tunnin kestävä yli 100 rem:n säteilyannokset. Mikäli potilas saa 400-500 rem:n suuruisen säteilyannoksen, se aiheuttaa hoitamattomana kuoleman 50 % potilaille 30 päivän aikana. Jo lyhytaikainen altistus 700 rem säteilyannokselle aiheuttaa kuoleman viikkojen kuluessa altistuksesta. (Ayala, 2016, 21 - 22.) Taulukosta 6 havainnollistuu röntgenlaitteeseen kohdistuvia kyberfyysisiä hyökkäyksiä.

TAULUKKO 6 Mahdollisia röntgenlaiteeseen kohdistuvia hyökkäyksiä (Ayala, 2016, 22)

Haitallinen hakkeritoiminta	Seuraukset
Jännitteen kasvattaminen (KVp)	Röntgensäteitä, joilla on korkeammat keV fotonit
Jännitteen määrän kasvattaminen (mA)	Enemmän röntgenfotoneita
Aiheuttaa tilanteen, jossa röntgenlaite ylittää suositellut säteilyaltistuksien määrät	Hakkeri voi muuttaa annostuksen määrän huomattavasti suosituksia korkeammaksi, joka aiheuttaa palovammoja ja säteilysairautta
Kaikkien hälytyksien hiljentäminen	Radiologit eivät saa tietää vaarallisesta tilanteesta
Röntgenlaitteen sammuttaminen ja sisäisten tiedostojen salaaminen	Häiritsee röntgenoperaatioita. Lunnaita röntgenlaitteen avaamiseksi voidaan vaatia
Näytön informaation vaihtaminen	Aiheuttaa sekaannusta säteilylle altistumisessa
Saa röntgenlaitteen tekemään satunnaisia hälytyksiä	Häiritsee röntgenoperaatioita
Saa röntgenlaitteen käynnistymään uudelleen	Pyyhkii konfiguraatioasetukset
Yhdistää jonkun potilaan kuvantamistiedosto toisen potilaan vastaavaan	Diagnoosi toimitetaan väärälle potilaalle

Tietokonetomografia

Tietokonetomografia, toiselta nimeltään viipalekuvaus (CT-kuvaus eli Computer Tomography) on radiologian alaan kuuluva lääketieteellinen tutkimusmenetelmä, joka perustuu röntgenkuvauksen kaltaisesti röntgensäteiden erilaiseen absorptioon eri kuvauksissa ja elimissä. Kuvauksessa otetaan röntgensäteiden avulla poikkileikkauskuvia halutulta alueelta, joka voidaan määritellä esimerkiksi pään, kaulan, vartalon tai raajojen alueelle. CT-kuvantamisessa otetuista leikekuvista pystytään erottelemaan yksityiskohtia, kuten luut, rasvakudokset, sisäelimet, verisuonet jne. hyödyntämällä tietokonetomografian kuvausmenetelmiä ja kuvanmuokkausta. Leikkeinä otetuista viipalekuvista voidaan lopuksi muodostaa kolmiulotteisia malleja. Tutkimus on kivuton ja tutkimuksen kohteena oleva potilas makaa tutkimuspöydällä liikkumatta pöydän liikkuessa laitteen sisään. Kuvausaika on vain muutamia minuutteja pitkä, tosin valmisteluineen aikaa kuluu enemmän. Tutkimusprosessiin

kuuluu myös tutkittavan ohjaus erilaisine hengitysohjeineen. Tutkimukseen kuuluu osana monesti myös varjoaineen ruiskuttaminen kanyylin kautta laskimoon, joka saa suoliston piirteet erottumaan. Varjoaine poistuu elimistöstä lopulta virtsan mukana.

Tietokonetomografiaa pidetään diagnosointiteknologiana, jonka säteilyn määrä vaihtelee välillä keskinkertainen – korkea. Kuitenkin, säteilyannokset, joita CT-kuvauksesta voidaan saada, ovat 100 - 1000 kertaa suurempia kuin tavanomaiset röntgenkuvat. Tyypillisessä röntgenkuvauksessa säteilyannoksen määrä on välillä 0.01 - 0.15 mGy (milligray). Tietokonetomografiakuvauksissa säteilyannos voi olla 10-20 mGy tietyille elimille ja se voi myös nousta jopa 80 mGy:n asti tietyille spesifisille viipalekuvauksille. Säteilyannoksen vaikutus on kumulatiivinen ja mitä enemmän potilas säteilylle altistuu, sen suurempi on syöpäriski. Pitkäaikaisvaikutukset kroonisesta altistumisesta ionisoivalle säteilylle lisäävät leukemian ja muiden syöpien lisääntymistä. Esimerkkejä potentiaalisista CT-skannerin hakkeroinneista on ilmaistu taulukossa 7.

TAULUKKO 7 Mahdollisia CT-skanneriin kohdistuvia hyökkäyksiä (Ayala, 2016, 26)

Haitallinen hakkeritoiminta	Seuraukset
Jännitteen kasvattaminen (KVp)	Röntgensäteitä, joilla on korkeammat keV-fotonit
Jännitteen määrän kasvattaminen (mA)	Enemmän röntgenfotoneita
Konfiguraatiotiedostojen peukalointi ja säteilyaltistuksen raja-arvojen muuttaminen, jotka vaikuttavat potilaiden saamaan säteilyyn	Hakkeri voi muuttaa annostuksen määrän huomattavasti suosituksia korkeammaksi, joka aiheuttaa palovammoja ja säteilysairautta
Kaikkien hälytyksien hiljentäminen	Radiologit eivät saa tietää vaarallisesta tilanteesta
CT-skannerin sammuttaminen ja sisäisten tiedostojen salaaminen	Häiritsee CT-skannaus-operaatioita. Lunnaita röntgenlaitteen avaamiseksi voidaan vaatia
Näytön informaation vaihtaminen	Aiheuttaa sekaannusta säteilylle altistumisessa
Saa röntgenlaitteen tekemään satunnaisia hälytyksiä	Häiritsee tomografiaoperaatioita
Operaattorin asettaman kynnysarvon vaihtaminen	Operaattori ei voi erottaa erilaisia rakenteita, tehden segmentoinnin mahdottomaksi
Saa röntgenlaitteen käynnistymään uudelleen	Pyyhkii konfiguraatioasetukset
Yhdistää jonkun potilaan kuvantamistiedosto toisen potilaan vastaavaan	Diagnoosi toimitetaan väärälle potilaalle

Robottikirurgiset koneet

Robottikirurgisia koneita on hyödynnetty useammanlaisissa kirurgisissa operaatioissa, kuten urologia, kardiologia, paksu- ja peräsuolen leikkaukset, gynekologia, neurokirurgia ja verisuonistoon kohdistuvat leikkaukset. Robottikirurgia on suhteellisen uusi teknologia ja se on myös vähemmän invasiivinen tapa leikkausoperaatioiden toteuttamiseksi. Robottikirurgiassa verenvuoto on vähäisempää ja robottikirurgiset leikkaukset lisäksi vähentävät sairaalassaolopäiviä. Robottikirurgiassa kirurgi operoi potilasta videoyhteyden kautta käyttämällä robottikäsivarsia kirurgisten instrumenttien suoran hyödyntämisen sijasta. Kirurgin ei välttämättä tarvitse olla läsnä leikkaussalissa, vaan hän voi olla periaatteessa missä tahansa maailmalla ja suorittaa potilaalle leikkausoperaatioita etänä. (Ayala, 2016, 30.)

Tällä hetkellä robottikirurgiassa hyödynnettävät robotit ovat kuitenkin hyvin monimutkaisia ja niiden hyödyntäminen vaatii kokeneen kirurgin, joka on koulutettu niiden käyttöön. Aiemmin kirurgit keskittyivät kirurgiseen menettelyyn, mutta nykyään he ovat lisäksi huolissaan laitteiden vikaantumisista. Uusia uhkakuvia syntyy kyberhyökkäyksien aiheuttamina, sillä mikäli hakkeri kykenee saavuttamaan leikkausrobotin kontrollin, sillä voi olla jopa potilaan henkeä uhkaavia vaikutuksia. (Ayala, 2016, 31.) Taulukossa 8 havainnollistetaan mahdollisia leikkauskirurgisiin robotteihin kohdistuvia kyberfyysisiä hyökkäyksiä.

TAULUKKO 8 Mahdollisia kirurgisiin robotteihin kohdistuvia hyökkäyksiä (Ayala, 2016, 31)

Haitallinen hakkeritoiminta	Seuraukset
Näytön informaation vaihtaminen	Aiheuttaa hämmennystä teknisessä tuessa
Spontaani uudelleen käynnistäminen	Pyyhkii kokoonpanoasetukset
Saa röntgenlaitteen tekemään satunnaisia hälytyksiä	Häiritsee potilasprosessia
Kaikkien hälytyksien hiljentäminen	Kirurgit eivät saa tietää vaarallisesta tilanteesta
Videosyötteen sammuttaminen	Kirurgi päättää operaation ja aloittaa ilman robottia toteutettavan menettelyn
Aiheuttaa robotin käsivarsien kontrolloimattoman liikkeen	Kirurgi päättää operaation ja aloittaa ilman robottia toteutettavan menettelyn
Robotin sammuttaminen	Kirurgi päättää operaation ja aloittaa ilman robottia toteutettavan menettelyn
Saa verkon pudottamaan paketteja	Häiritsee potilasprosessia

Anestesiakone

Anestesiakonetta käytetään anestesian antamiseen. Yleisin anestesiakoneen tyyppi on jatkuvan virtauksen anestesiakone, joka on suunniteltu toimittamaan anestesiakaasuja (happi ja typpioksidi) mahdollisimman tarkasti ja jatkuvalla syötöllä. Anestesiakaasuja sekoitetaan anestesiahöyryihin (kuten isofluraani) ja kohdistetaan potilaaseen turvallisella paineistuksella ja virtauksella. Modernit laitteet käsittävät tuulettimen, imuyksikön ja potilasmonitorointilaitteistot. Anestesialaitteistot eivät useimmiten ole verkossa ja eivät mahdollista Web-pohjaista hallintaa, jolloin jollain käyttäjistä

tulee olla fyysinen pääsy laitteistojen kontrolleihin. Taulukossa 9 havainnollistetaan potentiaalisia anestesiakoneisiin kohdistuvia kyberfyysisiä hyökkäyksiä.

TAULUKKO 9 Mahdollisia anestesiakoneisiin kohdistuvia hyökkäyksiä (Ayala, 2016, 27)

Haitallinen hakkeritoiminta	Seuraukset
Happivirhehälytyksen huijaus	Ilmanpaineen ollessa 38 PSI (pounds per square meter) ja laskeva, soitetaan hälytys. Uudemmissa laitteissa on sähköinen sensori
Poistetaan käytöstä typpioksidi- ja hapenvikojen suojauslaite	Typpioksidiregulaattori on happiregulaattorille ”orjan” asemassa (jos happipainetta ei ole, muut kaasut eivät voi virrata regulaattorien kautta)
Hypoksisen seoksen hälytyksen sammuttaminen	Hypoksisuojat (Suhdeluvun kontrolloijat) estävät kaasuseoksien, jotka sisältävät vähemmän kuin 21 % - 25 % happea, toimittamisen potilaalle
Kaikkien hälytyksien hiljentäminen	Anestesialääkärit eivät saa tietää vaarallisesta tilanteesta
Höyrystimien välisten lukituksien estäminen	Suunniteltu estämään useamman kuin yhden haihtuvan aineen samanaikaisesti tapahtuvan antamisen potilaalle
Näytön informaation vaihtaminen	Tekee mahdottomaksi kaasujen monitoroinnin ja aiheuttaa sekaannusta hapen, ilman ja typpioksidin virtauksessa
Saa anestesialaitteen tekemään satunnaisia hälytyksiä	Häiritsee potilaan toimintaa
Häiritsee potilaan sykkeen, sydänkäyrän, verenpaineen ja happisaturaation seurantajärjestelmää	Tekee mahdottomaksi monitoroida sisään- ja uloshengityksen konsentraatiota tai hiilidioksidin osittaista painetta sekä epäsuoraa hiilidioksidin osittaispainetta valtimoverenkierrossa
Muuttaa potilaiden annostusta	Katastrofaaliset seuraukset mahdollisia (potilas ei ole täysin nukutettu, lääkeaineen yliannostus, lääkkeiden välinen haitallinen vuorovaikutus)
Aiheuttaa laitteen uudelleen käynnistyksen	Tyhjentää konfiguraatioasetukset

Digitaaliset potilastietueet

Sairaalat luottavat vahvasti kliinisiin tietovarastoihin, kliiniseen informatiikkaan, terveystietojärjestelmiin ja potilastietueisiin. Hakkeri voi ilman vaadittavaa autentikointia salassa toimiessaan hyödyntää diagnostiikkapalvelinhyökkäyksiä toteuttaakseen seuraavia hyökkäyksiä:

- Kohdetietokoneen muistin vedokset (memory dump)
- Kohdetietokoneen muistin peukalointi (memory patch)
- Etäkutsut toimintoihin (calls to functions)
- Etätehtävänhallinta (task management)

Hakkeri, jolla on pääsy digitaalisiin potilastietueisiin voi muuttaa dataa siten, että se voi saada lääkärit tekemään virhediagnooseja, määräämään vääränlaisia lääkityksiä tai määrätä vääränlaista hoitoa, jotta potilas ei saa oikeanlaista ja tarvittavaa hoitoa. Ilman pääsyä tietoturvallisiin potilastietueisiin, lääkärit joutuvat turvautumaan vanhanaikaisiin kommunikaatioteknologioihin, kuten puhelimet ja faksit. (Ayala, 2016, 35 - 36). Esimerkkejä potentiaalisista hakkeroinneista on esitelty taulukossa 10.

TAULUKKO 10 Digitaalisiin potilastietueisiin kohdistuvia hyökkäyksiä (Ayala, 2016, 35 - 36)

Haitallinen hakkeritoiminta	Seuraukset
Digitaalisen potilastietueen muokkaaminen	Hakkeri voi muuttaa informaatiota (veriryhmää, sairastaako diabetesta vai ei jne.)
Datan poistaminen	Potilashistoria häviää
Muuntaa potilaan hoitohistoriaa	Potilashoitoon sekaantuminen (estää tarkan diagnosoinnin)
Saa verkon pudottamaan IP-paketteja	Häiritsee potilasmenettelyä
Lääkityshistorian muuttaminen	Häiritsee hoitoproseduuria, jolloin voidaan antaa väärä annos lääkitystä tai lääkitys voidaan vahingossa antaa väärälle potilaalle, jolloin seurauksena voi olla vammautuminen tai kuolema
Hoitotyönjärjestyksen muuntaminen	Mahdolliset katastrofaaliset seuraukset (väärän jalan amputointi, lääkityksen yliannostus, negatiiviset lääkityksen yhteisvaikutukset)
Lääketieteen ammattilaisten harhaan johtaminen	Mahdollinen potilasvahinko
Testi tai hoitoaikataulun muuntaminen	Hoitoproseduurin häirintä
Elinluovuttajan lääketieteellisen informaation muuntaminen	Tekee mahdottomaksi elinluovuttajien elimien hyödyntämisen tai niitä voidaan hyödyntää väärälle potilaalle

Viivakoodin lukujärjestelmät

Sairaaloilla ja terveydenhuollon organisaatioilla on vahva luottamus lääkkeiden skannauslaitteisiin, jotta potilaiden nimi ja tunnistusinformaatio voitaisiin lukea sekä parantaa potilashoitoa ja ehkäistä lääketieteellisten virheiden syntyminen. Hakkeri voi manipuloida näitä laitteita saadakseen viivakoodin luvun näyttämään virheettömältä, vaikka kyseessä on samanaikaisesti yhteensopivuusongelma. Farmaseutit luottavat viivakoodi-informaatioon lääkkeiden inventaariojärjestelmissä varmistaakseen potilasturvallisuuden tarkastaessaan lääkkeiden yhteisvaikutuksia alkoholin, ruoan, lisäravinteiden ja sairauksien suhteen. (Ayala, 2016, 35 - 36.)

Peukaloimalla viivakoodin lukujärjestelmää hakkeri voi manipuloida verensokeri- tai lääkenäytteitä sairaalassa, joka voi aiheuttaa väärän lääketyypin ja annostuksen toimituksen sekä sekoittaa verinäytteet. Datan muuttaminen potilaan tietojen, rannekkeen tai lääkkeiden etikettien skannaamisen aikana voi muodostaa henkeä uhkaavia tilanteita, joita voi olla vaikea käsitellä ajan ollessa kriittinen tekijä. (Ayala, 2016, 35 - 36.)

Terroristihakkeri voi kyetä tuhoamaan näytteiden jäljitysohjelmiston ja saada viivakoodin lukijat varastoimaan luetun informaation väärään potilastiedostoon. Lääkeaineiden yhteisvaikutukset tulisivat tässä tapauksessa realisoitumaan hyvin todennäköisesti ja vakavin seurauksin. Näiden virheiden etsiminen massiivisista potilastiedostoista olisi myös erittäin vaikeaa. Lääkärit luottavat vahvasti digitaalisiin lääketieteellisiin potilastietueisiin, joita hakkerit voivat muuttaa. Tämä aikaansaa lääkärit diagnosoimaan sairaudet värin, määräämään vääränlaisia lääkkeitä tai keskittymään epäolennaiseen hoitoon. (Ayala, 2016, 35 - 36.) Esimerkkejä potentiaalisista viivakoodilukujärjestelmän hakkeroinneista on esitelty taulukossa 11.

TAULUKKO 11 Viivakoodin lukemisjärjestelmiin kohdistuvia hyökkäyksiä (Ayala, 2016, 35 - 36)

Haitallinen hakkeritoiminta	Seuraukset
Potilaiden viivakoodi-informaation muuttaminen	Hakkeri voi muuttaa informaatiota (veriryhmä tai onko potilaalla diabetes vai ei jne.)
Viivakoodidatan tuhoaminen	Potilashistoria on vääristynyt tai hävinnyt
Potilaan hoitohistorian muuttaminen	Hoidon häiritseminen (akuutin diagnosoinnin estäminen)
Saa verkon pudottamaan IP-paketteja	Häiritsee potilasmenettelyä
Lääkityshistorian muuttaminen	Mahdollinen virhediagnoosi
Hoitotyönjärjestyksen muuntaminen	Mahdolliset katastrofaaliset seuraukset (väärän jalan amputointi, lääkityksen yliannostus, negatiiviset lääkityksen yhteisvaikutukset)
Lääketieteen ammattilaisten harhaan johtaminen	Mahdollinen potilasvahinko
Testi tai hoitoaikataulun muuntaminen	Hoitoproseduurin häirintä

Lääketieteelliset laboratoriot

Hyökkääjä, joka hakkeroi sairaalan automaattisen laboratoriojärjestelmän (Laboratory Automation System eli LAS) voi sulkea esimerkiksi jääkaapit ja muut kriittiset järjestelmät ja laitteet. Hakkeri voi myös pitää kaiken tallennetun tutkimustiedon panttina ja romuttaa lämmitys-, ilmanvaihto- ja ilmastointijärjestelmän (Heating, Ventilation and Air Conditioning eli HVAC). (Ayala, 2016, 34 - 35.) Esimerkkejä potentiaalisista lääketieteelliseen laboratorioon kohdistuvista hyökkäyksistä on mainittu taulukossa 12.

TAULUKKO 12 Lääketieteellisiin laboratorioihin kohdistuvia hyökkäyksiä (Ayala, 2016, 28)

Haitallinen hakkeritoiminta	Seuraukset
Informaation siirron estäminen	Järjestelmä ei kykene toimittamaan kriittistä informaatiota
Laboratoriolaitteiston asetusten tai testiproseduurien muokkaaminen	Tuhoutuneet testitulokset
Saa verkon pudottamaan IP-paketteja	Häiritsee potilasmonitorointia
Laboratoriotestien tuhoaminen	Potilasmonitoroinnin häirintä
Hoitotyönjärjestyksen muuntaminen	Potilashoidon häirintä
Näytteiden saastuttaminen	Epäasiallisen hoidon aiheuttaminen
Potilasnäytteiden hävittäminen	Potilashoidon häirintä

Sydän-keuhkokone

Sydän-keuhkokonetta käytetään hoitamaan verenkiertoon ja hapetukseen liittyvät toimenpiteet potilaan sydämen ollessa pysähtynyt. Sitä myös hyödynnetään sydän-keuhko -sairauksien ohitusleikkauksissa. Veri johdetaan painovoimaa hyödyntäen sydän-keuhko-koneeseen, jossa se kulkeutuu keinotekoisen keuhkon (tai ”hapettimen”) lävitse ja systeemiseen valtimojärjestelmään. Heparinisaatiota käytetään antikoagulaation turvallisen tason määrittämiseen. Hapettimeen on sisällytetty sydämen laajennin, jonka tehtävänä on viilentää sekä lämmittää (veri) potilasta tarpeen mukaan. Taulukossa 13 on esimerkkejä potentiaalisista sydän-keuhko-koneeseen kohdistuvista hakkeroinneista.

TAULUKKO 13 Sydän-keuhkokoneeseen kohdistuvia hyökkäyksiä (Ayala, 2016, 28)

Haitallinen hakkeritoiminta	Seuraukset
Hepariinipumpun sulkeminen	Potilaan veren hyytyminen mahdollinen
Pumppu tuottaa liian paljon hepariinia	Liian korkea antikoagulaation määrä, joka täytyy sitten vaihtaa päinvastaiseksi. Veri ei hyydy tarkoituksenmukaisella tavalla aiheuttaen sisäistä verenvuotoa. Sisäisen verenvuodon ollessa riittävän vakavaa se voi aiheuttaa potilaan kuoleman
Kaikkien hälytyksien hiljentäminen	Biolääketieteen henkilöstö ei ole tietoinen vaarallisesta tilanteesta
Näytön informaation vaihtaminen	Biolääketieteen henkilöstön hämmentäminen
Saa laitteen tekemään satunnaisia hälytyksiä	Potilasmenettelyn häirintä
Näytteiden saastuttaminen	Epäasiallisen hoidon aiheuttaminen
Aiheuttaa laitteen uudelleen käynnistyksen	Tyhjentää konfiguraatioasetukset

LIITE 3: Kyberhyökkäyksiä terveydenhuollossa

Hyökkäys	Hyökkäyksen kuvaus/vaikutus
Kiristysohjelma UW Medicine USA 1.10.2013	90 000 potilasrekisterä vuotanut ulos. Sähköpostiliitteen avaus aiheutti haittaohjelmat. Todettu päivää myöhemmin. Tiedot potilaista ovat saattaneet sisältää seuraavat tiedot: nimi ja muut henkilötiedot, muut tiedot (mukaan lukien osoite, puhelinnumero), hoitopäivät ja hoitomaksut. (KnowBe4.)
Kiristysohjelma Varsinais-Suomen SHP Suomi 6.3.2015	Hyökkääjä käytti kiristyshaittaohjelmaa. Toinen tapaus tapahtui kahden päivän sisällä. Molemmat tapahtumat vaikuttivat yhteen tietokoneeseen. Salattu 30.000 paikallista tiedostoa ja ajanvarausilmoitusjärjestelmä ei ollut käytettävissä. Infektio tuli Facebook-käytön kautta. (Varsinais-Suomen sairaanhoitopiiri, 2015.)
Kiristysohjelma HUS Suomi 1.2.2016	Husin tietoverkossa oli kiristyshaittaohjelma. Se oli ottanut tietokoneen haltuunsa ja uhannut, että hävittäisi kaikki tiedostot, jos sen lunnasvaatimukseen ei suostuttaisi. Lukittuja tiedostoja oli palautettava varmuuskopioista. (Rissanen & Koivuranta, 2016.)
Kiristysohjelma Lukas Hospital Saksa 1.2.2016	Röntgenlaitetta ei voitu käyttää. 15 - 20 prosenttia toimenpiteistä peruutettu. Samanlaiset ongelmat kahdessa muussa Saksan sairaalassa. (Steffen, 2016.)
Kiristysohjelma Ottawa Hospital Kanada 13.3.2016	Neljään tietokoneeseen vaikutettiin kiristysohjelmalla, jolloin tietojen käyttö sairaalassa estyi. Ei vaikuttanut potilastietojen sisältöön. Haittaohjelmat lukitsivat tiedostot. Palautettu varmuuskopioista. (Pilieci, 2016.)
Kiristysohjelma Desert Valley Hospital USA 18.3.2016	Kiristyshaittaohjelma havaittu. Potilaan tai työntekijöiden tietoja ei vaarannettu. Suurin osa toiminnoista jatkui samalla, kun ryhdyttiin toimiin palauttamaan sairaalajärjestelmät toiminta normaaliksi. (Monegain, 2016a.)
Kiristysohjelma Chino Valley Medical Center USA 18.3.2016	Kiristyshaittaohjelma havaittu. Potilaan tai työntekijöiden tietoja ei vaarannettu. Suurin osa toiminnoista jatkui samalla, kun ryhdyttiin toimiin palauttamaan sairaalajärjestelmät toiminta normaaliksi. (Monegain, 2016a.)
Kiristysohjelma Methodist Hospital USA 18.3.2016	Kiristyshaittaohjelma havaittu verkossa. Sairaala käytti varmuusjärjestelmäänsä, kun pääverkko oli lukittu. Organisaation sisäinen tila, joka rajoitti sähköisten web-pohjaisten palvelujen käyttöä. (Monegain, 2016b.)

Kiristysohjelma MedStar Medical System USA 29.3.2016	MedStar, voittoa tavoittelematon ryhmä, joka ylläpitää 10 sairaalan toimintaa Baltimore ja Washington alueella, joutui Samsam-kiristyshaittaohjelman hyökkäyksen kohteeksi. Verkkopalveluja jouduttiin eristämään, nopea toiminta esti haittaohjelman leviämisen, varmuuskopioista palautukset. (Krishnan, 2016.)
Kiristysohjelma Kansas Heart Hospital USA 18.5.2016	Kiristyshaittaohjelma vaikutti sairaalan toimintaan usean päivän ajan. Maksettu lunnaita, mutta tiedostoja ei purettu. Rikolliset pyysivät toista maksua. Potilastiedot eivät olleet vaarassa ja vaikutukset toimintaan. (Ms. Smith, 2016.)
Kiristysohjelma Lincolnshire Hospitals UK 30.10.2016	Iso-Britannian Kansallinen terveydenhuoltopalvelu (NHS) vaarantui kiristyshaittaohjelman vuoksi. Satoja suunniteltuja toimintoja, avohoitopäiviä ja diagnoosimenettelyjä on peruutettu useissa sairaaloissa Lincolnshiressä Englannissa sen jälkeen, kun "suuri" tietokonevirus on vaarannuttanut National Health Service (NHS) –verkon (yhteensä 2800). (Kumar, 2016.)
Kiristysohjelma Urology Austin USA 27.1.2017	Hyökkääjät pystyivät salaamaan palvelimelle tallennetut tiedot kiristyshaittaohjelmalla. Potilaistiedot ovat saattaneet altistua haittaohjelmalle yli 279 000 potilastietokannasta (nimet, syntymäajat, osoitteet, lääketieteelliset tiedot ja sosiaaliturvatunnukset). Toiminta estettiin sammuttamalla palvelinverkko. Potilastiedot palautettu varmuuskopiosta. (Davis, 2017.)
Kiristysohjelma Erie County Medical Center USA 9.4.2017	Hyökkääjä käytti kiristyshaittaohjelmaa, joka sulki sähköisen terveysrekisterin (EHR). EHR ei ollut käytettävissä 4 päivään. Noin 6000 pöytätietokonetta pyyhittiin puhtaaksi ja henkilökunta pystyi katsomaan EMR-potilastietoja, mutta ei voinut syöttää järjestelmään mitään tietoja. Henkilökunta käytti kannettavia tietokoneita ja käsikäyttöisiä prosesseja potilastoimenpiteissä. Kesti noin 2 kuukautta, kunnes toiminta voitiin täysin palauttaa. Tiedot oli varmuuskopioitu. (Landi, 2017.)

Kiristysohjelma Greenway Health USA 24.4.2017	Kiristyshaittaohjelman uskotaan vaikuttaneen kohteessa 400 terveydenhuollon lääketieteelliseen käytäntöön eli noin viiteen prosenttiin palveluntarjoajan asiakaskunnasta. Organisaatio joutui oletettavasti tekemään huomattavan määrän toiminnan palautustehtäviä. Tietoja ei joutunut vääriin käsiin. Järjestelmät palautettiin varmuuskopioiden avulla. (Bisson, 2017.)
Kiristysohjelma National Health Service UK 12.5.2017	Hyökkääjä käytti WannaCry-kiristyshaittaohjelma, joka levisi kohteen verkossa 48 NHS-organisaatioon. Aiheutti häiriöitä potilastietojen käyttöön, ambulanssien toiminnan ohjaukseen ja leikkauksiin. Potilastiedot eivät tiettävästi vaarantuneet. Lääkemääräyksiä tai hoitohistorioita ei vuotanut rikollisille. (BBC, 2017.)
Kiristysohjelma TYKS Suomi 8.6.2017	Hyökkääjä käytti Wannacry-kiristys haittaohjelmaa Turun yliopistollisessa keskussairaalassa useisiin lääkintälaitteisiin. Keskussairaala joutui haittaohjelman toisen aallon uhriksi viime viikolla. Haittaohjelma häiritsi useita sairaalan lääkintälaitteita. Joukossa oli muun muassa mammografiaan ja sädehoitoon liittyviä tietokoneita. Potilastiedot eivät olleet vaarassa hyökkäyksen aikana. (Savolainen, 2017.)
Kiristysohjelma MEDHOST USA 19.12.2017	Hyökkääjä käytti kiristyshaittaohjelmaa, jolloin kohteen tili internet-verkkotunnuksen rekisteröijän kanssa vaarantui ja julkiset URL-osoitteemme ohjattiin sivustoon, jossa ilmoitettiin, että potilastietoja myydään, jos lunnaisiin ei suostuta. Kohteessa ei merkkejä siitä, että potilastiedot olisivat vaarantuneet. Tilannehallinta hoidettiin sisäisissä järjestelmissä. (DataBreaches.net, 2017a.)
Kiristysohjelma Allscripts USA 18.1.2018	Hyökkääjä yhdistettiin SamSamin ransomware-ryhmään. Sen vaikutukseen kuuluivat sähköinen terveysrekisterin toimittaja Allscripts-yhtiö. Allscripts ei onnistunut turvaamaan ja tarkastamaan järjestelmäänsä, mikä aiheutti järjestelmän katkoksen noin viikon ajan aiheuttaen asiakkailleen merkittävän liiketoiminnan keskeytymisen. (Davis, 2018.)

Hakkerointi Excellus BlueCross BlueShield USA 1.12.2013	Haitantekijät saivat haltuunsa 11 miljoonan asiakkaan tiedot. Murto havaittiin vasta noin kaksi vuotta myöhemmin. Hyökkääjät eivät ole tähän mennessä käyttäneet tietoja, mutta heillä on hallussaan asiakkaiden nimiä, sosiaaliturvanumeroita, osoitteita, syntymäpäivätietoja ja taloudellisia tietoja. (Groden, 2015.)
Hakkerointi Anthem USA 1.4.2014	Haitantekijät saivat haltuunsa 80 miljoonan asiakkaan tiedot; nimet, syntymäpäivät, lääketieteelliset tunnukset, sosiaaliturvatunnukset, katuosoitteet, sähköpostiosoitteet ja työllisyystiedot, taloudelliset tiedot. (Terhune, 2015.)
Hakkerointi Community Health Systems USA 1.4.2014	Haitantekijät saivat haltuunsa 4,5 miljoonaa potilaskertomusta sairaalan verkoista 206 sairaalasta. Tietoihin lukeutuivat nimet, sosiaaliturvatunnukset, fyysiset osoitteet, syntymäpäivät ja puhelinnumerot. (Pagliery, 2014.)
Hakkerointi Premera Blue Cross USA 5.5.2014	Haitantekijät saivat haltuunsa 11 miljoonan asiakkaan tiedot; lääketieteelliset kirjat, pankkitilitiedot, sosiaaliturvatunnukset ja syntymäpäivät kolmetoista vuoden ajalta. (Vinton, 2015.)
Hakkerointi CareFirst Blue Cross and Blue Shield USA 1.6.2014	Haitantekijät vaaransivat 1,1 miljoonaa asiakastietoa; käyttäjätunnukset, nimet, syntymäpäivät, sähköpostiosoitteet ja tunnistenumerot, kun taas sosiaaliturvan numeroita, taloudellisia tietoja, salasanoja ja luottokorttien numeroita ei ole ilmoitettu varastettaviksi. (HACKREAD, 2015.)
Hakkerointi UCLA Health USA 1.9.2014	Haitantekijät saivat haltuunsa 4.5 miljoonana henkilön tiedot; nimet, lääketieteelliset tiedot, sosiaaliturvatunnukset, terveystunnuksen tunnukset, syntymäpäivät ja fyysiset osoitteet. Tietomurto vaikuttaa kaikkiin, jotka ovat käyneet tai työskentelevät yliopiston lääketieteellisessä verkostossa, UCLA Health, johon kuuluu neljä sairaalaa ja 150 toimistoa Etelä-Kaliforniassa. (Pagliery, 2015.)
Hakkerointi Medical Informatics Engineering USA 7.5.2015	Terveydenhuollon ohjelmistoyrityksen tietoihin murtauduttiin. Varastetut tiedot sisälsivät nimiä, syntymäpäiviä, osoitteita, terveysrekistereitä ja sosiaaliturvatunnuksia noin 3,9 - 4,0 miljoonan ihmisen osalta. Vaikutusalueella oli 11 terveydenhuollon tarjoajaa (44 sairaalaa). (Amir, 2015.)
Hakkerointi 21st Century Oncology USA 3.10.2015	Haitantekijät saivat haltuunsa 2,2 miljoonan henkilön potilastiedot. Potilaiden nimet, sosiaaliturvatunnukset, lääkäreiden nimet, diagnoosi- ja hoitotiedot sekä vakuutustiedot joutuivat rikollisten käsiin. Huomattavia viiveitä havainnoinnissa ja tilanteen ilmoittamisessa. Oikeusjuttua organisaatiota kohtaan käynnissä laiminlyödystä tietoturvasta. (McGee, 2016.)

Hakkerointi Valley Anesthesiology and Pain Consultants USA 30.3.2016	Haitantekijät saivat haltuunsa lähes 900 000 henkilö tiedot. Vaarantuneet potilaiden tiedot sisältävät henkilöiden nimiä, hoitopäivämäärä, hoitopaikkoja, vakuutustunnuksia, diagnoosi- ja hoitokoodeja sekä sosiaaliturvatunnuksia. Palveluntarjoajan pankkitilitiedot ovat olleet myös vaarassa. (ASC COMMUNICATION, 2019a.)
Hakkerointi Jinan Kiina 8.4.2016	Haitantekijät saivat haltuunsa 200 000 tiedostoa lapsista sairaaloista, joissa lapset rokotettiin. Tiedot sisälsivät vanhempien matkapuhelinnumeroita ja kotiosoita. Vanhemmat ovat saaneet monia puheluita rikollisilta vuodon jälkeen. Heitä huolestuttavia vaaroja ovat rahan kiristys tai jopa lapsien kidnappaukset. (Ruohan, 2016.)
Hakkerointi Medical Colleagues of Texas USA 19.5.2016	Haitantekijät saivat haltuunsa 50 000 henkilön tiedot, jotka koskivat työntekijä- ja potilastietietoja, kuten nimet, osoitteet, sosiaaliturvatunnukset ja sairausvakuutustiedot. (LaPointe, 2016b.)
Hakkerointi Newkirk Products USA 21.5.2016	Haitantekijät saivat haltuunsa 3,3 miljoonan henkilö tiedot. Murto havaittiin noin 1,5 kuukautta tapahtuman jälkeen. Mahdollisesti vaarantuneet tiedot ovat henkilöiden nimiä, osoitteita, hoitosuunnitelma, erilaisia jäsen- ja ryhmätunnusnumeroita, huollettavien nimiä, perusterveydenhuollon tarjoajia, syntymäpäiviä, laskutustietoja ja terveydenhuollon tunnusnumeroita. (ASC COMMUNICATIONS, 2019d.)

Hakkerointi Athens Orthopedic Clinic USA 14.6.2016	Haitantekijät vaaransivat 200 000 potilaan tiedot. Murtautumisessa käytettiin ulkopuolisen myyjän kirjautumisvaltuutuksia rekisterijärjestelmän käyttämiseen. Vaarantuneet tiedot sisältävät henkilöiden nimiä, osoitteita, sosiaaliturvatunnuksia, syntymäpäiviä, puhelinnumeroita ja tilinumeroita sekä joitain diagnooseja ja lääketieteellisiä tietoja. (Bowman, 2016b.)
Hakkerointi Banner Health USA 17.6.2016	Haitantekijät saivat haltuunsa 3.7 miljoonan potilaan tiedot palvelimilta. Vuoto havaittiin noin kuukauden päästä oletetusta tapahtumasta. Vaarantuneet tiedot olivat potilaiden nimiä, syntymäaikoja, osoitteita, lääkäreiden nimiä, hoitopäivämääriä, kliinisiä tietoja, mahdollisesti myös sairausvakuutustietoja ja sosiaaliturvatunnuksia sekä edunsaajien tietoja. Kaksi erillistä järjestelmää hakkeroitiin (maksut ja potilastiedot). (Snell, 2016a.)
Hakkerointi North Ottowa Medical Group Bizmatics Banner Health USA 21.7.2016	Haitantekijät saivat haltuunsa 22 000 potilasasiakirjaa kumppanuusyrityksen kautta. Kumppanin kautta vaarantuivat potilaiden nimet, osoitteet, terveystiedot, hoidot, sairausvakuutustiedot ja sosiaaliturvatunnukset. Tapahtuma kautta saattoi vuotaa voi myös luottokortin numeron neljä viimeistä numeroa joillekin potilaiden osalta. Oikeudeton käyttäjä pääsi potilaiden tietoja sisältäviin palvelimiin. (LaPointe, 2016a.)
Hakkerointi Central Ohio Urology Group USA 1.8.2016	Haitantekijät saivat haltuunsa 223 gigatavua dataa: 401 828 tiedostoa, jotka sisältävät 16 646 tekstitiedostoa, 1 1212 ZIP-tiedostoa, 13 RAR-tiedostoa, 108 SQL-tiedostoa, 130 CSV-tiedostoa, 10 BAK-tiedostoa, 33 841 DOC / Docx-tiedostoa, 150 325 XLS / XLSX-tiedostoa, 8 videota tiedostoja, 64,312 pdf-tiedostoa, 1,234 jpg-tiedostoa, 4264 TIF-tiedostoa ja 9 327 .crypt-tiedostoa. Ne sisältävät käyttäjätunnuksia, salasana-, maksu- ja lääketieteellisiä tietoja. Lisäksi datakeskuksen koko arkkitehtuuri on myös vuotaneiden tietojen joukossa. (HACKREAD, 2016.)

Hakkerointi Man Alive USA 24.8.2016	Rikolliset saivat haltuunsa 43 000 asiakirjaa hoitoa antavalta klinikalta. Potilastietokannan tietoja, jossa oli henkilökohtaisia tietoja ja hoitotietoja, myytiin pimeässä netissä (nimet, syntymäaika, sosiaaliturvatunnus, osoite, sähköpostiosoite, puhelinnumerot, pituus / paino / etninen tausta, erialisia lupanumeroita, siviilisääty, ammatti, hoidot, annostus, maksutiedot…). (DataBreaches.net, 2016.)
Hakkerointi Central Ohio Urology Group USA 23.9.2016	Haitantekijät saivat haltuunsa asiakirjoja, jotka käsittelevät 300 000 terveydenhoidon toimijaa tai asiakasta. Se koski potilaita, työntekijöitä ja lääketieteellisiä palveluita tuottavia henkilöt. Tiedot sisältävät nimiä, osoitteita, puhelinnumeroita, sähköposteja, syntymäpäiviä, sosiaaliturvatunnuksia, kuljettajakortin numeroita, potilaan tunnistenumeroita, lääketieteellisiä ja terveyttä koskevia suunnitelmatietoja, tilitietoja, diagnoosi- ja hoitotietoja, sairausvakuutustietoja ja työhön liittyviä tietoja. Ukrainan hakkeri tekee poliittisia tarkoituksia varten SQL-injektioita. (ASC COMMUNICATIONS, 2019b.)
Hakkerointi Community Health Plan of Washington USA 7.11.2016	Haitantekijät saivat haltuunsa lähes 400 000 henkilö tiedot. Tiedoista selviää nimiä, osoitteita, sosiaaliturvatunnuksia ja terveystilaa koskevia tietoja. Ilmoituksen vuodosta teki tytäryritys. (ASC COMMUNICATIONS, 2019c.)
Hakkerointi Emory Healthcare USA 3.1.2017	Haitantekijät saivat haltuunsa 80 000 potilastietuetta. Potilastiedot, kuten nimet, syntymäaika, yhteystiedot, mukaan lukien sosiaaliturvatunnukset, sisäiset lääketieteelliset tietolomakkeet, tapaamisinfo ja eräät taloudelliset tiedot ovat vaarantuneet. (Goud, 2019.)

Hakkerointi The International Association of Athletics Federations Monaco 31.1.2017	Maailmanlaajuisen yleisurheiluliiton (IAAF) hallintoviranomainen on todennut, että organisaatio oli joutunut tietoverkkohyökkäyksen kohteeksi. Sen seurauksena on urheilijoiden lääketieteelliset tiedot vaarantuneet. (Homewood, 2017.)
Hakkerointi Plastic Surgery Clinic Liettua 28.4.2017	Haitantekijät saivat haltuunsa 25 000 potilaan henkilötietoja ja kuvia plastiikkakirurgiaan erikoistuneelta klinikalta. Ne sisälsivät nimiä, osoitteita, puhelinnumeroita, syntymäpäiviä, passiinformaatiota ja myös potilaan alastonkuvia. Rikolliset julkaisivat tiedot myyntiin verkossa (50 - 200 € yksittäisestä tiedosta tai 344 000 € yhteensä). Myös joitakin potilaita on kiristetty erikseen. (Černiauskas, 2017.)
Hakkerointi Chase Brexton Health Care USA 17.10.2017	Haitantekijät saivat haltuunsa 16 562 potilaan tiedot, kun neljä työntekijää joutuivat tietojenkalastushyökkäyksen kohteeksi. Tietojenkalasteluviestit lähetettiin 2. ja 3. elokuuta, ja 4. elokuuta, jonka jälkeen työntekijöiden palkkojen tilitiedot vaarantuivat. Tuntematon tekijä kirjautui sisään näiden neljän työntekijän tileillä ja ohjasi työntekijöiden palkat tuntemattoman henkilö pankkitilille. Potilastietojen vaarantuminen jäi epäselväksi. (DataBreaches.net, 2017b.)
Hakkerointi London Bridge Plastic Surgery & Aesthetic Centre UK 24.10.2017	Korkean kyvykkyyden omaava hakkerointiryhmittymä (Dark Overlord) ilmoitti murtautuneensa plastiikkakirurgiasairaalaan. Rikollisryhmittymä on murtautunut useisiin vastaaviin kohteisiin mm. USA:ssa. Hakkeroidut tiedot saattavat sisältävät yksityiskohtaisia potilastietoja julkisuuden henkilöistä ja jopa kuninkaallisista. (Morley, 2017.)
Muu tapahtuma St. Joseph Health USA 1.2.2011	Organisaatio ilmoitti, että potilastietoja on ollut julkisesti saatavilla internetissä helmikuun 1. päivästä lähtien. 2011. 31 800 potilaan tiedot vaarantuivat; nimet, terveydentila, diagnoosit ja väestötiedot. Potilaat olivat olleet hoidossa useissa eri terveydenhoitopaikoissa. (Bowman, 2016a.)
Muu tapahtuma Children's Medical Center of Dallas USA 4.4.2013	Varastettu tietokone tilasta, jonne oli pääsy ilman kulunseurantaa. Tietokoneen mukana oli 2 462 lapsen terveystietoja, jotka olivat salaamattomia. (HHS, 2017.)

Muu tapahtuma Lucille Packard Children's Hospital USA 1.6.2013	Varastettu kannettavan tietokone, joka sisälsi 12 900 potilastietoa. Kone oli salasanasuojattu ja se varastettiin sairaalan valvotulta alueelta. (Gold, 2013.)
Muu tapahtuma Advocate Medical Group USA 1.7.2013	Varastettuja tietokoneita. Yli neljälle miljoonan potilaan tiedot vaarantuivat. Tiedot sisältävät nimiä, osoitteita, sosiaaliturvatunnuksia ja syntymäpäiviä, mutta ei lääketieteellisiä tietoja. (Gold, 2013.)
Muu tapahtuma University of Washington Medical Center USA 1.10.2013	Tietokonevirus vaaransi 90 000 potilastietoa. Työntekijä avasi sähköpostiliitteen, joka sisälsi haittaohjelmia. Haittaohjelmat vaikuttivat tietokoneeseen, joka sisälsi henkilökohtaisia tietoja potilaista. Potilastietoihin sisältyi muun muassa nimet, puhelinnumerot, osoitteet, lääketieteelliset tietolomakkeet ja sosiaaliturvatunnukset. (The Farber Law Group, 2013.)
Muu tapahtuma Boston Childrens Hospital USA 1.4.2014	Lasten sairaala joutui aktivistiryhmän toteuttaman kohdennetun palvelunestohyökkäyksen vaikutuksen alaiseksi. Samassa verkossa oli useita muita sairaaloita (7), joten vaikutukset laajimmillaan olisivat voineet olla merkittäviä. (Radware Ltd, 2018.)
Muu tapahtuma kolme eri sairaalaa USA 8.6.2013	Hakkerit kaappaavat lääkinnällisiä laitteita ja siten pystyivät luomaan virusohjelman avulla takaportteja sairaalan verkkoihin pääsylle. Hyökkääjät tarttuvat haittaohjelmia lääketieteellisiin laitteisiin ja liikkuvat sitten sivusuunnassa sairaalaverkkojen kautta varastaakseen luottamuksellisia tietoja. Näitä laitteita olivat röntgenlaitteet, kuva-arkisto- ja viestintäjärjestelmät ja veren kaasuanalysaattorit. Turvajärjestelyjen puutteet laitteissa mahdollistavat pääsyn työasemille. Toimintaa voi liittyä myös tietojen manipulointia laitteilla. (Storm, 2015.)

Muu tapahtuma Hurley Medical Center USA 21.1.2016	Hakkeriryhmä kohdistui palvelunestohyökkäyksen terveydenhoito-organisaatioon pian sen jälkeen, kun se oli julkaissut videon vaatien "oikeudenmukaisuutta" kaupungin jatkuvaan vesikriisiin Potilastiedot eivät vaarantuneet. (Miliard, 2016.)
Muu tapahtuma California Correctional Institute USA 25.2.2016	Työntekijän salakirjoittamaton, salasanalla suojattu kannettava tietokone varastettiin työtekijän omasta ajoneuvosta. Tietokone sisälsi vuosien 1006-2014 väliseltä ajalta huomattavan määrän potilastietoja. Tietoihin saattoi sisältyä potilaiden tunnistustietojen lisäksi ja mm. heidän luottamuksellisia lääketieteellisiä tietoja ja mielenterveyttä koskevia tietoja. (State of California, 2019.)
Muu tapahtuma Blue Ridge Surgery Center USA 17.3.2016	Kannettava tietokone varastettiin työntekijän kotoa. Laite sisälsi potilaiden tunnistetietoja ja terveystietoja. Tietokoneessa saattoi olla myös sähköposteja, jotka sisältävät potilaista nimet, osoitteet, hoito-ohjeet, vakuutusyhtiötiedot, tunnistenumerot ja sosiaaliturvatunnukset. (LaPointe, 2016b.)
Muu tapahtuma Medical Colleagues of Texas USA 17.3.2016	Kannettavan tietokoneen varastaminen johti noin 50 000 potilaan ja henkilökunnan tietojen vaarantumiseen, kun varastettu tietokone sisälsi terveydenhoito-organisaation verkkosalasanan. Potilas- ja henkilökuntatietoja kuten nimiä, osoitteita, hoitotietoja, vakuutustietoja, henkilötunnisteita ja sosiaaliturvatunnuksia on voinut joutua ulkopuoliselle taholle. (LaPointe, 2016b.)
Muu tapahtuma Imperial Valley Family Care Medical Group USA 21.3.2016	Lääkäreiden toimistosta varastettu kannettava tietokone sisälsi potilastietoja, kuten nimiä, osoitteita, syntymäpäiviä, terveystietoja, sosiaaliturvatunnuksia, kuljettajan lisenssitietoja ja henkilöllisyystodistustietoja. Noin 4 100 potilaan tiedot vaarantuivat. (LaPointe, 2016b.)

Muu tapahtuma Bon Secours Health System USA 18.4.2016	Terveydenhuoltoalan yritysasiakas jätti potilastiedot alttiiksi neljän päivän ajaksi verkkohyökkäykselle verkkoasetuksien muuttamisen yhteydessä. Tiedot sisälsivät nimiä, sosiaaliturvatunnuksia, vakuutustietoja ja pankkitietoja sekä joitain kliinisiä tietoja. Kaiken kaikkiaan 655 000 potilaan tiedot vaarantuivat. (Bryant, 2016.)
Muu tapahtuma North Ottowa Medical Group USA 21.7.2016	Asiaan kuulumaton käyttäjä pääsi potilastietoja sisältäviin palvelimiin terveydenhuollon palveluja toimittavan kumppanin toimien seurauksena. Toimija ei voinut vahvistaa, olivatko kohdeorganisaation potilastiedostot olleet mukana tapahtumassa, mutta siitä aiheutui uhka noin 22 000 potilaan osalle. Potilastiedot, jotka ovat olleet vaarassa sisältävät nimiä, osoitteita, terveystietoja, hoitotietoja, sairausvakuutustietoja ja sosiaaliturvatunnuksia. Tapahtuma on voinut altistaa myös luottokortin neljä viimeistä numeroa tietovuodolle joillekin potilaiden osalta.(LaPointe, 2016b.)
Muu tapahtuma Kaiser Permanente USA 21.7.2016	Useiden ultraäänilaitteiden varkaus aiheutti potentiaalisen terveydenhuollon tietoturvauhan, joka koski 1100 toimijaa jotka integroidun hoitoprosessin kautta ylläpitävät terveydenhuoltoa 9 miljoonalle henkilölle. Käytössä olevan tiedon mukaan kaksi entistä työntekijää varastivat julkistamattoman määrän ultraäänilaitteita. Varastettujen laitteiden palauttamisen yhteydessä selvisi, että laitteet sisälsivät potilastietoja kuten nimiä, lääketieteelliset tietoja ja kuvia. (LaPointe, 2016b.)
Muu tapahtuma Appalachian Regional Healthcare USA 1.9.2016	Kahdessa sairaalassa jouduttiin ajamaan kaikki järjestelmät alas, mukaan lukien potilaan hoitoon, rekisteröintiin, lääkitykseen, kuvantamiseen ja laboratorioon liittyvät palvelut kuudeksi päiväksi. Tapauksen osalta ei tiedetä, onko potilastietoja käytetty väärin (tiedot, pankkitiedot, sosiaaliturvatunnukset, syntymäaika ja lääketieteelliset tiedot). Sammuttamalla kaikki tietokoneet estettäisiin viruksen leviäminen sairaaloissa. (Davis, 2016.)

Muu tapahtuma Kela Kanta palvelut Suomi 14.10.2016	Valtakunnallisen Kanta-palvelun toiminta estyi saman päivän aikaan kahdesti noin tunniksi. mm. sähköinen resepti ei toiminut. Kanta-palvelu joutui palvelunestohyökkäyksen kohteesi. (MTV Uutiset, 2016.)
Muu tapahtuma Red Cross Blood Service Austraalia 18.10.2016	Tietokannan varmuuskopion kautta on vuotanut potilastietoja, kun varmuuskopio oli nähtävissä julkisesti organisaation verkkosivuilla. Tiedot ovat peräisin verenluovutuksesta ja ovat: nimi, sukupuoli, osoite, sähköpostiosoite, puhelinnumero, syntymäaika, veriryhmä ja joissain tapauksissa syntymämaa, luovutustyyppi (plasma, verihiutale, verihiutaleiden verenkierto). (Hunt, 2016.)
Muu tapahtuma Barts Health NHS Iso-Britannia 13.1.2017	Sairaalan patologinen järjestelmä otettiin pois käytöstä muutamaksi päiväksi ennalta tuntemattoman viruksen aiheuttaman haitan takia. Sairaala sanoi, että potilastiedot eivät vaarantuneet. Virustentorjuntaohjelmisto oli ollut ajan tasalla, muta kyseessä oli uusi virus, jota ei ollut aiemmin havaittu. (Palmer, 2017.)
Muu tapahtuma Kela Kanta palvelut Suomi 4.6.2017	Kaksi palvelunestohyökkäystä vaikeutti Kanta-palvelujen toimintaa. Ensimmäinen häiritsi palveluita 2,5 tuntia ja toinen hyökkäys seuraavana päivänä keskeytti palvelut 4 tunniksi. Häiriöt vaikeuttivat asiakkaiden pääsyä Kanta.fi-, Omakanta- ja Kelain-verkkopalveluihin. Sähköisten reseptien käyttö estyi. (Finnish News Network, 2017.)
Muu tapahtuma Washington Health System Greenerecently USA 11.10.2017	Tietokoneen ulkoisen kovalevyasema varastettiin sairaalan radiologian osastolta. Se sisälsi potilastiedot 4 145 potilaasta. Aseman sisältämät tiedot, kuten nimet, korkeus, paino, etninen tieto ja sukupuolen vaarantuivat. Lisäksi potilaan terveydenhoidon rekisterinumero, terveyskyselytieto, lääkemääräykset ja hoitavan lääkäri sisältyvän joihinkin potilastietoihin. (DataBreaches.net, 2017c.)

Muu tapahtuma UNC Health Care USA 8.12.2017	Henkilökohtaiset potilastiedot sisältyivät tietokoneen kiintolevyyn, joka oli varastettu. Tietokone oli salasanasuojattu. 24 000 potilaan tiedot vaarantuivat. Tietokoneen potilastietokanta sisälsi potilaiden nimet, syntymäpäivät, sosiaaliturvatunnukset, osoitteet, puhelinnumerot, työkykytiedot ja työnantajien nimet. (Murawski, 2017.)
Muu tapahtuma Laden kaupunki Suomi 9.2.2018	Virtuaalivaluuttaa louhiva haittaohjelma saastutti Lahden kaupungin tietojärjestelmän – terveyskeskukset ruuhkautuivat. Lahdessa on ollut vakavia tietojärjestelmäongelmia kaupungin tietoverkkoon levinneen haittaohjelman takia. Terveyskeskusten potilastietojärjestelmät ovat olleet pois käytöstä, kaupungin nettisivut kaatuivat eivätkä kirjaston verkkopalvelut ole toimineet. (Pirkkalainen, 2018.)

Informaatioteknologian tiedekunnan julkaisuja
No. 75/2019

ISBN 978-951-39-7699-6 (verkkoj.)
ISSN 2323-5004

JYVÄSKYLÄN YLIOPISTO