Kyberturvallisuus sosiaali- ja terveydenhuollossa

Martti Lehto
Jouni Pöyhönen
Miikael Lehto

Kyberturvallisuus sosiaali- ja terveydenhuollossa

Loppuraportti
Vol. 2

JYVÄSKYLÄN YLIOPISTO

Value From Public Health Data With Cognitive Computing (VFH) ja
Watson Health Cloud Finland (WHC) -hankkeiden (2016–2019) loppuraportti, Vol. 1–4.

Editointi ja taitto: Timo Siukonen, Siukin Sanomat.

Kansien suunnittelu: Keijo Halttunen.

ISBN 978-951-39-7710-8 (nid.)
ISBN 978-951-39-7711-5 (verkkoj.)

Kustantaja: Jyväskylän yliopiston IT-tiedekunta.

Painopaikka: Yliopistopaino, Jyväskylä (2019).

Tämä julkaisu on toteutettu osana VFH- ja WHC-hankekokonaisuutta, johon
Jyväskylän yliopisto on saanut päärahoituksen Business Finlandilta.

SISÄLLYS

Kyberturvallisuus sosiaali- ja terveydenhuollossa

Hankekokonaisuuden loppuraportti koostuu neliosaisesta kirjasarjasta:

Vol. 1: Tekoäly ja terveydenhuolto Suomessa.

Vol. 2: Kyberturvallisuus sosiaali- ja terveydenhuollossa.

Vol. 3: Interventiot ja tekoäly terveydenhuollossa.

Vol. 4: Suomen terveysdata ja sen hyödyntäminen.

JOHDANTO

Tässä kirjassa raportoidaan Tekoäly ja terveydenhuolto Suomessa -hankekokonaisuuden tuloksista, mikä muodostui kahdesta osahankkeesta: Value from Public Health Data with Cognitive Computing (VFH) ja Watson Health Cloud Finland (WHC). Nämä aiheet liittyvät ajankohtaiseen Suomen SOTE-järjestelmän uudistamiseen.

Hankkeissa tutkittiin, kuinka tekoälyn keinoin voidaan hyödyntää terveysdatan käyttöä, palveluprosessien tehostamista sekä omaehtoisen terveydenhoidon ja hyvinvoinnin liittämistä osaksi kansalaisten arkipäivän toimintoja. Hankkeissa tutkittiin myös, miten digitalisaatioon liittyvää lisääntyvää terveysdataa voidaan hyödyntää tekoälyn avulla yksilö - ja maakuntatasolla sekä kansallisesti. Lisäksi tutkittiin kyberturvallisuutta sosiaali- ja terveydenhuollossa ja sairaalaympäristössä.

Kirjasarjan toisessa osassa käsitellään kyberturvallisuutta sosiaali- ja terveydenhuollossa sekä sairaalaympäristössä ja millaisilla arkkitehtuuriratkaisuilla uhkia voidaan torjua.

Tiivistelmään on koottu keskeiset havainnot ja johtopäätökset tehdyistä tutkimuksista. Ensimmäisessä luvussa esitellään kyberturvallisuuden perusteita erityisesti sosiaali- ja terveydenhuollon toimintaympäristössä. Toisessa luvussa esitellään pelkistetysti kansallinen SOTE IT -järjestelmä. Kolmannessa luvussa käsitellään sairaalan kybertoimintaympäristöä, sen laitteita ja järjestelmiä sekä niihin liittyviä kyberturvallisuusnäkymiä ja esitetään sairaalajärjestelmien kyberrakennemalli.

Neljäs luku käsittelee terveydenhuollossa todettuja kyberuhkia, kyberhyökkäyksiä sairaaloihin, lääkinnällisiä laitteita kyberturvallisuuden näkökulmasta sekä sairaalaa kyberhyökkäyskohteena. Viidennessä luvussa esitellään sairaalan kyberturvallisuuden perusteita, parhaita käytäntöjä ja lääkinnällisten laitteiden kyberturvallisuuden perusteita.

Kuudennessa luvussa määritellään tarve sairaalan kyberturvallisuuden arkkitehtuurille ja luodaan sen rakennemalli. Seitsemännessä luvussa esitellään toimenpiteitä sairaalan kyberturvallisuuden edistämiseksi ja millaisia mahdollisuuksia IBM:n tuottamat ratkaisut voivat antaa. Kahdeksannessa luvussa käsitellään pelkistetysti SOTE-lainsäädäntöä. Luvussa 9 esitellään tutkimuksen perusteella käyttäjäkokemuksia liittyen käyttäjien näkemyksiin terveystietojen yksityisyydestä ja tietojen jakamisesta heidän omista hyvinvointilaitteistaan.

Esittelemme tässä kirjassa tuloksia, jotka ovat tärkeitä SOTE- ja sairaalaympäristön kyberturvallisuuden kehittämiseksi. Kyberturvallisuutta käsittelevät raportit löytyvät hankkeen julkaisusarjan verkkosivuilta osoitteesta www.jyu.fi/it/julkaisut/tekes/.

Kiitokset johtoryhmälle, rahoittajille, yhteistyöverkostolle ja hankkeeseen osallistuneille tutkijoille sekä Timo Siukoselle tämän kirjan editoinnista ja taitosta.

Maaliskuussa 2019

Martti Lehto
ST, kyberturvallisuuden työelämäprofessori

Jouni Pöyhönen
Projektitutkija, tohtorikoulutettava

Miikael Lehto
Projektitutkija

TIIVISTELMÄ

Yleinen teknologian ja digitalisaation nopea kehittyminen näkyy myös terveydenhuollossa, minkä seurauksena 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.

Viime vuosina terveydenhuoltoon on kohdistunut merkittäviä datamurtoja. Esimerkiksi vuonna 2018 tietomurron kohteeksi joutui Yhdysvalloissa 13,3 miljoonaa potilastietoa (nimiä, sosiaaliturvatunnuksia, puhelinnumeroita, osoitteita, luottokorttitietoja ja myös terveystietoja).

Tämän tutkimuksen tausta-aineistoksi tutkittiin pääosin vuosina 2013–2018 raportoituja kyberhyökkäyksiä. Niissä korostuvat tietojen kalastelumenetelmät, kiristysohjelmat, palveluestohyökkäykset, hakkeroinnit, virusohjelmat ja laiteiden 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 kyberfyysiseen 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, kiristäneet yrityksiä ja 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 osalta. 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. 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 tutkimus ottaa huomioon sairaalan eri päätöksentekotasoilla tarvittavien kyberturvallisuustoimenpiteiden tarpeellisuuden, mutta keskittyy pääosin sairaalaympäristön teknillistaktisen 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. Kybersuojausta lähestytään systeemiajattelun kautta rakentuvien turvallisuusratkaisujen aikaansaamiseksi.

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.

Terveydenhuoltoalalla tietojenkäsittelyyn kohdistuu aivan erityisiä vaatimuksia. Potilastietojen eheys ja saatavuus ovat äärimmäisen tärkeitä potilaiden turvallisen hoidon kannalta. Toisaalta tietojen luottamuksellisuutta on suo-

jattava paitsi yksityisyyden suojan takaamiseksi, myös henkilötietojen rikollisen käytön estämiseksi. Sairaalaympäristön toimivuus on kriittisen tärkeää potilaiden hoidolle, mikä asettaa muun muassa sairaalarakennusten kiinteistöautomaation kyberturvallisuuden tärkeään asemaan.

Terveydenhuoltoa kohtaan tapahtuu perinteisiä hyökkäyksiä kuten hakkerointeja ja viruksia, laitteiden varastamista sekä hajautettuja palvelunestohyökkäyksiä (DDoS). Näillä hyökkäyksillä on merkittäviä vaikutuksia terveydenhuollossa, koska toiminta vaatii usein reaaliaikaisen pääsyn palveluihin kuten potilastietojärjestelmiin tai sähköisiin resepteihin. Huolestuttavaa on, että usein hyökkäyksiä ei huomata ennen kuin usean kuukauden päästä, jolloin tutkinta on vaikeaa ja isoja määriä tietoja on jo voinut päätyä rikollisten käyttöön. Kiristyshaittaohjelmahyökkäyksissä tartunta selviää nopeasti, mutta näissäkin tapauksissa palveluiden palauttaminen normaalitilaan voi kestää useita päiviä riippuen järjestelmän koosta, tartunnan laajuudesta ja varmuuskopiojärjestelyistä.

Tarkasteltaessa kyberhyökkäyksiä sairaaloita ja muita SOTE-alan toimijoita kohtaan viimeisen viiden vuoden aikana nousevat kiristyshaittaohjelmat ja hakkerointi yleisimmiksi tapauksiksi (ks. liite 4). Tässä tutkimuksessa koottiin ja analysoitiin 65 tapausta, jotka jakautuivat hyökkäysvektoreiden perusteella seuraavasti:

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

Finanssialan yritykset ovat edelleen hyökkäyksien kohteena, mutta rikolliset ovat siirtäneet huomiotaan terveydenhuoltoon sen sisältämien potilastietojen ja muiden arvokkaiden tietojen vuoksi. Rikolliset voivat myydä potilastietoja, jotka ovat perinteisiä luottokorttitietoja arvokkaampia niiden tiedon määrän ja laadun vuoksi. Kiristyshaittaohjelma hyökkäykset ovat myös tuoneet esiin kuinka elintärkeitä potilastietojärjestelmät ovat sairaaloiden toiminnalle, joten organisaatiot ovat valmiita maksamaan lunnaita, jotta saavat tietonsa takaisin käyttöön.

Terveydenhuoltoalan nouseminen tietomurtojen ykköskohteeksi selittyy myös sillä, että kohdetta pidetään ”pehmeänä”, ts. sairaalat ovat heikosti varautuneet kyberhyökkäyksiin. Yhdysvalloissa eri toimialat käyttävät 5–15 % IT-menoistaan kyberturvallisuuteen, mutta SOTE-alalla vain 3 %.

Teknologiamarkkinoiden kasvu vaikuttaa siihen, kuinka yksilöt keräävät ja säilyttävät omia terveystietojaan. Ennen nykyisiä tekniikoita terveystieto tallennettiin vain lääketieteellisiin tiedostoihin, jotka olivat saatavilla vain terveydenhuollon ammattilaisille. Nyt terveystietoja tallennetaan useisiin eri paikkoihin, mukaan lukien henkilökohtaiset kannettavat laitteet, älypuhelimet ja pilvipalvelut, joita eri organisaatiot tarjoavat. Koska terveystietopalvelut ovat hajautuneet ja yksilöillä on helpompi pääsy tietoihinsa, tämä on tuonut esiin uusia yksityisyyden suojaa koskevia kysymyksiä ja riskejä.

Tutkimuksessa ilmeni, että henkilöt eivät pidä aktiivisuusrannekkeiden tietoja yksityisinä tai arkaluontoisina vaan enemmän yleisinä. Toisaalta henkilöiden mielestä heidän lääkäreillänsä olevat terveystietonsa ovat hyvin yksityisiä ja sensitiivisiä. Lääkäreillä olevat tiedot

koettiin yksityiskohtaisiksi, koska ne sisältävät henkilökohtaista tietoa sekä numeerisessa että kirjallisessa muodossa. Tutkimuksessa selvisi, että käyttäjät eivät jaa aktiivisuusrannekkeidensa tietoja sosiaalisessa mediassa. Käyttäjät olivat valmiita antamaan keräämiään tietoja lääkärille, mikäli niistä olisi hyötyä heidän terveydenhoidossaan sekä työterveyshuollon käyttöön. Käyttäjät olivat myös valmiita antamaan tietojaan lääketieteelliseen tutkimukseen sekä antamaan laitevalmistajan käyttää heidän tietojaan tuotteiden ja palveluiden kehittämiseen.

LUKU 1

Kyberturvallisuuden perusteita

Digitalisaation vaikutukset koskevat laajasti niin yksilöitä, organisaatioita, yrityksiä kuin yhteiskuntaa yhteisesti. Digitalisaatiossa integroidaan digitaalitekniikka osaksi elämän jokapäiväisiä toimintoja ihmisten arjessa ja työelämässä. Digitalisaatiossa on kyse yhteiskunnallisesta prosessista, jossa hyödynnetään teknologisen kehityksen uusia mahdollisuuksia. Digitalisaatio on luonut spesifisiä ilmiöitä, luonut erilaisia toimintaympäristöjä ja mahdollistanut käyttäytymistä, joita ei ole ennen digitaalista aikaa. (Lehto & Neittaanmäki 2016, 56–64.)

Digitalisaatiosta on tullut yhä tärkeämpi osa yritysten ja ihmisten toimintaa. Digitaalisuus vaikuttaa yhä syvemmällä ihmisten ja yritysten arjessa; digitaaliset palvelut helpottavat yritysten ja ihmisten arkea ja elämää.

Digitaalisuuteen pohjautuvia innovaatiomahdollisuuksia syntyy yhä enemmän. Näköön, kuuloon ja kosketukseen perustuvat teknologiat luovat uusia mahdollisuuksia ja tapoja käsittää maailma ja olla yhteyksissä maailman kanssa aivan uudella tavalla. Tavaroista ja palveluista tulee älykkäämpiä ja ne liittyvät toisiinsa sekä ihmisiin aivan uusilla tavoilla. Myös yritykset voivat luoda syvempiä reaaliaikaisia suhteita kumppaneihin, asiakkaisiin, palvelun- ja tavarantoimittajiin sekä julkishallintoon.

Samaan aikaan digitalisaation seurauksena syntyy yhä uudenlaisia uhkia. Digitaalinen kybermaailma houkuttelee rikollisia, jotka etsivät uusia mahdollisuuksia varastaa, hyödyntää ja myydä tietoa. Tiedon ja informaation siirtyminen verkkoon on tuonut sinne myös tiedusteluorganisaatiot. Terroristeille kybermaailma on yhteydenpidon, viestinnän ja vaikuttamisen toimintaympäristö, minkä lisäksi se on heille houkutteleva hyökkäyskohde.

Asevoimien digitalisaatio on luonut sotilaallisen kybermaailman, jossa vaikuttavat verkottuneiden sotilaiden lisäksi älykkäät ja yhä itsenäisemmät asejärjestelmät.

Digitaalinen murros perustuu ihmisten muuttuneisiin odotuksiin, yhteiskunnan palvelurakenteiden ja -tuotannon kasvaneisiin tehokkuusvaatimuksiin ja teknologioiden tarjoamiin mahdollisuuksiin. Uudet teknologiat, työkalut ja toimintatavat muuttavat ihmisten tapaa toimia arjessa ja työssä, organisaatioiden tapaa toteuttaa tehtäviään ja julkishallinnon tapaa tuottaa palveluita. (Lehto & Neittaanmäki 2016, 56–64.)

Tekniikan nopea kehittyminen perustuu digitalisaation aikaan saamaan ”kierteeseen”, jossa 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.)

Mitä tarkoittavat *kyber* ja *kyberturvallisuus?* Kyber tarkoittaa ympärillämme olevaa digitaalista biteistä koostuvaa keinotekoista maailmaa, johon kuuluvat muun muassa internet ja sosiaalinen media, erilaiset tietoverkot- ja järjestelmät, älylaitteiden ohjelmistot jne. Kybersana tulee kreikankielisestä sanasta kybereo tarkoittaen ohjaamista, opastamista ja hallitsemista.

Kyberturvallisuus yleisesti viittaa kykyyn kontrolloida pääsyä verkossa sijaitseviin järjestelmiin ja informaatioon, joita ne sisältävät. Kyberturvallisuuden kontrollien ollessa tehokkaita, myös kyberavaruutta voidaan pitää varmana, joustavana ja luotettavana digitaalisena infrastruktuurina. Kyberturvallisuus viittaa teknologioihin, prosesseihin ja käytänteisiin, jotka on suunniteltu suojelemaan verkkoja, laitteita, ohjelmia, dataa hyökkäyksiltä, vahingoilta tai luvattomalta käytöltä. Kyberturvallisuutta voidaan myös kutsua informaatioteknologian turvallisuudeksi. Kyberturvallisuus on tietokoneiden ja palvelinten, mobiililaitteiden, elektronisten järjestelmien, verkkojen ja datan turvaamisen menetelmiä haitallisia hyökkäyksiä vastaan. Termi on laaja-alainen ja soveltuu kaikkeen tietokoneiden turvallisuudesta katastrofeista toipumiseen ja loppukäyttäjien koulutukseen saakka.

Terveydenhuollon tietojärjestelmien toimivuuden turvaaminen on osa yhteiskunnan turvallisuusstrategiaan kuuluvaa talouden, infrastruktuurin ja huoltovarmuuden varmistamista. Yhteiskunnan varautumisen tavoitteena on turvata elintärkeät toiminnot niin normaaliolojen häiriötilanteissa kuin poikkeusoloissakin. Elintärkeillä toiminnoilla tarkoitetaan ”yhteiskunnan toimivuuden kannalta välttämättömiä, kaikissa tilanteissa ylläpidettäviä toimintokokonaisuuksia”. Lähtökohtana on se, että asiakas- ja potilastietojen lisäksi myös kansallisten sosiaali- ja terveydenhuollon (SOTE) tietovarantojen, erilaisten digitaalisten diagnostisten palveluiden sekä verkkoihin kytkettyjen laitteiden kyberturvallisuus on varmistettava. Terveydenhuollon organisaatioiden tuleekin varautua hybridivaikuttamisen ja kyberuhkien eri muotoihin. (Yhteiskunnan turvallisuusstrategia, 2017)

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 teknillistaktisen tason järjestelmiin tunkeutumiselle, joista on suora yhteys kyberfyysiseen 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) 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. (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, ym. 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 internetiin 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.)

LUKU 2

Kansallinen SOTE IT -järjestelmä

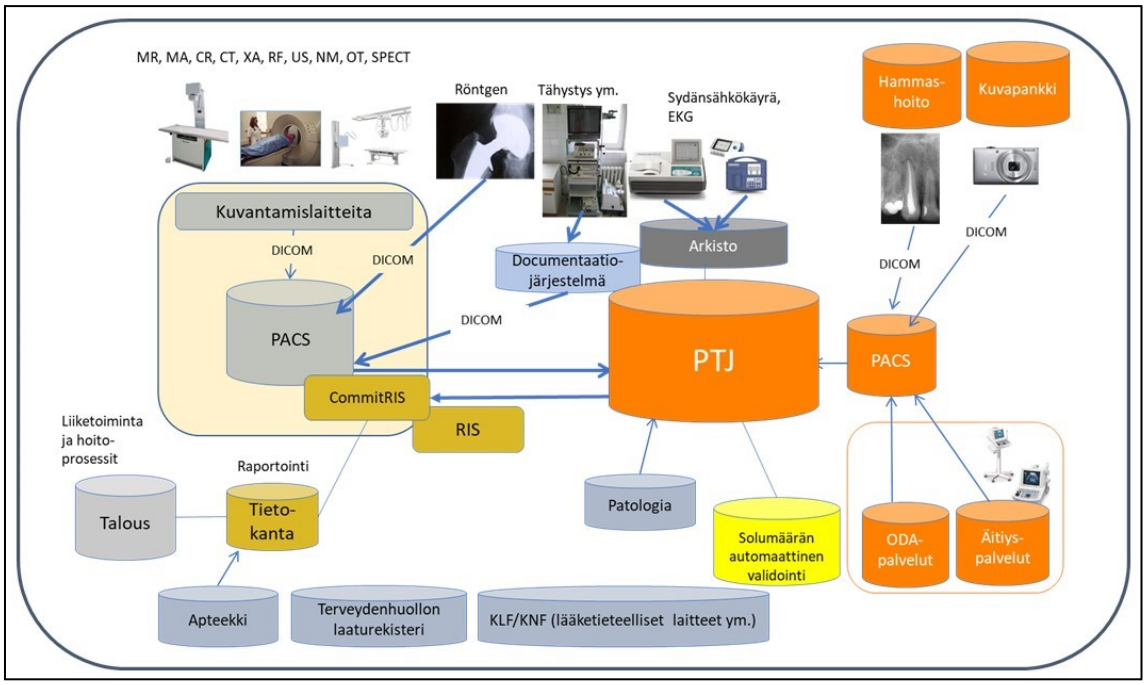
Sosiaali- ja terveyspalveluiden infostruktuuri sisältää ICT-palvelut, alustat sekä sisällölliset ja tekniset standardit ja määrittelyt, jotka tukevat tiedonjakoa ja yhteen toimivuutta. Kansalaisen aktivointiin, palvelujärjestelmän tehostamiseen ja tietojen toissijaiseen käyttöön liittyvät strategiset tavoitteet edellyttävät, että tietotekniset ratkaisut rakennetaan avoimelle ja skaalautuvalle pohjalle yhteisesti sovittuja menettelytapoja noudattaen.

Kokonaisuuden on oltava modulaarinen, avoin ja hallitusti kehitetty, ja sen on mahdollistettava sekä palvelujen, rakenteiden että teknisten ratkaisujen uudistaminen. Tämä edellyttää myös yhteistyöhön nojautuvaa ja verkostomaista ratkaisujen kehittämistapaa, jossa kannustetaan kokeilemaan erityyppisiä ratkaisumalleja ja kokoamaan näyttöä sellaisista ratkaisuista, jotka tuottavat haluttuja vaikutuksia. Näytön pohjalta vaikuttavia ratkaisuja levitetään tehokkaasti laajamittaiseen käyttöön ja niiden pohjalta kehitetään myös uusia palveluita ja tuotteita. (Sitra verkkosivut)

Terveyteen ja hyvinvointiin liittyvää tietoa kertyy reaaliajassa valtavat määrät eri lähteistä, kuten esimerkiksi liikkumista mittaavista rannekkeista, implanteista ja muista terveyden ja lääketieteen laitteista.

Kuvassa 1 on esitetty esimerkinomaisesti merkittävimmät datalähteet Keski-Suomen sairaanhoitopiirin sairaalassa.

Ihminen tuottaa elinaikanaan keskimäärin yli miljoona gigatavua terveyteen liittyvää dataa.



KUVA 1: Geneerinen sairaalan tietojärjestelmäkokonaisuus (KSSHP).

DICOM Lääketieteellisen kuvadatan siirtoon käytetty sovellustason standardi (Eng. Digital Imaging and Communications in Medicine)	PACS Lääketieteellisten kuvien arkistointijärjestelmä (Eng. Picture Archiving and Communication System)	RIS Kuvantamisen toiminnanohjausjärjestelmä (Eng. Radiology Information System)
ODA Omahoito ja digitaaliset palvelut	KFI kliininen fysiologian ja isotooppilääketiede (Eng. Clinical Physiology and Isotope Medicine)	KNF kliininen neurofysiologia (Eng. Clinical neurophysiology)

TAULUKKO 1: Alan suomen– ja englanninkielisiä lyhenteitä.

Lisäksi käytettävissä ovat perinteiset tietolähteet, kuten potilas- ja perimätiedot. Data on pirstaloitunut sinne tänne, eikä sitä ole helppo jakaa tai analysoida.

SOTE-tietojärjestelmäkokonaisuudessa on noin 400–800 järjestelmää, näiden välisiä liityntöjä yli 500, käyttäjiä noin 10 000 (SOTE-alalla työntekijöitä 200 000), järjestelmäomistajia 10–100.

Potilastietojärjestelmien kokonaisuus on noin 10 % koko lukumäärästä. Jokainen erikoisala tarvitsee omat erikoisjärjestelmät (niiden toimittajia on maailmalla vain muutama). Myös uudessa SOTE IT -järjestelmässä tulee olemaan edelleen reilut 200 järjestelmää, vaikka niitä yhdistettäisiinkin ja vanhasta SOTE-järjestelmästä jäisi iso osa käyttöön.

Sairaaloissa on monia digitaalisia terveydenhuollon järjestelmiä, jotka ovat käytännössä automaatiojärjestelmiä. Potilaiden elintoimintoja mittaavat laitteet voivat kerätä tietoja potilaista ja lähettää hoitohenkilökunnalle tietoja ja hälytyksiä huomiota vaativista tilanteista tietoverkon yli. Lääkepumput voivat ottaa vastaan tietoja potilaille annettavista lääkemääristä ja muuttaa toimintaansa saamiensa tietojen perustella. Lisäksi tulevat monet kiinteistöautomaatiojärjestelmät, joiden toiminnalla voi olla suuri merkitys potilaiden terveydelle.

Automaatiojärjestelmien yhteinen piirre on, että ne koostuvat herkistä laitteista, jotka digitaalisen tiedon varassa vaikuttavat fyysiseen maailmaan tai muuttavat fyysisestä maailmasta tekemiään havaintoja digitaaliseksi tiedoksi päätöksentekoa varten. Laitteiden odotetaan toimivan tosiaikaisesti. (Viestintävirasto, 2016)

LUKU 3

Sairaala kybertoimintaympäristönä

3.1 Sairaalan tietojärjestelmät ja laitteet

Yleistä sairaalajärjestelmistä ja -laitteista

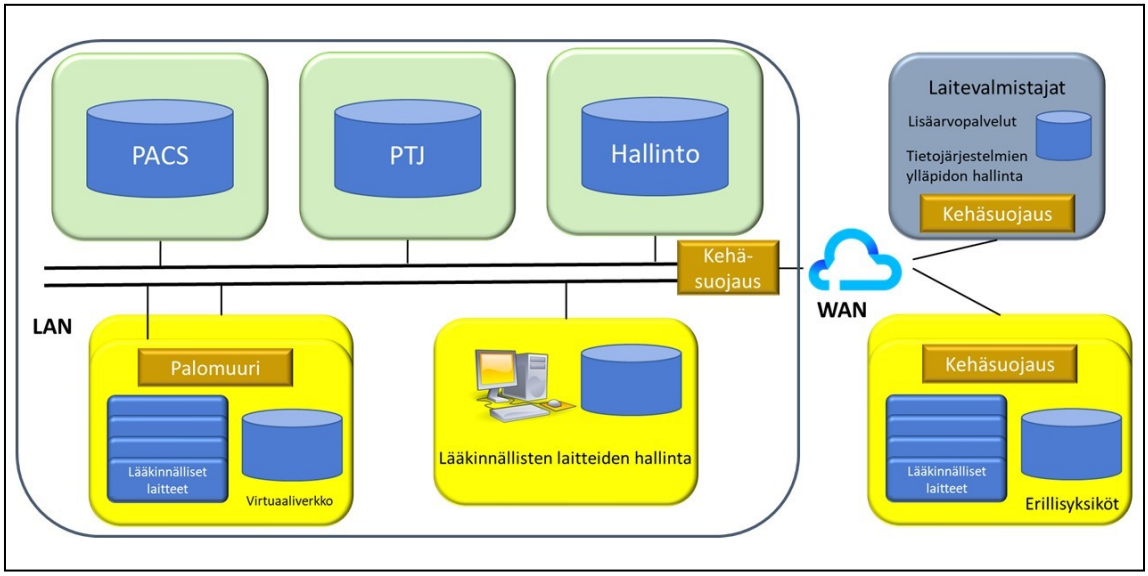
Sairaalaympäristön toimivuus edellyttää useiden erilaisten tietojärjestelmä- ja automaatiojärjestelmäkokonaisuuksien hyödyntämistä. Niitä voidaan tunnistaa tarvittavaksi ainakin neljän eri prosessin alueella. Järjestelmät yleisellä tasolla ovat:

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.

Kuvassa 2 on esitetty geneerinen rakenne sairaalan tietojärjestelmästä.

Terveydenhuollon tietojärjestelmistä keskeisimpiä ovat potilastietojärjestelmät. Potilastietojärjestelmien ydinjärjestelmiä käytetään sairaaloissa laajasti. Ydinjärjestelmiä ovat mm. 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.



KUVA 2: Geneerinen sairaalan tietojärjestelmäkokonaisuus. (Integrating the Healthcare Enterprise, 2015, 21).

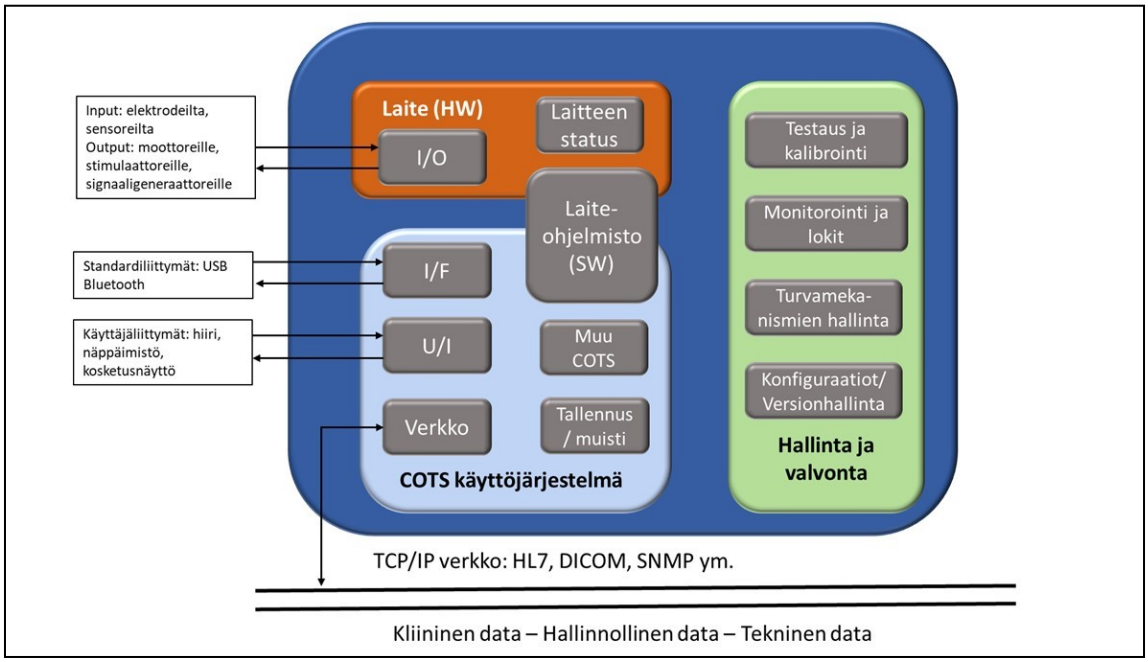
Edellä mainittujen tietojen lisäksi potilastietojärjestelmiin tallennetaan yhä enemmän potilaan hoidollisia tietoja kuten hoitoon tulon syy, hoidon tavoitteet, tehdyt toimenpiteet ja tutkimukset, erilaiset lausunnot, suunnitelmat, hoito-ohjeet, hoitopalautteet ja epikriisit (hoitotiivistelmät).

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 mm. matkapuhelimet, tablettitietokoneet ja erilaiset puettavat laitteet, joihin liittyy lääkinnällisiä sovelluksia/ohjelmistoja. Tällaisia laitteita on jo löydettävissä kodeista.



KUVA 3: Geneerinen lääkinnällisten laitteiden arkkitehtuuri. (Integrating the Healthcare Enterprise, 2015, 16).

Kuvassa 3 on esitetty geneerinen malli lääkinnällisten laitteiden arkkitehtuurista ja keskeisistä komponenteista kyberturvallisuuden näkökulmasta.

Laitteissa käyttöjärjestelmä perustuu usein kaupallisiin arkkitehtuureihin ja myös niihin liittyvä laitteistoalusta (Commercial off-the-shelf, COTS). Käyttöjärjestelmä voi käyttää kaupallisia laitteistokomponentteja (emolevy, tietokone) ja myös käyttäjälle räätälöityjä alustoja.

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).
* Liitteessä 1 on ote WHO:n listauksesta lääkinnällisistä laitteista.

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.)

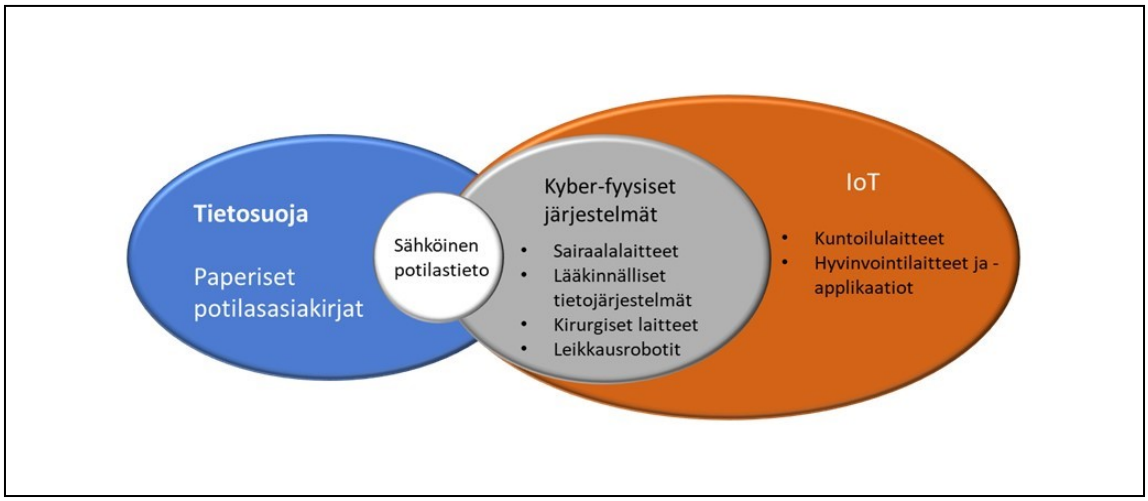
Kyberturvallisuuteen liittyvät uhkatekijät, kuten kyberhyökkäykset em. infrastruktuuria vastaan, ovatkin merkittävästi lisääntyneet. Lääkinnällisten laitteiden kyberturvallisuudesta onkin tullut ensisijainen terveydenhuollon turvallisuushuoli useiden potentiaalisesti haitta-asteeltaan vakavien tapahtumien 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 seuraavalla sivulla kuvassa 4. (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.



KUVA 4: Terveydenhuollon toimintaympäristö.

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 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 antoi äskettäin suosituksia uusista tietoturvastandardeista ja toimintapuitteista.

Suositukset eivät kuitenkaan käsitelleet edelleenkään potilasturvallisuutta eikä lääkinnällisiä laitteita. (Piggin, 2017, 5.)

Sairaalaympäristö kyberhyökkäyskohteena

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

Vuonna 2018 Yhdysvalloissa terveydenhuollon järjestelmiin kohdistui 365 tietosuojaloukkausta. Niistä 158 oli hakkerointeja sairaaloiden IT-järjestelmiin (noin 9 miljoonan tiedot kohteena), 143 tapausta aiheutui luvattomasta pääsystä tietojärjestelmiin (noin 3 miljoonan tiedot kohteena), 55 tapauksessa kyse oli varastetuista laitteista tai tallenteista (noin 1 miljoonan tiedot kohteena) ja 9 muuta tapausta (noin 0,35 miljoonan tiedot kohteena). Nousua tapahtui kahdessa ensimmäisessä ryhmässä ja kokonaismäärä nousi hieman (vuonna 2017: 359). Yhteensä tietosuojaloukkauksia kohdistui noin 13,35 miljoonaan tietoon. (HIPAA, 2019)

Yhdysvaltain FDA (Food and Drug Administration) on analysoinut kyberturvallisuushaavoittuvuuksia ja tapauksia, jotka voivat vaikuttaa suoraan lääkintälaitteisiin tai sairaalan verkon toimintaan, mukaan lukien:

* 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, vahva salasana ohjelmistossa, johon tulisi olla pääsy erityishenkilöstöllä (esim. hallinto, tekninen, tai huoltohenkilökunta).

* Turvallisuusohjelmistopäivityksien ja -paikkauksien epäonnistunut jakelu lääkintälaitteille ja tietoverkoille, sekä vanhojen lääkintälaitemallien (legacy) haavoittuvuuksien hoitamattomuus.

Uhat sairaalan tietojärjestelmiin tulevat useista eri lähteistä kuten tahalliset kyberhyökkäykset, tahattomat häiriöt, jotka johtuvat mm. järjestelmän monimutkaisuudesta, inhimillisistä virheistä, tapaturmista tai laitevioista sekä luonnonkatastrofeista.

Kyberhyökkäysten takana olevilla yksilöillä, ryhmillä tai valtiollisilla toimijoilla on tunnistettavissa erilaisia motiiveja. Näillä ryhmillä on motiivien lisäksi käytössään erilaista osaamista ja resursseja, joita on lueteltu ohessa (Piggin, 2017, 5):

* Kybervandalistit (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 useita IT-pohjaisia järjestelmiä haltuunsa toteuttamaan laaja-alaisia hyökkäyksiä ja lähettämään BOT-verkon avulla tietojenkalasteluviestejä, haittaohjelmia ja roskaposteja. Palveluja voidaan käyttää myös

palvelunestohyökkäyksiin tai roskapostin ja tietojenkalastelun välittämiseen.

* Kyberrikolliset/rikollisryhmät/järjestäytynyt rikollisuus hyökkäävät järjestelmiin taloudellisen edun saamiseksi hyödyntäen roskaposteja, tietojenkalastelua, tai haittaohjelmia, joiden avulla he voivat kerätä tarvittavia tietoja (mm. henkilötietoja, luottokorttitietoja) toteuttaakseen tietoverkkopetoksia ja -huijauksia sekä kiristyksiä. Lisäksi voidaan uhata kyberhyökkäyksillä lunnaiden saamiseksi tai toteuttaa yrityksen liiketoiminnan tuhoamiseen tähtääviä operaatioita. Rikollisten hankkimia tietoja järjestelmiin tunkeutumisesta voidaan myydä kolmansille osapuolille.

* Valtiolliset turvallisuustoimijat käyttävät kybertyökaluja kybertiedusteluun, -vakoiluun ja hyökkäyksiin yhteiskunnan kriittistä infrastruktuuria vastaan (kybersabotaasi). Näillä valtiollisilla toimijoilla on hyökkäyskyvykkyyksiä, joita voidaan tarvittaessa käyttää kybersodankäyntiin. Nämä toimijat voivat hankkia sensitiivisiä tietoja terveydenhuoltojärjestelmistä tiedustelutarkoituksessa ja kybersabotaasihyökkäyksellä voivat jopa lamauttaa terveydenhuoltojärjestelmien toimintaa.

* Sisäpiiriläiset (työntekijät, tavarantoimittajat, ulkoistettu kiinteistönhuoltohenkilöstö jne.), joilla on rajoittamaton tai osin rajoitettu pääsy järjestelmiin, voivat joko haitantekotarkoituksessa tai tahattomasti tuoda haittaohjelmia tai tehdä ei-toivottuja muutoksia sairaalan tietojärjestelmiin.

* Tietojenkalastelijat tekevät tietojenkalastelua yksilöiltä, millä pyritään saamaan henkilötietoja ja muita tietoja, joiden avulla kyberrikoksia voidaan toteuttaa.

* Roskapostin lähettäjät lähettävät ei-toivottuja sähköposteja markkinointitarkoituksessa, jotka usein sisältävät piilotettuja haittaohjelmia tai linkkejä haitallisille sivustoille.

* Vakoiluohjelmien ja haittaohjelmien tekijät tuottavat eri tarkoituksiin tarkoitettuja haittaohjelmia ja usein myyvät niitä varsinaisille hyökkäysoperaatioiden tekijöille.

* Terroristit pyrkivät häiritsemään, lamauttamaan tai tuhoamaan yhteiskunnan kriittistä infrastruktuuria. Hyökkäysten tavoitteena on tuottaa vahinkoa ja levittää pelkoa ihmisten keskuuteen ja saada poliittiset toimijat suostumaan terroristien ehtoihin.

* Teollisuusvakoilijat pyrkivät saamaan haltuunsa yritysten immateriaalioikeuksia ja muita luottamuksellisia tietoja.

Eräänä merkittävimmistä sairaalajärjestelmien ja -laitteiden kyberturvallisuuden riskitekijöistä on pidettävä puutteellisesti testattuja laitepäivityksiä. Niistä aiheutuvia uhkia voivat hyödyntää niin sisäpiiriläiset kuin ulkopuoliset toimijatkin.

Piggin (2017, 5) luokittelee kyberhyökkäystoiminnan passiiviseksi ja aktiiviseksi. Passiivista on erilaisin vakoiluohjelmin tiedon kerääminen tietoverkoista ja -laitteista (hyvin toteutettuna yksilö tai organisaatio ei huomaa laitonta toimintaa). Aktiivinen toiminta ilmentyy mm. seuraavina kyberhyökkäysmuotoina:

* Tietokantainjektio: käytetään tietoihin tai järjestelmiin pääsemiseen ja tietojen varastamiseen.

* Väärentäminen tai jäljittely: laitteistolle tai ohjelmistolle tuleva kommunikaatio saadaan tulemaan muualta kuin alkuperäislähteestä.

* Sosiaalinen manipulointi: pyrkimys saada luottamuksellista tietoa henkilöiltä harhauttamalla.
* Tietojenkalastelu: sosiaalisen manipuloinnin muoto, jossa käytetään väärennettyjä sähköposteja tai verkkosivustoja houkuttelemaan uhri paljastamaan tietoja.
* Haittakoodi: kerätään tietoja, tuhotaan tietoja, muutetaan tietoja, luodaan takaportin tietojärjestelmään jne.
* Palvelunestohyökkäys (DDoS): vaikuttaa verkkojen ja tietojenkäsittelyresurssien saatavuuteen niitä huonontamalla.
* 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-haittaohjelma).

Kyberturvallisuuden perinteiset attribuutit (luotettavuus, saatavuus, eheys) lääketieteellisissä järjestelmissä eroavat toisistaan niiden käyttötarkoituksen suhteen. Tiedon luottamuksellisuuden varmistaminen on sairaalajärjestelmien ensisijainen tavoite, kun tavoitellaan tietomurtojen tai kiristyshaittaohjelmien aiheuttamien uhkilta suojautumista.

Tiedon saatavuuden varmistaminen on etusijalla, kun potilaat tarvitsevat lääkinnällisiä laitteita osana hoitoa, mukaan lukien implantoitavat laitteet. Ei-lääketieteellisillä laitteilla tai henkilöiden hyvinvointilaitteilla, kuten aktiivisuusrannekkeilla, on myös tiedon luottamuksellisuus etusijalla, vaikkakin niillä on pienempi vaikutus terveydenhuollossa kyberturvallisuuteen kuin edellä mainituissa tapauksissa. (Piggin, 2017, 12)

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 hyödyntävät puutteellisista suojaustoimenpiteistä ja päivitysten puutteista aiheutuvia mahdollisuuksia.

Hyökkääjä voi haittaohjelmiensa avulla tunkeutua 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 kovin 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 ja järjestelmien kustannusten rinnalla.

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

* Sähkömagneettinen häirintä.
* Testaamaton tai viallinen ohjelma ja laiteohjelmisto.
* Lääkinnällisten laitteiden varkaus tai häviäminen (ulkoiset tai kannettavat).

* Tietosuoja.

* Väärin määritellyt verkot tai huonot turvallisuuskäytännöt.

* Valmistajien tietoturvapäivitysten ja korjaustiedostojen asennuksien laiminlyönti lääkinnällisiin laitteisiin.

* Potilastietojen tai datan virheellinen hävittäminen, ml. testitulokset ja terveystiedot.

* Heikko salasanojen käyttökulttuuri (heikot salasanat, sama salasana useassa järjestelmässä, sama salasana usean eri henkilön käytössä, laitteiden tai järjestelmien oletussalasanoja ei vaihdeta, käytetään salasanoja, jotka on tarkoitettu rajoitettuun pääsyyn lääkinnällisiin laitteisiin (esim. hallinnointiin, tekniselle tuelle ja huoltopalvelulle).

* Potilastietojen manipulaatio, varkaus, tuhoaminen, valtuuttamaton julkistaminen tai potilaiden tietojen saatavuuden puute niitä tarvitseville.

* Luvaton laitteen asetusten muuttaminen, uudelleenohjelmointi tai tartunta haittaohjelmien avulla.

* Palvelunestohyökkäykset.

* Hyökkäykset mobiiliterveydenhuollon laitteisiin, jotka hyödyntävät potilastietoihin pääsyyn langattomia teknologioita, niiden valvontajärjestelmiin ja niihin integroituihin lääkinnällisiin laitteisiin.

3.2 Sairaalaympäristön tietojärjestelmien kyberrakennemalli

Sosiaali- ja terveydenhuollon organisaatiokohtaisia tietojärjestelmiä ovat sairaalan tietojärjestelmät, perusterveydenhuollon tietojärjestelmät, laboratorion, erillisyksikköjen tietojärjestelmät (esim. radiologia) sekä sosiaalitoimen tietojärjestelmät.

Näiden lisäksi sairaalaorganisaatiot käyttävät hallinnon tietojärjestelmiä (mm. talous- ja henkilöstöhallinto), asianhallinnan tietojärjestelmät (mm. tekstinkäsittely ja taulukkolaskenta), viestintäjärjestelmät (mm. sähköposti, hoitajakutsujärjestelmät), toiminnanohjausjärjestelmät, turvallisuusjärjestelmät (mm. 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). 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.

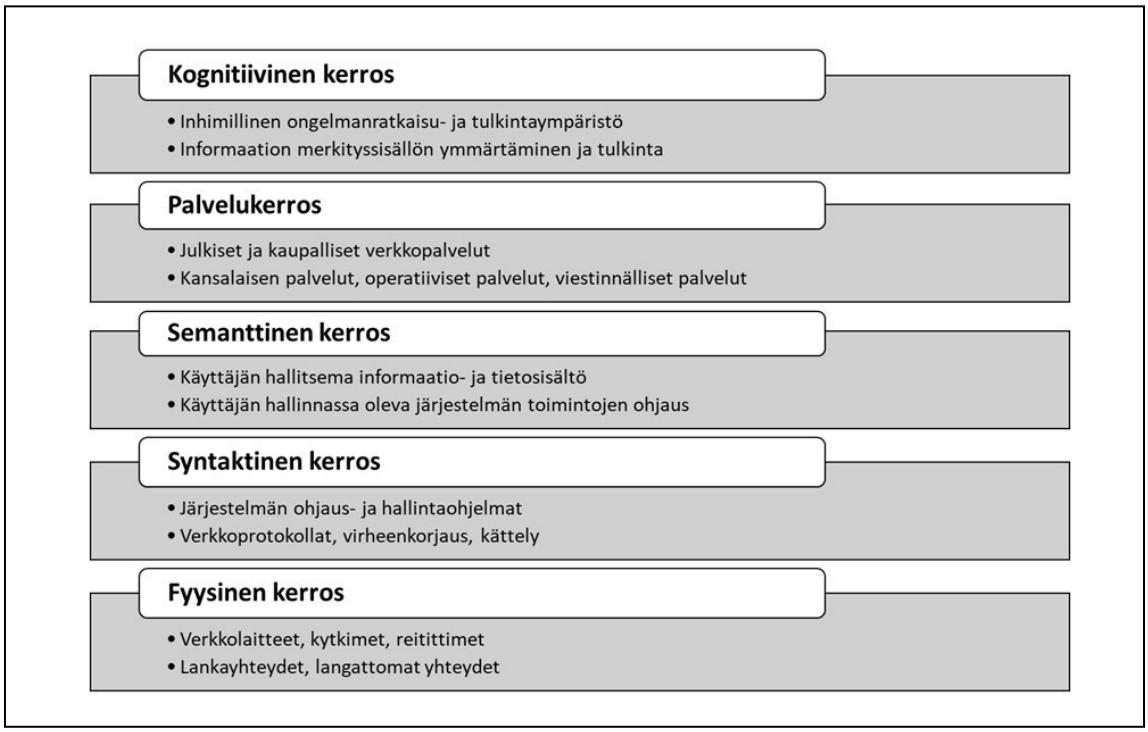
5. Kognitiivinen kerros kuvaa sairaalan päätöksentekijän ja toimijan informaation ongelmanratkaisu- ja tulkintaympäristöä, maailmaa, jossa informaatiota tulkitaan ja muodostetaan henkilökohtainen tilanneymmärrys.

Kuvassa 5 on esitetty kybertoimintaympäristön hierarkkinen rakennemalli.

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 Face-



KUVA 5: Kybertoimintaympäristön hierarkkinen rakennemalli (Lehto, 2015, 21).

book- 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.

LUKU 4

Kyberhyökkäyksiä sairaalajärjestelemiin

4.1 Kyberhyökkäykset ja -tekniikat

ENISA käyttää oheisen taulukon 2 kyberuhkamallia, joka muodostuu hyökkäysmenetelmistä ja -tekniikoista, haittaohjelmista ja fyysisen maailman uhkista: (ENISA, 2012, 13–15).

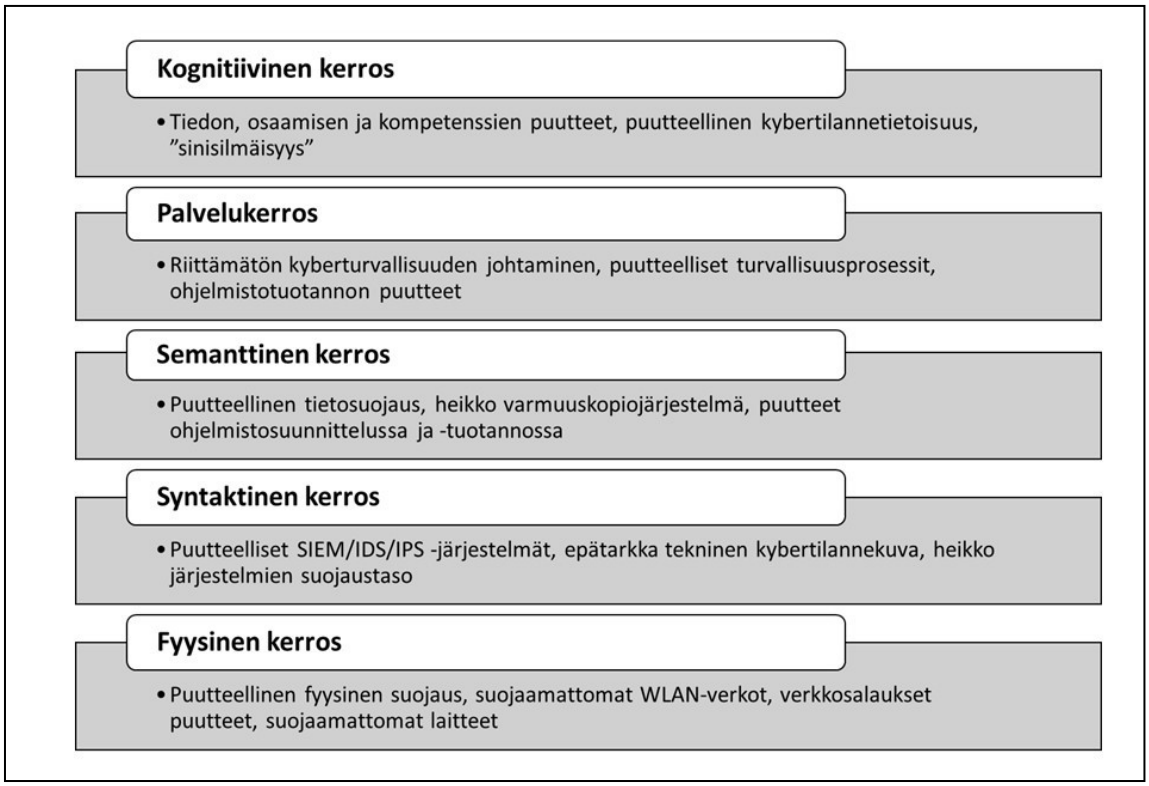
Richard Hundley ja Robert Anderson jakavat kybermaailman haavoittuvuudet seuraavasti (Hundley & Anderson, 1995, 237–238):

1. **Toimintoperustaisia:**
   * Toimintajärjestelmät.
   * Prosessit.
2. **Käyttäjäperustaisia:**
   * Autentikointi.
   * Salasanat.
3. **SW-perustaisia:**
   * Takaovi.
   * Ohjelmistovirheet.
   * Asennusvirheet.
4. **HW-perustaisia:**
   * Suunnitteluvirheet.
   * Komponenttivirheet.
5. **Verkkoperustaisia:**
   * 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 ha-

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

TAULUKKO 2: Yhteiseurooppalainen verkko- ja tietoturvasta vastaavan organisaation, ENISA:n luokittelemia kyberhyökkäysmenetelmiä ja -tekniikoita.



KUVA 6: Kybertoimintaympäristön haavoittuvuuksia, (Lehto, 2014, 168).

vaita ja jäljittää tunkeutumiset systeemin sisälle. Verkottuminen lisää tehokkuutta ja suorituskykyä, mutta samalla se lisää kyberturvallisuutta vaarantavia haavoittuvuuksia. Kuvassa 6 on esitetty tyypillisiä toimintaan liittyviä haavoittuvuuksia sijoitettuna aiemmin esitettyyn viisiportaiseen kyberrakennemalliin.

4.2 Terveydenhuollossa todettuja kyberuhkia

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:

* Potilaiden turvallisuuteen.
* IT-ohjelmistojen saatavuuteen, joka voi estää potilaiden hoidon.
* Potilaiden ja työntekijöiden tietojen yksityisyyteen ja turvallisuuteen.
* Sairaalan maineeseen.
* 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.)

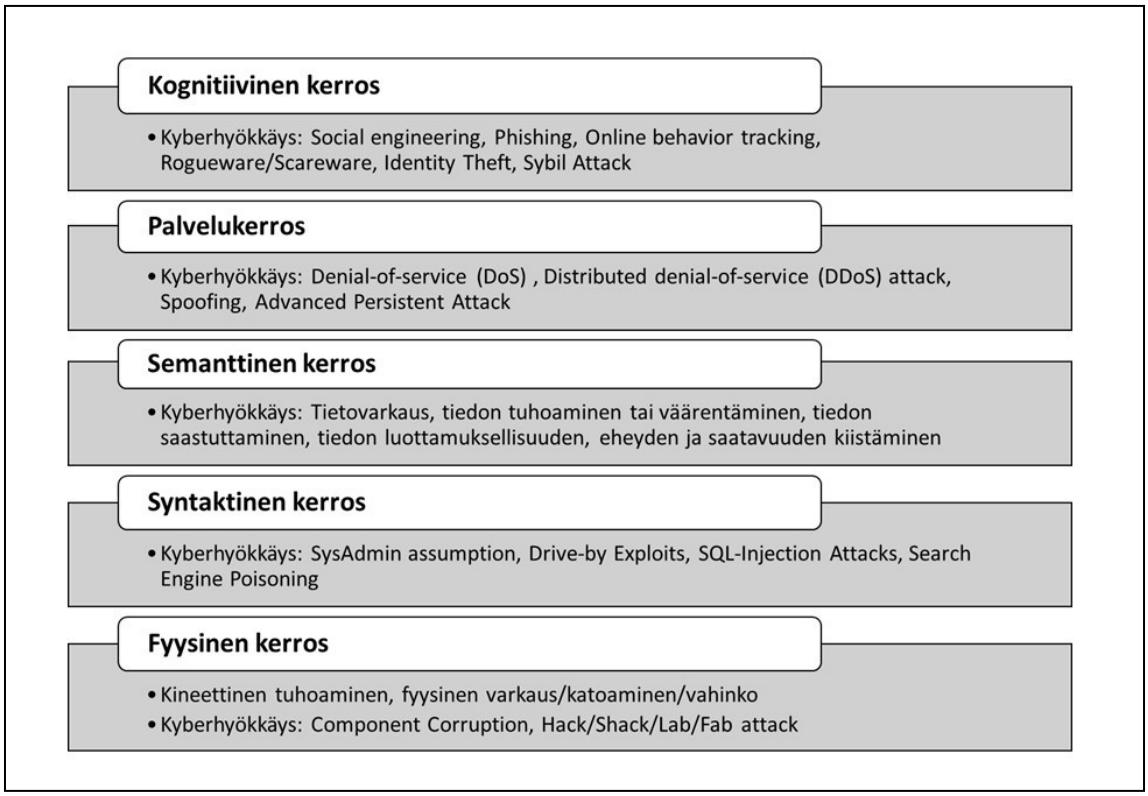
Haitan aiheuttaja toteuttaa kyberhyökkäyksiä kybermaailman eri rakenteisiin. Kyberrakenteen fyysiseen kerroksen voidaan kohdistaa sekä kineettistä että ei-kineettistä vaikutusta. Kineettisellä asevaikutuksella voidaan tuhota fyysisiä verkkoja, järjestelmiä ja niiden osia sekä tietovarastoja (Data Warehouse). 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, 177–182)

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



KUVA 7: Hyökkäysvektoreita kybertoimintaympäristön eri tasoille (Lehto, 2014, 167–168).

kaikkia järjestelmien käyttäjiä vastaan. Hyökkäyksillä pyritään estämään esimerkiksi toiminnan oikeanlaisen tilannetietoisuuden syntyminen. Kuvassa 7 on esitetty erilaisia hyökkäysmalleja ja -vektoreita kybermaailman eri kerroksia vastaan. (Lehto 2014, 157–178)

4.3 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:
    * Tietokoneen (vast.) varkaus, 9.
    * Virushyökkäys, 5.
    * DDos, 4.
    * Muu, 5.

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.

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.)

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.

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.)

4.4 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.

Hyökkäysvektoreita sairaalalaitteisiin

Sairaalalaitteiden turvallisuuskatsauksessa kerättiin 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. Haltuun ottamisen helppouteen vaikuttaa hyökkäysvektoreiden lisäksi laitteen tietojärjestelmän rakenne.

Jos käytössä on yleinen käyttöjärjestelmä, on hyökkääjän helpompi hyödyntää aikaisempaa kokemusta ja valmiita työkaluja. Tutkituista laitteissa oli Windows Philipsin Intellivue MX800-monitorissa tai Linux Drägerin Infinity Delta -monitorissa. Täytyy kuitenkin muistaa, että valmiissa käyttöjärjestelmässä tietoturvaa on todennäköisesti koeteltu ja parannettu enemmän kuin alusta alkaen laitteelle tehdyssä järjestelmässä.

Erityisen kiinnostuksen kohteena oli WLAN-yhteys. Langattomien laitteiden murtaminen tai niiden toiminnan häiritseminen langattomassa verkossa ei välttämättä vaadi samassa tilassa olemista ja hyökkääjä voi toimia verrattain salassa. Lisäksi WLAN-verkon kuuntelemiseen ja sen kautta hyökkäämiseen on valmiita työkaluja, jotka madaltavat kynnystä hyökkäämisen kokeiluun. Langattoman verkon avulla voidaan salakuunnella potilastieto-

ja, 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 laitetta voidaan hallita. Sammuttaminen, järjestelmän tekeminen toimintakyvyttömäksi ja järjestelmän hallittu käskyttäminen ovat mahdollisia hakkeroinnin tuloksia.

Toinen tärkeä hyökkäysvektori on USB-portti. Saastuneella muistitikulla voi halutun viruksen saada laitteeseen väliaikaisellakin yhdistämisellä. Lisäksi mainitaan SD-kortin käyttö. GE:n EKG-piirturi 3500 sisältää paikan SD-kortille. Ohjelmistopäivitykset asennetaan SD-kortin avulla. Uuden ohjelmiston asentaminen SD-korttia vaihtamalla ei varmasti ole helppo tehtävä, mutta maininnan arvoinen reitti laitteen tietojärjestelmiin. Mahdollisesti kortin varastava voi saada haltuunsa potilastietoja. Korttipaikka on laitteen näytön takana ja helposti saavutettavissa.

Monissa laitteissa ei ole WLAN-yhteyttä, mutta joissakin voidaan käyttää erilaisia adaptereita tämän ominaisuuden saamiseksi. Vain kolmen laitteen WLAN-salauksesta löytyi tietoa. Surullisin on Drägerin *Infinity Delta*, jonka kaikki versiot tukevat salaamatonta liikennettä ja WEP-salausta. WEP-salaus on kuitenkin murrettavissa. Jotta Infinity Delta käyttäisi WPA2-salausta, tulee laitteessa olla asennettuna ohjelma nimeltä VR8. EKG-piirturi Cardiovit AT-102+ on Schillerin valmistama. Langaton verkkoyhteys on valinnainen ominaisuus tässä laitteessa. Laite tukee WPA-, WPA2- ja WEP-salauksia. GE:n EKG-piirturi merkkiä 3500 voidaan yhdistää langattomaan verkkoon Silex-merkkisellä adapterilla. Tällä adapterilla voidaan salaus ja autentikointi hoitaa erittäin kattavasti, joten siitä ei turvallisuus jää kiinni.

Ultraäänilaitteita oli kaksi: GE Healthcare:n LOGIQ P9 ja Philipsin EPIQ 5c, joka on erityisesti sydämen kuvaamisen tarkoitettu. Molemmissa laitteissa on WLAN-valmius, mutta kummankaan salauksista tai niiden puutteesta ei löytynyt tietoa. Philipsin EPIQ 5c sisältää palomuurin ja McAfeen virustentorjuntaohjelman, lisäksi potilasdatan salaus on mahdollista. Lisäksi laitteeseen voidaan muodostaa etäyhteys valmistajan tukipalveluista. Tämä on kätevä ominaisuus, mutta toteutuksen tulisi olla turvallinen. Etäyhteys, jonka ulkopuolinen voi helposti muodostaa on todella houkutteleva ominaisuus hyökkääjälle. EPIQ 5c:ssä on lisäksi USB-portti, jonka kautta voidaan syöttää haitallista dataa laitteeseen. EPIQ 5 jouduttiin vetämään takaisin markkinoilta vuonna 2014 epätarkkojen mittaustulosten vuoksi. Epätarkkuudet korjattiin ohjelmistomuutoksella.

Liikuteltavia röntgenlaitteista Ziehman RFD ja Fuji FDR Go voidaan yhdistää adapterilla langattomaan verkkoon. Näiden salauksista ei ole tietoa. Pulserasta ei löydy mainintaa LAN tai WLAN yhteyksistä, mutta esitteissä mainostetaan etäyhteysmahdollisuutta Philipsin tukeen. Jonkinlainen yhteys Internetiin täytyy siis olla, mutta sitä ei vain olla mainittu.

Philipsin valmistamassa potilasmonitorissa Intellivie MX800 on Ethernet-portti ja viisi USB porttia. WLAN-yhteys on saatavissa valinnoilla J20 tai J35. Oletettavasti nämä ovat lisävarustekoodeja, mutta tarkempaa tietoa ei löytynyt. Käyttöjärjestelmä on Windows 7 tai XP. Linux-pohjainen GE:n potilasmonitori Carescape B850 tyytyy LAN-yhteyteen kahden RJ45-portin kautta. Lisäksi laitteesta löytyy neljä USB-porttia ja kaksi sarjaporttia (DB9M). Drägerin Infinity Deltan WLANin suojaamattomuus ilman oikeita ohjelmistoja

mainittiinkin aiemmin. WEP on parasta, mihin laite pystyy ilman VR8-ohjelmistoa. LAN-verkkoon laite on yhteydessä telakka-aseman tai DirectNet-järjestelmän kautta. Laite pystyy muodostamaan yhteyden erittäin moneen muuhun laitteeseen erilaisten liittimiensä ansiosta. Monet näistä yhdistettävistä laitteista ovat Drägerin valmistamia.

Telemetrialähetin TelesSmart M300 on Drägerin valmistama ja se ottaa langattoman yhteyden Infinity-keskusyksikköön. Tämän laitteen kohdalla verkkohyökkäysten mahdollisiin tuloksiin on pieni lisä: äänisaaste. Keskusyksiköstä voidaan lähettää TeleSmart:ille käsky pitää ääntä, jotta se voidaan löytää. Riippuen kuinka tämä toiminto on toteutettu, voi joku lähettää jatkuvasti paikallistamisäänen pyyntöä laitteelle ja häiritä ja hämmentää käyttäjiä.

Radiometerin verikaasuanalysaattori ABL90 FLEX ei yhdisty langattomaan verkkoon, mutta LAN verkkoon kylläkin. Lisäksi siinä on kolme USB-porttia ja sarjaportteja. Epäselväksi jäi, onko laitteessa levynlukija. Käyttöohjeissa kerrotaan, kuinka tiedot voi varmuuskopioida CD-levylle tai USB-massamuistilaitteelle, mutta muuta mainintaa levynlukijasta ei ole. Hiirelle ja näppäimistölle löytyvät vanhanaikaiset pyöreät liittimet, jos vanha näppäimistö vaikka kaipaa uutta sijoituspaikkaa USB-liitettävien vallattua markkinat.

GE 3500 yhdistetään WLAN:iin Silex-adapterilla, joka tukee seuraavia salausmenetelmiä: WPA2, WPA, WPA2-WPA, WEP ja seuraavia langattomia autentikointimenetelmiä: WPA-PSK, Open System, Shared Key, TTLS, TLS, LEAP, PEAP, EAP-FAST. Schillerin Cardiovit AT-102+:sta löytyy seuraavat menetelmät: WPA, WPA2 sekä WEP. Mortaran Eli 250c:n salauksista ei löytynyt mainintoja. LAN-yhteys voidaan saada kaikkiin mutta USB-portit uupuvat GE 3500:sta. Siinä on kuitenkin SD-korttipaikka ohjelmistopäivitysten asentamista ja datan tallennusta varten. Sekä GE 3500:an että Mortatan Eli 250c:hen voi halutessaan saada puhelinjohtopaikan. Cardiovit AT-102+ puolestaan voi olla yhteydessä mobiiliverkkoon valinnaisen GPRS-lisäosan avulla.

Ruiskupumpputelakka Injectomat MC Agilia ei sisällä valmiuksia kommunikointiin minkään muun kuin Link+-yksikön kautta. Laitteita voidaan laittaa useita yhteen yksikköön ja se kommunikoi infrapunan avulla ruiskupumpputelakoiden kanssa. Link+ on puolestaan yhteydessä 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 painiketta painamalla ei ole kovin pitkäikäisen häirinnän keino, mutta mahdollinen.

Kuvalevyjen lukulaitteet Agfan CR 85-X, Fujin Capsula XL ja Soredexin Digora Optime eivät voi liittyä langattomaan verkkoon, mutta Agfan CR 85-X ja Soredexin Digora Optime sisältävät Ethernet-portin. Capsula välittää kuvansa CR-konsolille, josta kuvia voi tarkastella ja mahdollisesti lähettää eteenpäin DICOM-muotoisena. Soredexin Digora Optimen käyttöohje kehottaa käyttämään palomuuria ja virustentorjuntaohjelmaa.

Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat yleistyneet viime vuoksien aikana ja herättäneet huomiota erityisesti mediassa niiden laajan levinneisyyden vuoksi. Isot organisaatiot mukaan lukien sairaalat eivät ole säästyneet näiltä haittaohjelmilta ja erityistä huomioita sai toukokuussa 2017 laajalti levinnyt WannaCry kiristyshaitta-

ohjelma, joka levisi 48:aan National Health Service organisaatioon Isossa Britanniassa (ks. liite 1).

Kirityshaittaohjelmat leviävät usein muiden haittaohjelmien tavoin sähköpostien liitetiedostoina, joka vaatii, että käyttäjä saadaan avaamaan tiedosto. Toinen tartunta tapa on roskapostit, joissa on linkkejä nettisivuille, joille mennessä latautuu haittaohjelma tietokoneelle. Nämä kaksi tartuntatapaa vaativat, että käyttäjä saadaan avaamaan liitetiedosto tai linkki tekemällä viestistä mielenkiintoinen tai sellainen, joka vaatii toimintaa kuten maksamattomaksi jäänyt lasku.

Esimerkki

Keväällä 2016 kiristyshaittaohjelma saastutti monia sairaaloita ympäri Yhdysvaltoja, hyödyntäen vanhentunutta JBoss palvelinohjelmistoa. Näissä tapauksissa hyökkääjä latasi haittaohjelman palvelimille ilman minkäänlaista yhteyttä kohteen kanssa, vaan sen sijaan ensin pyrki saastuttamaan tavallisen työaseman.

Kalifornialaisen Hollywood Presbyterian sairaalan tapauksessa potilaiden hoito hidastui ja johti siihen, että sairaala maksoi $17 000 saadakseen pääsyn tiedostoihinsa ja verkkoonsa. Tekijät käyttivät avointa lähdekoodia hyödyntävää työkalua JexBoss, jolla he etsivät haavoittuvia JBoss palvelimia ja tartunnan saaneita verkkoja, välittämättä minkä toimialan ne olivat.

Vaikka ei ole tarkkoja todisteita, on spekuloitu, että tekijät olivat tietoisia tartunnan saaneista terveydenhuollon organisaatioista, josta syystä lunnasvaatimukset olivat niin korkeat. He olivat mahdollisesti tietoisia, että tartunnan saaneet laitteet olivat keskeisiä sairaalan toiminnalla ja että kiristyshaittaohjelma estäisi niiden käytön ja tämä toisi paineen ratkaista ongelma nopeasti, jotta potilaiden hoito voisi jatkua. Tämä paine ja se että, usein sairaaloilla on rahaa maksaa, mahdollisesti nosti maksamistodennäköisyyttä.

Terveydenhuolto oli kohteena 88 % kaikista kiristyshaittaohjelma tapauksista Yhdysvalloissa viime vuonna, Solutionary turvallisuusyhtiön mukaan. Ponemon Instituutin julkaiseman rapotin mukaan 89 % tutkituista terveydenhuollon organisaatioista olivat kokeneet tietomurron viimeisen kahden vuoden aikana, jossa potilastietoja menetettiin tai varastettiin.

Kun käyttäjän koneessa on kiristyshaittaohjelma niin tämä salaa koneelle olevat tiedostot niin että niitä ei voi käyttää ilman että salaus puretaan käyttämällä salausavainta. Kun tiedot ovat salattu ohjelma näyttää käyttäjälle lunnasvaatimukset, joiden tarkoituksena on saada käyttäjä maksamaan summa rahaa usein Bitcoineissa, ja maksusta luvataan, että käyttäjä saa salausavaimen tiedostojen purkamista varten.

Mikäli kiristyshaittaohjelma on kirjoitettu hyvin ei tiedostoja ole mahdollista saada takaisin ilman salausavainta, joten paras suojaus tätä vastaan on, että käyttäjällä on ajantasaiset päivitykset, joita voidaan käyttää tietokoneen palauttamiseen. Lunnaiden maksaminen ei takaa, että käyttäjä saa salausavaimen ja käyttäjiä neuvotaan olemaan maksamatta lunnaita, koska tämä tukee rikollistoimintaa ja uusien haittaohjelmien kehittämistä.

WannaCry kiristyshaittaohjelma oli poikkeuksellinen, sillä se levisi tietokoneiden välillä käyttäen haavoittuvuutta Windows käyttöjärjestelmässä. Microsoft oli korjannut haavoittuvuuden maaliskuussa 2017, mutta useat organisaatiot eivät pidä päivityksiään ajan tasalla

tai käyttävät vanhempia ei tuettuja versioita. Tämä leviämistapa mahdollisti haittaohjelman nopean ja laajan leviämisen hyvin lyhyessä ajassa.

Kiristyshaittaohjelmien tarkoitus on saada käyttäjät maksamaan usein vain muutamia satoja euroa, koska tarkoitus on tehdä kynnys alhaiseksi ja rikolliset luottavat siihen, että he saavat lunnaita suurelta määrältä käyttäjiä. Näiden hyökkäyksien tarkoituksena ei ole anastaa tietoa vaan rajoittaa käyttäjän pääsy tietoihin, joka usein on tärkeää liiketoiminalle tai kuten sairaaloiden tilanteessa potilaiden hoitamiselle. Erityisesti sairaalat ovat huolissaan, mikäli tällaisissa tilanteissa heidän potilastietojensa eheys säilyy, senkin jälkeen, kun tiedot on joko purettu tai palautettu varmuuskopioista.

Sairaalat ovat olleet kiristyshaittaohjelmien kohteena ainakin kahdesta eri syystä. Ensimmäinen syy on, että sairaaloilla on usein suuri määrä tietojärjestelmiä ja käytössä myös vanhoja käyttöjärjestelmiä, ja kaikkia laitteita, joita on kliinisessä käytössä ei ole mahdollista päivittää usein koska ne ovat käytössä jatkuvasti. Toinen syy on, että sairaaloiden toiminta vaatii sitä, että tietojärjestelmät ovat saatavissa kuten potilastietojärjestelmä ja ilman näitä tietoja sairaaloiden toiminta hidastuu merkittävästi.

Kun tarkastelee viime viiden vuoden aikana tapahtuneita kiristyshaittaohjelma tapauksia, jotka ovat kohdistuneet sairaaloihin ja muihin terveydenhuollon palveluihin on niiden vaikutus ollut mittava. Tartunnat ovat saaneet aikaan sen, että esimerkiksi potilastietojärjestelmä, ajanvaraus, ja röntgenlaiteet eivät ole olleet käytettävissä. Joissakin tapauksissa myös potilastietoja on varastettu (ks. liite 1). Vain muutamat sairaalat ovat kertoneet julkisuudessa, että he ovat maksaneet lunnaita ja monilla sairaaloilla on ollut varmuuskopiot, joita on voitu käyttää palautumiseen.

Hakkerointi ja tietomurrot

Hakkerointi on yleisin hyökkäys organisaatioita kohden mukaan lukien sairaaloita. Viimeisen viiden vuoden aika on ollut useita tapauksia, joissa suuria määriä potilastietoja on varastettu (ks. liite 1). Hakkeroinnissa hyödynnetään järjestelmissä ja ohjelmistoissa olevia haavoittavuuksia ja mitä suurempi organisaatio on niin sitä enemmän mahdollisia kohteita ja haavoittuvuuksia on. Hakkeroinnin osana hyödynnetään myös muita hyökkäystapoja kuten sosiaalista manipulointia, jota kautta voidaan saada tietoa tai tunnuksia, joita tarvitaan järjestelmään pääsyyn.

Terveydenhuollon sektorilla näkyneiden tietomurtojen taustalle on erilaisia tapauksia, kuten käyttäjätunnuksien varastaminen haittaohjelmalla, sisäpiiriläinen joka tarkoituksella tai vahingossa paljastaa potilastietoja, tai hävinneet tai varastetut tietokoneet ja muut laitteet.

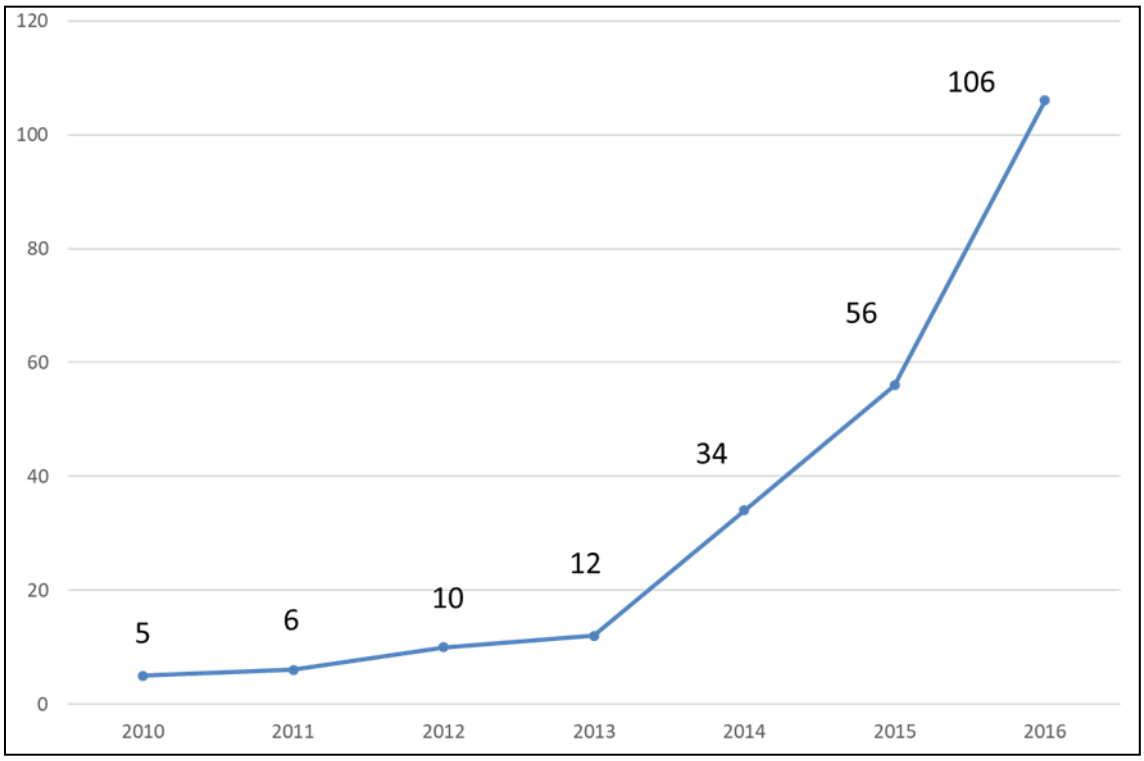
Kyberhyökkäykset ovat olleet vakaasti nousussa kuluneina vuosina, Health & Human Services (HHS) on raportoinut 106 hakkerointi tapausta vuonna 2016, joka on melkein kaksinkertainen edelliseen vuoteen verrattuna ja yli 20-kertainen määrä hyökkäyksiä, kun niitä verrataan vuoteen 2010 (ks. kuva 8 seuraavalla sivulla). Hakkerit haluavat henkilökohtaisia tietoja kuten osoitteita, henkilötunnuksia ja luottokorttinumeroita. He myös haluavat terveystietoja, jotka ovat hyvin arvokkaita, koska ne mahdollistavat identiteettivarkaiden luoda vakuuttavia profiileita varastetuilla tiedoilla. (Rubenfire Adam, 2017)

Sairaalat ja terveydenhuollon organisaatiot ovat joutuneet hakkeroinnin kohteeksi ainakin

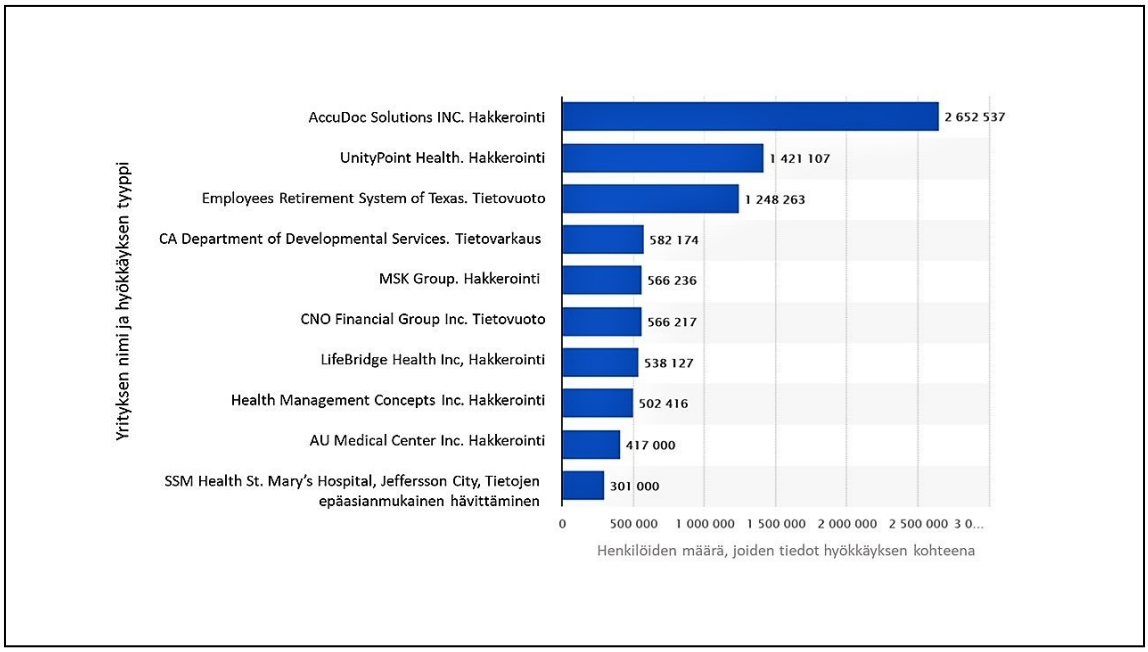
kahdesta eri syystä. Ensimmäinen syy on, että näissä organisaatioissa on useita järjestelmiä ja laitteita, sekä paljon ihmisiä, joten hyökkäystapoja on monia. Toinen syy on, että näillä organisaatioilla on potilastietoa, jota rikolliset voivat myydä eteenpäin. Tietoja voidaan käyttää esimerkiksi kiristyksessä tai identiteettivarkauksissa. Mikä tekee potilaistiedoista arvokasta, on se, että niissä usein on paljon yksityiskohtaisia tietoja yksilöstä, joita voi käyttää identiteettivarkauteen ja nämä tiedot yksilöstä ovat pysyä eikä niitä voi muuttaa. Finanssialan organisaatiot ovat pitkään olleet hakkeroinnin kohteena, mutta esimerkiksi varastettu luottokorttinumero voidaan helposti korvata uudella, mutta henkilötunnus ja lääkitys potilaistiedoista on pysyvämpää.

Potilastiedoissa on suuri määrä henkilökohtaista tietoa, joka kiinnostaa rikollisia ja voi olla hakkeroinnin kohteena. Tietoja, joita on varastettu terveydenhuollon järjestelmistä: nimi, osoite, syntymäaika, henkilötunnus, pankkitilinumero, luottokorttinumero, lääkitys, hoidot/leikkaukset, vakuutustiedot, ja paljon muuta henkilökohtaista tietoa (ks. liite 1). Kuten edellä mainituista tiedoista käy esiin on potilas- ja muissa sairaalajärjestelmissä valtava määrä tietoa yksilöistä. Tiedot mahdollistavat monenlaisen haitanteon yksilölle ja rikollisilla on mahdollisuus myydä tiedot suoraan tai käyttää tietoja osana esimerkiksi yksilöön kohdistettua hyökkäystä.

Organisaatiot eivät usein julkisesti kerro miten ovat joutuneet hakkeroinnin kohteeksi tai mitä kautta heidän organisaatioonsa on päästy sisään. Useat organisaatiot palkkaavat ulkopuolisia tietoturvayrityksiä hakkeroinnin selvittämiksi, jotta voivat reagoida paremmin tulevaisuudessa tai täyttää jonkin lain asettamat säädökset. Henkilökohtaisten tietojen menettäminen voi aiheuttaa organisaatiolle suuria sakkoja (ks. liite 1), ja näiden määrä tulee



KUVA 8: Terveydenhuollon hakkeroinnit Yhdysvalloissa 2010–2016.



KUVA 9: Kymmenen suurinta potilastietoihin kohdistunutta tietomurtoa Yhdysvalloissa 2018.

kasvamaan myös Euroopassa, kun Euroopan Unionin uusi tietosuoja-asetus tuli voimaan toukokuussa 2018.

Kuva 9 esittää kymmenen suurinta potilaiden terveystietoihin kohdistunutta tietomurtoa Yhdysvalloissa vuonna 2018. (Statiska, 2019)

Ponemon Instituutin mukaan tietomurrot maksavat vuosittain Yhdysvaltojen terveydenhuollolle noin $6.2 miljardia. Nämä hyökkäykset tulevat kalliiksi terveydenhuollolle, koska se on yksi säännellyimmistä toimialoista ja tästä johtuen tietomurrosta aiheutuneet kulut ovat henkilöä kohden korkeammat kuin keskiarvo ($221), Ponemon Instituutin raportin mukaan. Varastettu sähköinen potilastieto (Electronic Health Record, EHR) maksoi keskiverto yritykselle $355 vuonna 2016.

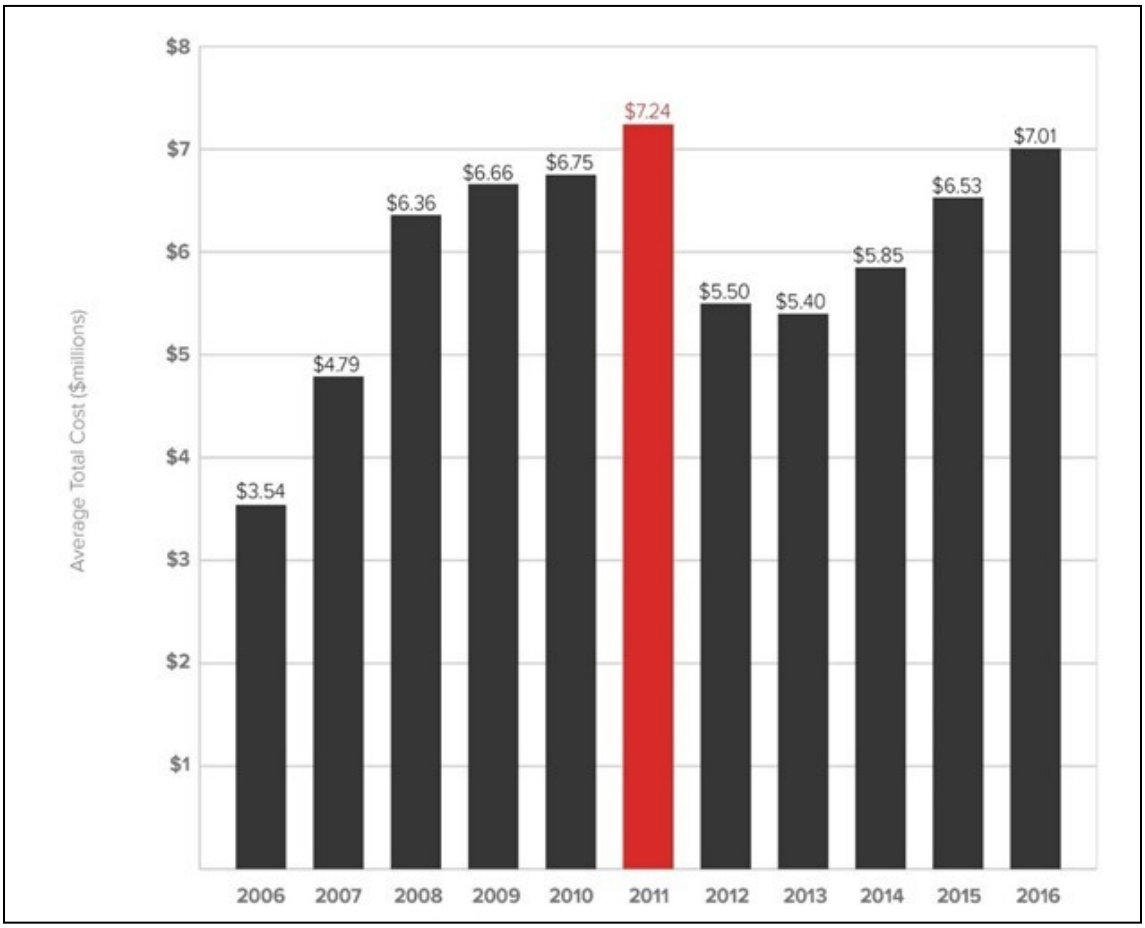
Kuva 10 seuraavalla sivulla näyttää organisaatioiden tietomurroista aiheutuneet keskimääräiset kustannukset 2006–2016.

Palveluestohyökkäykset

Sairaalat eivät ole myöskään säästyneet hajautetuilta palvelunestohyökkäyksiltä (DDoS). Näiden tarkoituksena on lähettää paljon turhaa verkkoliikennettä johonkin palveluun tai nettisivulle, mikä aiheuttaa sen, että palvelut lakkaavat toimimista tai hidastuvat, etteivät oikeat käyttäjät pääse niihin. Tällaiset hyökkäykset kestävät yleensä joitakin tunteja, mutta mikäli hyökkääjillä on käytössään merkittäviä resursseja ne voivat olla pidempiäkin tai jatkua uudestaan seuraavana päivänä.

Monet organisaatiot ovat joutuneet näiden kohteeksi koska niiden toteuttaminen on kohtuullisen helppoa. Hyökkääjien on usein tarkoituksena aiheuttaa haittaa tai näyttää omaa osaamistaan, tai mahdollisesti vaatia lunnaita hyökkäyksen lopettamiseksi. Palvelunesto-hyökkäyksiä käytetään myös osana laajempaa hyökkäystä, jolloin rikolliset toivovat, että heidän todelliset tarkoituksensa eivät paljastu, kun organisaation keskittyy ratkaisemaan DDoS-hyökkäyksen.

DDoS hyökkäyksissä potilastiedot eivät usein ole vaarassa, mutta potilaiden turvallisuus voi kärsiä siitä, kun he eivät voi päästä tietoihinsa tai sairaalan henkilökunta ei pysty toimitta-



KUVA 10: Organisaatioiden keskimääräiset tietomurtojen aiheuttamat kustannukset 2006–2016, miljoonaa dollaria/v. (Protenus , 2017).

maan suunniteltuja toimia koska heillä ei ole pääsy esimerkiksi lääkitystietoihin. Viime vuosian aikana mediassa on ollut vain muutamia tapauksia, joissa sairaalat tai muut organisaatiot, jotka ovat mukana terveydenhuollon palveluketjua ovat joutuneet DDoS-hyökkäyksen kohteeksi (ks. liite 1).

Esimerkki

Anonymous ryhmä kohdisti DDoS hyökkäyksen Bostonin Lastensairaalan vuonna 2014, sen jälkeen, kun sairaala oli ottanut 14-vuotiaan tytön osavaltion holhoukseen ja huoltajuus otettiin pois vanhemmilta. Lääkärit arvioivat, että lapsella oli psykologinen häiriö ja että hänen vanhempansa painostivat häntä tarpeettomiin hoitoihin sairauteen, jota hänelle ei ollut. Huoltajuusväittely asetti sairaalaan kiistanalaisen keskustelun keskiöön ja jotkut, ml. Anonymous, olivat sitä mieltä, että tytön oikeuksia loukattiin. Anonymous päätti aloittaa DDoS hyökkäyksen sairaalan tietoverkkoa vastaan, joka aiheutti sen, että heidän verkkonsa sekä Harvardin yliopiston ja kaikkien sen sairaaloiden verkot menettivät pääsyn internettiin. Verkoissa oli katkoksia melkein viikon ajan ja jotkut potilaat ja työntekijät eivät päässeet tänä aikana heidän online-tileilleen tarkastamaan ajanvarauksia, testituloksia, ja muita tapauskohtaisia tietoja. Tämän seurauksena sairaala käytti yli $300 000 korjatakseen hyökkäyksen aiheutumia vaurioita.

Sisäiset uhat

Organisaatiot ovat usein liian syventyneitä yhtiönsä ja verkon yhtenäisyyden puolustamiseen ulkoisilta uhkilta jättämällä ottamatta huomioon hyvin todellisen ja vaarallisen riskin, joka saattaa sijaita niiden oman organisaation sisällä - sisäpiirin jäsenet. Sisäpiirin jäsen aiheuttaa uhkan, koska hänellä on tai on ollut laillinen pääsy turvaluokiteltuihin tai yksinoikeudellisiin järjestelmiin. Usein organisaatiot väheksyvät perinteisten kyberturvallisuuspuolustuksen toimia kuten tunkeutumisen havaitseminen tai fyysinen turvallisuus. Sisäpiiriläisillä saattaa olla tietoa verkkorakenteista ja haavoittuvuuksista, tai kyky saada tarvittavaa tietoa kyberhyökkäystä varten paremmin kuin kukaan ulkopuolinen. Vaikka sisäpiirin jäsen saattaa olla yksinkertaisesti huolimaton, muut saattavat tällaisen huolimattomuuden vuoksi aiheuttaa vahinkoa pelkkää pahanilkisyyttään. Sisäinen uhka käsittää erilaisia työntekijöitä: niistä, jotka tietämättään klikkaavat vahingollista linkkiä, siten vaarantaen tietoverkon, tai hukaten arkaluonteista tietoa sisältävän työtietokoneen. Niitä, jotka pahansuopuuttaan luovuttavat käyttöoikeuskoodit, tai tahallaan myyvät henkilötietoja tavoitellen henkilökohtaista etua.

Oheisissa taulukoissa 3 ja 4 on kuvattu, kuinka moni on valmis myymään salasanansa kolmannelle osapuolelle tai kuinka moni on valmis myymään salasanansa alle $1000. (Chew Jonathan, 2016)

Sairaalanjärjestelmiin ja potilastietoihin on myös kohdistunut muita tietoturvahyökkäyksiä. Perinteisiä tietokoneviruksia on ollut tietojärjestelmissä, jotka ovat vaarantaneet potilastietoja ja myös tartuttaneet muita lääkintälaitteita (ks. liite 1). Myöskin kaikenlainen huolimattomuus on vaarantanut potilastiedot useassa eri tapauksessa ja osallisena näihin on myös yhteistyö organisaatiot ja heidän huolimattomuutensa.

Potilastiedot ovat myös vaarassa, kun niitä on taltioitu esimerkiksi kannettaville tietokoneille, joita viedään sairaalan ulkopuolelle. Kannettavia tietokoneita on varastettu lääkäriasemilta, autoista, ja terveydenhuollon ammattilaisten kotoa (ks. liite 1). Mikä tekee näistä tilanteista ongelmallisen, on se, että usein tietokoneissa on salasana, mutta itse kovalevyä

Kuinka moni on valmis myymään salasanansa kolmannelle osapuolelle	**%**
Yhdysvallat	27
Iso-Britannia	16
Saksa	20
Ranska	16
Alankomaat	12
Australia	12
Globaali keskiarvo	20

TAULUKKO 3: Salasanan myyminen kolmannelle osapuolelle.

Kuinka moni on valmis myymään salasanansa alle $1000	%
Yhdysvallat	40
Iso-Britannia	56
Saksa	45
Ranska	50
Alankomaat	33
Australia	42
Globaali keskiarvo	44

TAULUKKO 4: Salasanan myyminen alle $1000.

tai sen tietoja ei ole salattu, joten rikollinen voi päästä käsiksi kaikkiin tietoihin, jos saa esimerkiksi ohitettua salasana kyselyn.

Esimerkki

Erään texasilaisen sairaalan työntekijä rakensi botnetin hyväksikäyttäen sairaalaverkkoa hyökätäkseen kilpailevaa hakkeriryhmää vastaan. Henkilö saatiin kiinni sen jälkeen kun, hän oli videoinut sairaalaverkkoon tunkeutumistaan ja laittanut videon YouTubeen julkisesti nähtäväksi. Videosta näkyy selkeästi, kuinka yksilö käyttää tiettyä avainta tunkeutuakseen sairaalaan, mikä paljasti hänet yövartijaksi. Tutkimukset paljastivat, että hän oli ladannut haittaohjelmia kymmeniin koneisiin, mukaan lukien sairaanhoitajien koneeseen, jossa oli potilastietoja. Hän myös asensi takaportin HVAC laitteisiin, jotka rikkoutuessaan olisivat aiheuttanut vauriota lääkkeisiin ja sitä kautta vaikuttanut myös potilaisiin. Yövartija myönsi syyllisyytensä tietokoneiden peukalointiin ja on nyt vankilassa yhdeksän vuoden tuomiolla ja joutui maksamaan $31 000 sakot.

Tietokoneiden kovalevyille mahtuu helposti jopa miljoonien potilaiden tietoja, joten yksittäisen laitteen häviäminen voi vaarantaa monia. Monissa tapauksissa tulee myös ilmi se, ettei käyttäjillä ole tarkkaa tietoa millaista tietoa heillä on koneella tallennettuna, ja ketä kaikkia henkilöitä tapaus vaikuttaa, jos rikolliset saavat tiedot haltuunsa.

Havaitsemisaika ja toimintojen palauttaminen

Sairaaloihin ja terveydenhuollon organisaatioihin kohdistuneita hyökkäyksiä ei useasti tunnisteta nopeasti ja monissa tilanteissa tilanne selviää, kun esimerkiksi potilastietoja löytyy netistä myynnistä. Organisaatiot eivät usein puhu yksityiskohdista mediassa, mutta kun tutustuu saatavilla oleviin tietoihin, on huolestuttavaa, kuinka kauan voi kestää tietoturvamurron löytyminen tai hyökkäyksistä palautuminen (ks. liite 1).

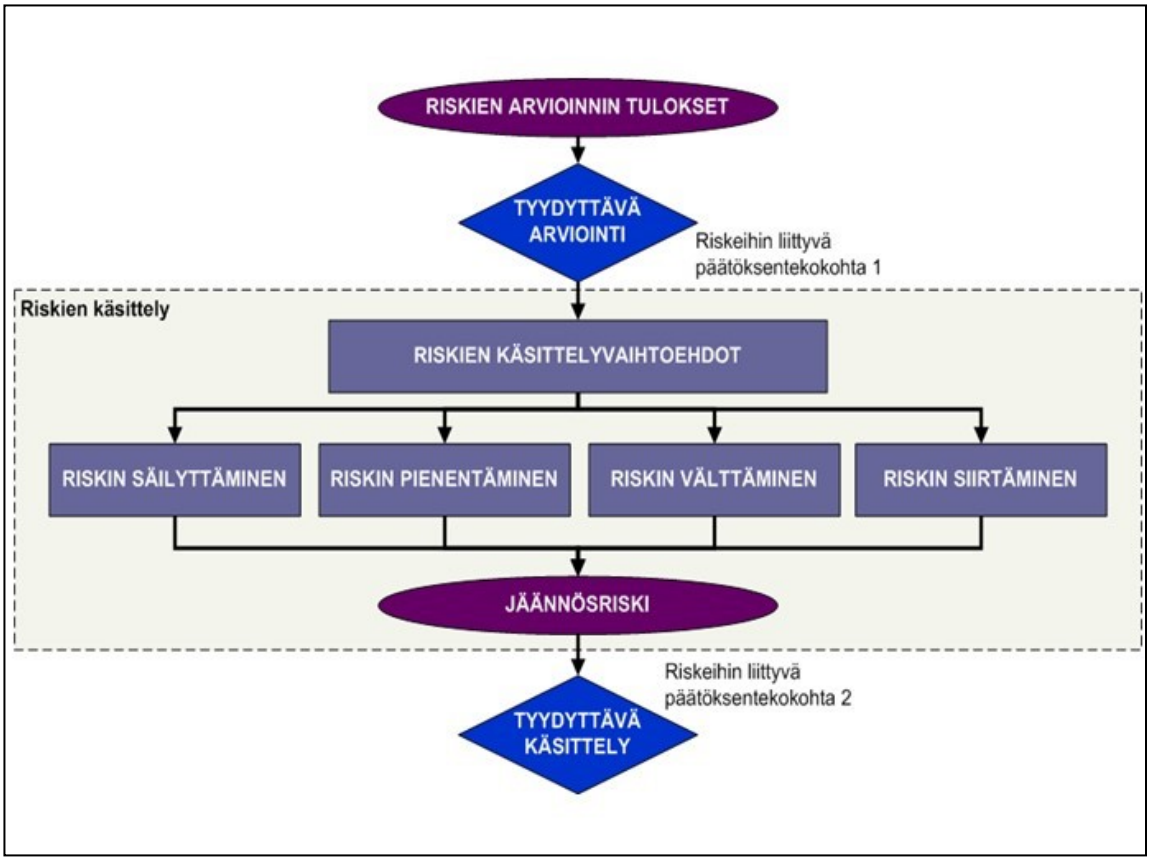
Positiivinen puoli kiristyshaittaohjelmissa on, että ne ilmoittavat heti salaamisen jälkeen, että ovat tartuttaneet tietokoneen. Kun tarkastelee tapauksia, joita sairaaloilla on ollut niin palautuminen kiristyshaittaohjelma hyökkäyksistä vie usein päiviä tai jopa yli viikon, jopa niissä organisaatioissa, joilla on varmuuskopiot. Aikaa menee koska kaikki tartunnan saaneet koneet pitää tunnistaa ja palauttaa toimivaan tilaan ja isoissa järjestelmissä on paljon tietoa, joten palauttamisprosessi vie pitkän aikaa. Sairaaloiden toiminta voi siis hidastua tai lakkautua moneksi päiväksi, vaikka varmuuskopiointi olisi kunnossa.

Kun tarkastelee hakkerointitapauksia, tilanne on hyvin erilainen verrattuna kiristyshaittaohjelmiin. Jotkut organisaatiot ovat tunnistaneet tapauksia jopa 1kk jälkeen, että heidän järjestelmiinsä on hakkeroitu, mutta joskus asia selviää vasta jopa 24kk päästä ja silloinkin vasta kun jokin ulkopuolinen taho on heihin yhteydessä. Tarkasteltujen tapauksia osalta keskiarvona oli 8kk siitä kun, hakkerointi oli tapahtunut ja ennen kuin organisaatio tulee siitä tietoiseksi. Tämä on hyvin huolestuttavaa koska tämä antaa hyökkääjälle pitkän ajan toimia huomaamatta ympäristössä ja kerätä niitä tietoja, joita he tarvitsevat. Pitkän ajan jälkeen on myös tutkinta hankalaa ja voi olla mahdotonta tunnistaa mitä kaikkea tietoja on varastettu, josta syystä tällaiset hyökkäykset saattavat koskea miljoonia potilaita.

4.5 Yhteenveto

Sairaaloiden ja terveydenhuollon organisaatioiden tulisi kiinnittää entistä enemmän huomiota kyberturvallisuuteen. Suuret järjestelmät, joissa on myös vanhoja osia, joita ei ole mahdollista päivittää ovat haavoittuvaisia. Kasvava määrä hyökkäyksiä on nimenomaan kohdistettu sairaaloihin ja potilastietojärjestelmiin ja ne eivät enää ole pelkästään laajojen roskaposti-kampanjojen kohteena.

Kaikilta hyökkäyksiltä ei ole mahdollista turvautua, mutta ainakin perus tietoturva pitäisi olla kunnossa ja erityishuomiota tulisi kohdistaa toiminnan kannalta kriittisiin järjestelmiin kuten potilastietoihin. Monien tapauksien taustalta on myös henkilöstön tietämättömyys tietoturvasta ja se aiheuttaa huonojen päätök-



KUVA 11: ISO27005: Riskien käsittely (SFS-käsikirja 2012, 205).

sien tekemisen. Henkilöstönkoulutus on yksi tapa lisätä tietoisuutta ja vähentää eri hyökkäyksien onnistumista. Monet kyberturvallisuuden ongelmista eivät ole ainutlaatuisia terveydenhuollossa, mutta niiden vaikuttavuus toimintaan ja potilaiden turvallisuuteen ja hoitoon tekee näistä organisaatioista erittäin haavoittuvaisia.

Rikolliset ovat myös tietoisia potilastietojen arvosta, sekä niiden kriittisyydestä toimintaan, joten näihin organisaatioihin heidän on kannattanut hyökätä.

Kyberturvallisuus ongelmat tulevat kasvamaan myös sairaala ympäristöissä, joissa on paljon järjestelmiä, joista vanhat laitteet käyttävät ei enää tuettuja käyttöjärjestelmiä. Sairaaloissa on myös järjestelmiä ja laitteita, joita ei ole mahdollista päivittää, joko sen vuoksi että niihin ei ole saatavissa päivityksiä tai nämä laitteet eivät voi olla pois toiminnasta päivityksien vuoksi.

Sairaala ympäristöt ovat myös haastavia koska sinne tuodaan henkilökunnan ja potilaiden omia laitteita, sekä valtava määrä erilaisia lääkinnällisiä laitteita, joita käytetään tutkimuksissa tai potilaiden seurannassa. Nämä järjestelmät ja laiteet avaavat rikollisille monia hyökkäys mahdollisuuksia ja pintoja.

Toiminnan riskitarkastelu

Riskiä voidaan tarkastella sekä taloudellisen arvon että maineen menettämisen kannalta. Riskien arvioinnin tuloksista tulee johtaa päätösprosessi esimerkiksi edellisellä sivulla olevan kuvan 11 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.

LUKU 5
Sairaalan kyberturvallisuus

5.1 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, et al, 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 tosiaisa 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 (esim. 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.

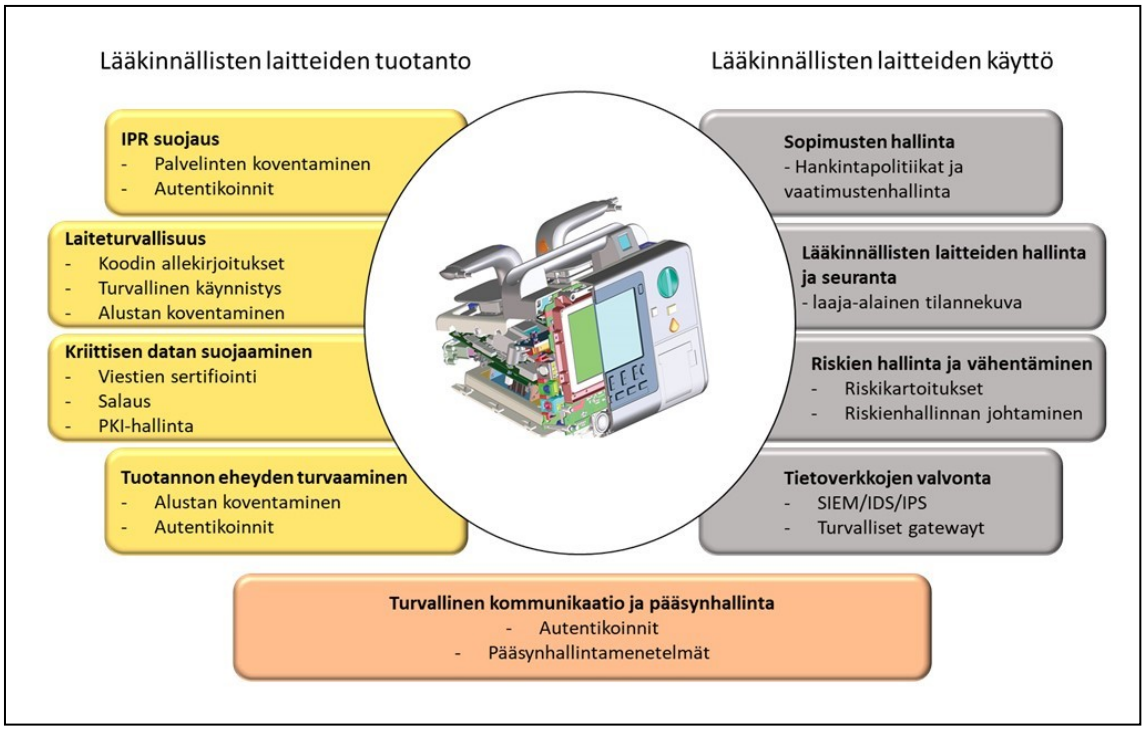
* Luodaan älykkäille sairaalalaitteille selkeä tietoturvastrategia, jossa roolit ja vastuut sekä säännöllinen koulutus ja tietoisuuden lisääminen ovat keskeisiä tekijöitä ennakoivan lähestymistavan aikaansaamiseksi tietoturvaan.

* 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



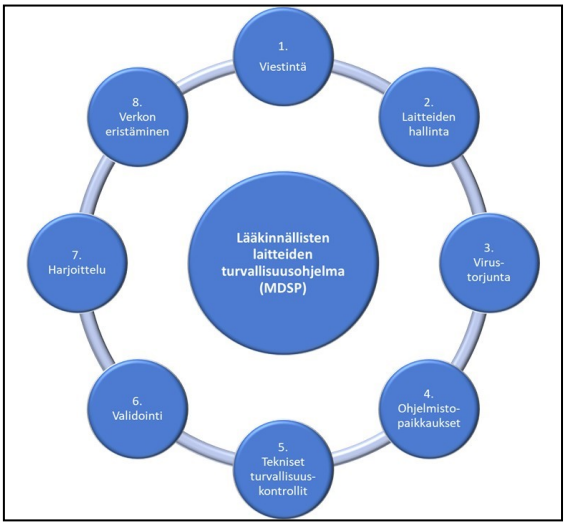
KUVA 12: Lääkinnällisten laitteiden kyberturvallisuus – Jaettu vastuu (Symantec Corporatio, 2016, 2.).

on kehitettävä kyberosaamisohjelmia kouluttaakseen toimintaketjujensa päätöksentekijöitä. (Csulak ym., 2017, 40.)

5.2 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. Kuvassa 12 on vastuutoimenpiteitä hahmoteltu laitevalmistajan ja käyttäjäorganisaation kesken.

Lääkinnällisten laitteiden turvallisuusohjelma (ks. kuva 13) 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 mal-



KUVA 13: Lääkinnällisten laitteiden turvallisuusohjelma (Meditology Services LLC, 2017, 10).

lin 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.)

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 (ks. taulukko 5 ja taulukko 6).

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.

5.3 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.)

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 5: Lääkinnällisten laitteiden prioriteettitasot (Meditology Services LLC, 2017, 10).

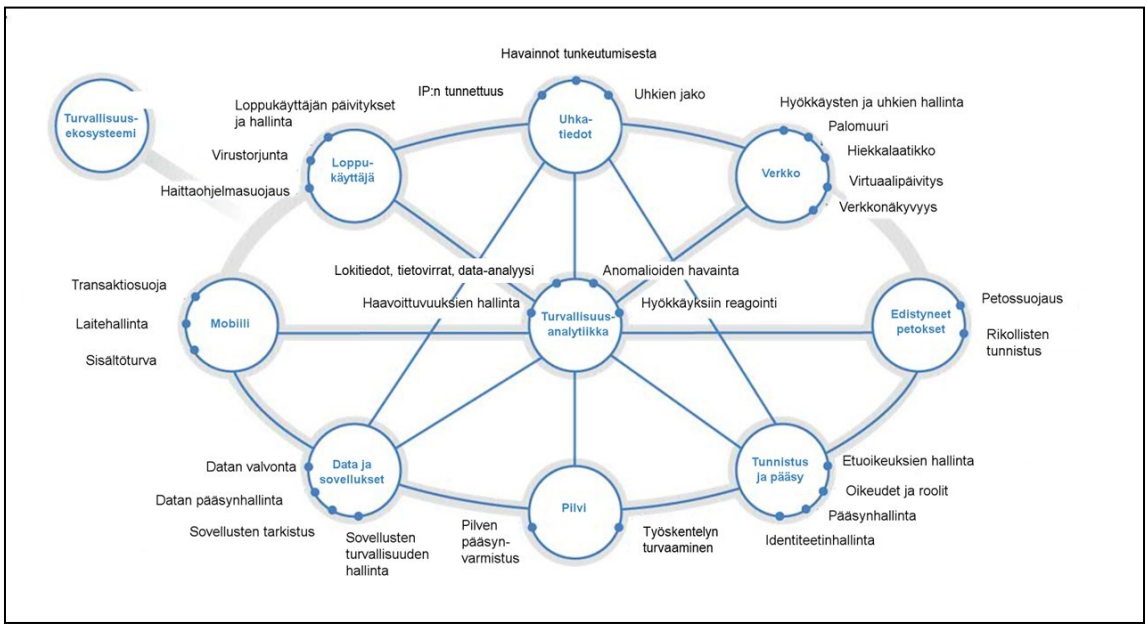
Turvallisuusluokitus	Kuvaus
A	Yli 100 000 merkintää tallennettu, lähetetty tai käsitelty
B	10 001–99 999 merkintää tallennettu, lähetetty tai käsitelty
C	Alle 10 000 merkintää tallennettu, lähetetty tai käsitelty
D	Laite ei tallenna, lähetä tai käsittele terveystietoja

TAULUKKO 6: Lääkinnällisten laitteiden turvallisuusluokitukset (Meditology Services LLC, 2017, 10).

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 (ks. kuva 15, s. 56).

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



KUVA 14: IBM:n integroitu kyberturvallisuuskonsepti (Falco, 2016).

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.

Edellisen sivun kuvassa 14 on esitetty esimerkkinä IBM:n konsepti integroidusta kyberturvallisuusratkaisusta, jossa analytiikkakyvykkyys on asetettu ratkaisun keskiöön.

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.)

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, 1):

* 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, 1):

* Toimintamallit luodaan salatun datan käsittelyyn, esim. 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 mm. ulkoistettujen toimintojen kautta (mm. 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 mm. digitaaliset älykkäät sopimukset, sähköiset omaisuusrekisterit, identiteettirekisterit, laitteiden väliset tiedot ja autonomiset organisaatiot (ks. kirjasarjan osa 1, s. 160).

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.)

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. (Daim, 2017).

LUKU 6

Sairaalan kyberturvallisuusarkkitehtuuri

6.1 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.

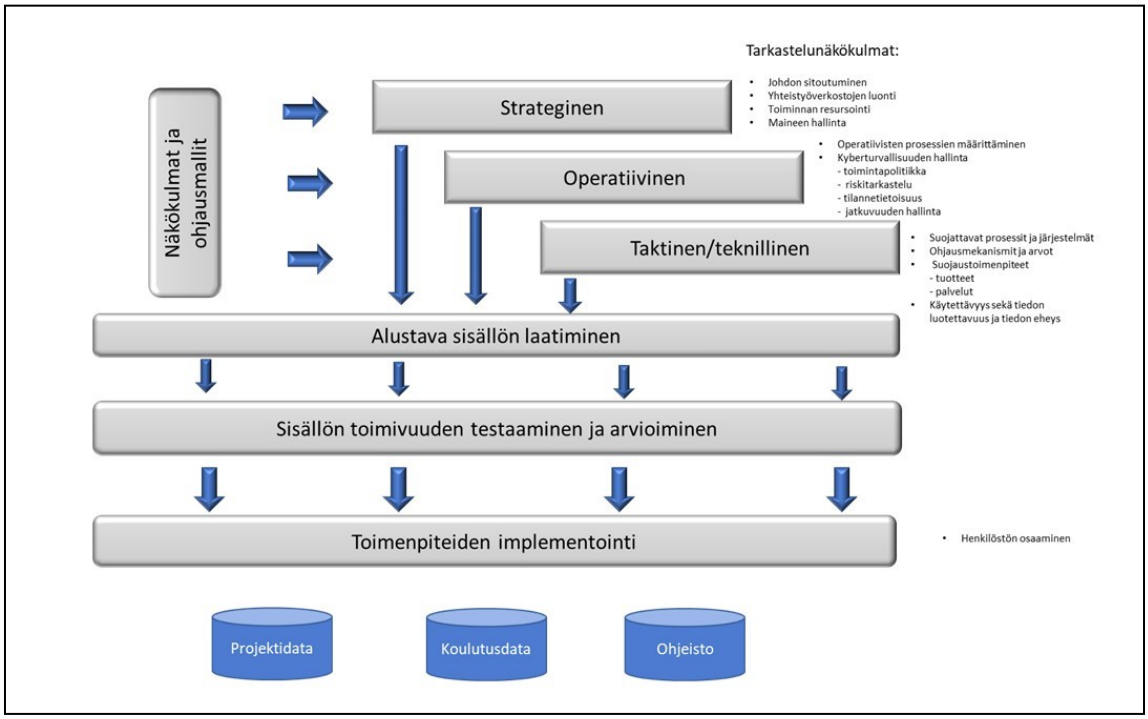
Alustaratkaisu voisi mahdollistaa tehokkaan kyberturvallisuuden asiantuntijaverkoston ja tekoälysovelluksen yhteistyön, jossa tekoäly toimii avustavan asiantuntijan roolissa toteuttamalla toimintaympäristössä tarvittavia toimenpiteitä ja samalla tuottamalla jalostettua informaatiota päätöksenteon pohjaksi.

Kehittäminen voi tapahtua muodostamalla älykäs järjestelmäalusta. Älykäs järjestelmäalusta vastaa kyberturvallisuusarkkitehtuurissa kysymykseen: miten IT-infrastruktuurin suojaustoimenpiteet on suoritettava? Se liittyy organisaation toimintatasolla teknillistaktiseen 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 kuvalla 15. Siitä ilmenevät sekä eri näkökulmat pääasiallisine sisältöineen, että sen toteutusprosessi vaiheineen.

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. Kuvan 15 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-



KUVA 15: Sairaalan kyberturvallisuusarkkitehtuuri.

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.
- Kehitetään 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.

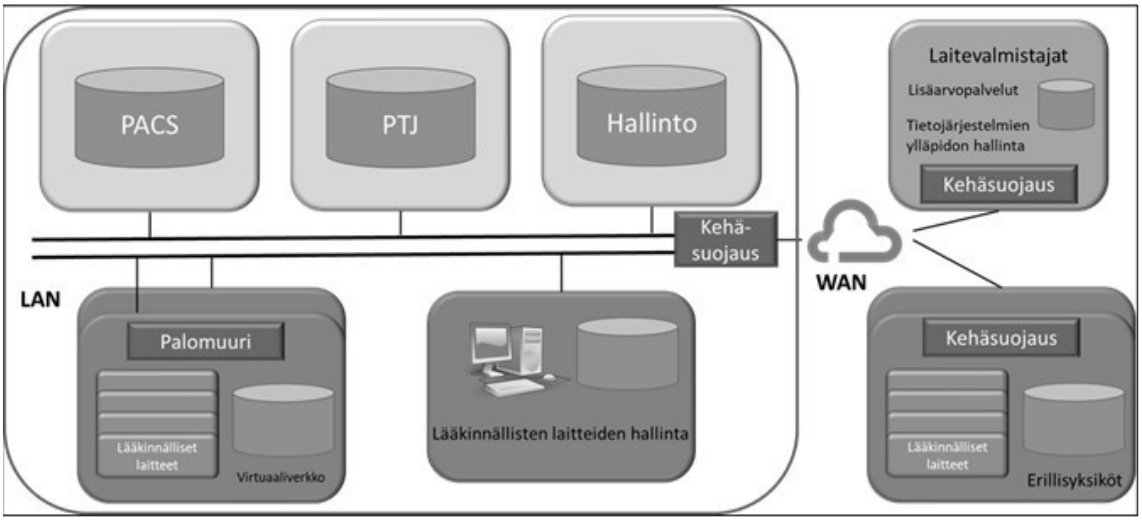
Kehitetään salassapidon ja yksityisyyden suojaa tiedonhankinnassa, tietojen analysoinnissa ja jakamisessa. Tähän lohkoketjutekniikka tarjoaa laajassa mitassa luotettavuutta.

6.2 IBM Security-kyberturvallisuuskonsepti

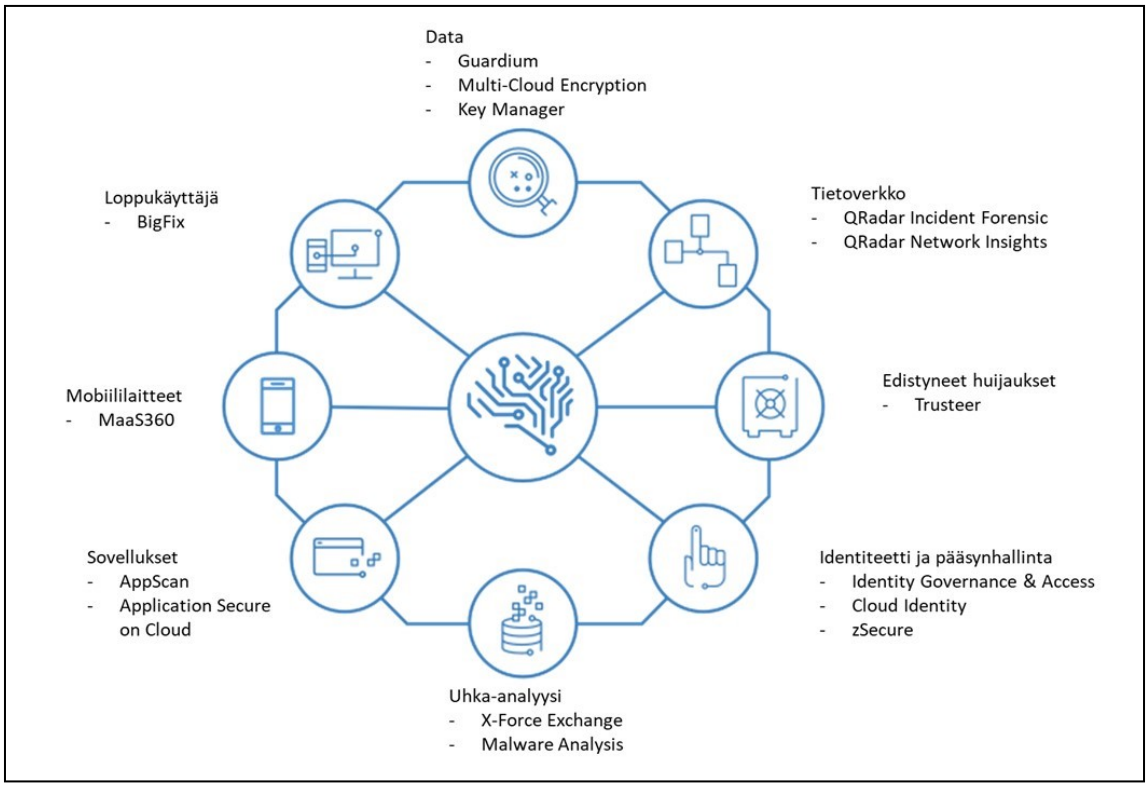
Vyöhykesuojaus ja älykkäät suojausratkaisut

Älykkään kyberturvallisuusarkkitehtuurin avulla voidaan kehittää kyberfyysisten järjestelmäalustojen turvallisuutta kaikilta osiltaan yhdistämällä perinteiseen vyöhykesuojausstrategiaan uuden teknologian avulla integroituja ratkaisuja. Kehittämisen seurauksena kokonaisuudesta muodostuu älykäs järjestelmäalusta. Kuvassa 16 vasemmalla on sairaalajärjestelmä, joka pitää sisällään vyöhykesuojauksen menetelmiä ja oikealla on IBM:n integroitu kyberturvallisuuskonsepti. (Falco, 2015; Integrating the Healthcare Enterprise, 2015, 9 –10.)

Kuvassa 16 A sairaalajärjestelmä on jaettu vyöhykkeisiin suojausvaatimusten ja -tason mukaisesti (Perimeter Security). Vyöhykkeiden välillä on tyypillisesti sekä fyysisiä että tieto-



KUVA 16 A: Sairaalajärjestelmän kyberturvallisuuskonsepti.



KUVA 16 B: IBM:n integroitu kyberturvallisuuskonsepti ja sen sovellukset.

teknisiä suojamuureja (esim. 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 kuvassa 16 B 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 (ks. kuva 5).

IBM konsepti

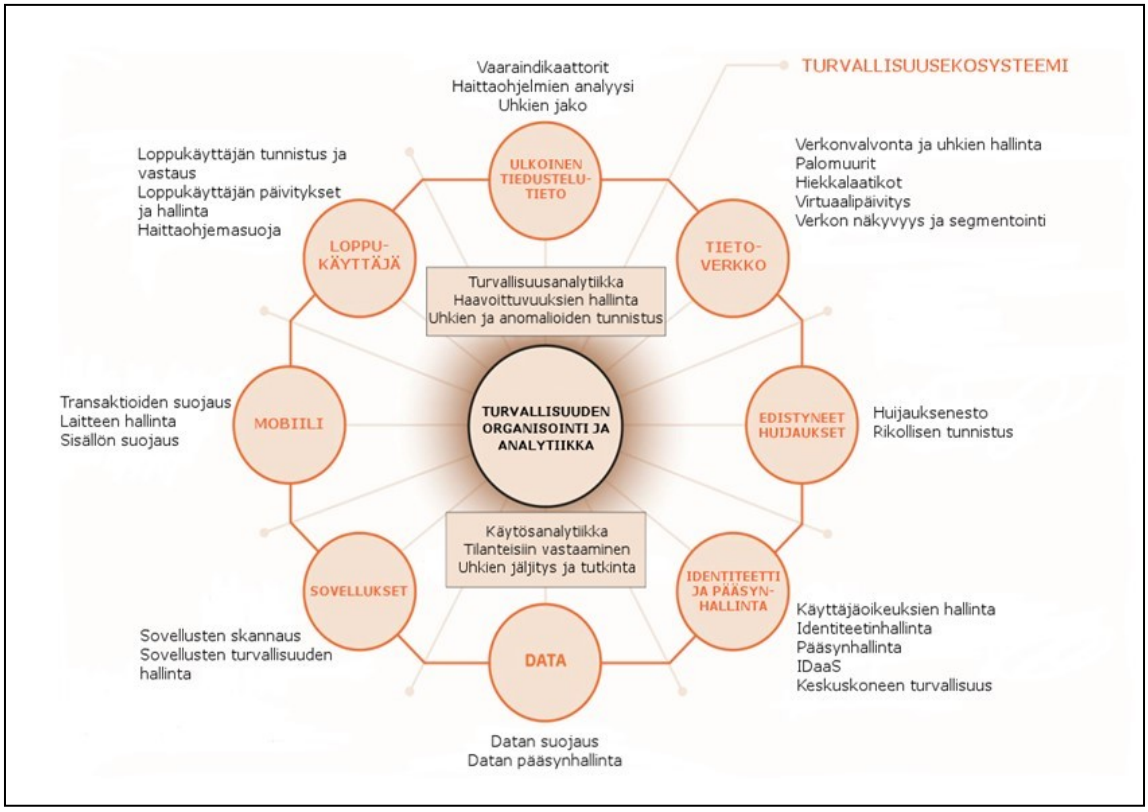
IBM:n konseptin ja sen sovellustason ratkaisujen (kuvat 16 B ja 17) keskeisenä kyberturvallisuutta analysoivana ja toimenpiteiden ohjaus-

ta 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 mm. 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.

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.



KUVA 17: IBM Security – integroitu kyberturvallisuuskonsepti.

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.

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.

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). Loppukäyt-

täjän 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-infrastruktuurin 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.

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.

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.

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 rutiineja 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.

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, joka 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.

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 iden-

titeetin 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 mm. 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.

LUKU 7

Toimenpiteet sairaalan kyberturvallisuuden edistämiseksi

7.1 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 (2016, 11.) painottaa uudistuksissa tietoturvastrategioiden ja kustannus-hyötyanalyysien merkitystä strategisella päätöksentekotasolla päätettävistä riittävistä kyberturvallisuutta edistävistä suojausratkaisuista. 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.

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 kustannushyötyanalyysien huomioimisesta päätöksenteosta.

Valituista toimenpiteitä tulee viestittää kattavasti organisaation henkilöstölle ja muille sidosryhmille.

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. 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.

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 (ks. 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 (esimerkiksi 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 (ks. kuva 18).

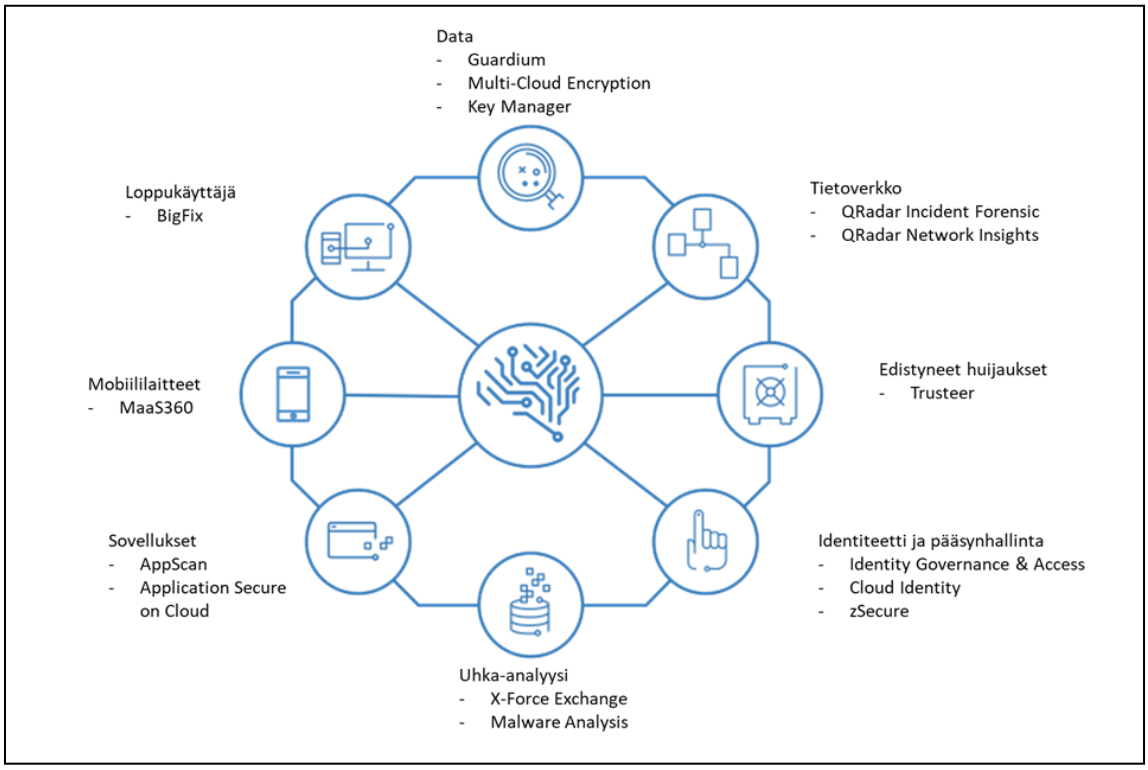
Sairaalan ICT-järjestelmistä ja niiden laitteista muodostuva teknillinen kokonaisuus on systeemiajatuksen mukaan terveydenhuollon osajärjestelmä. Sitä voidaan hyvin kutsua sairaalan ICT-alustaksi. Tällöin systeemitason näkökulmasta katsottuna tuleekin huolehtia siitä, että kaikilla terveydenhuollon toimijoilla 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.

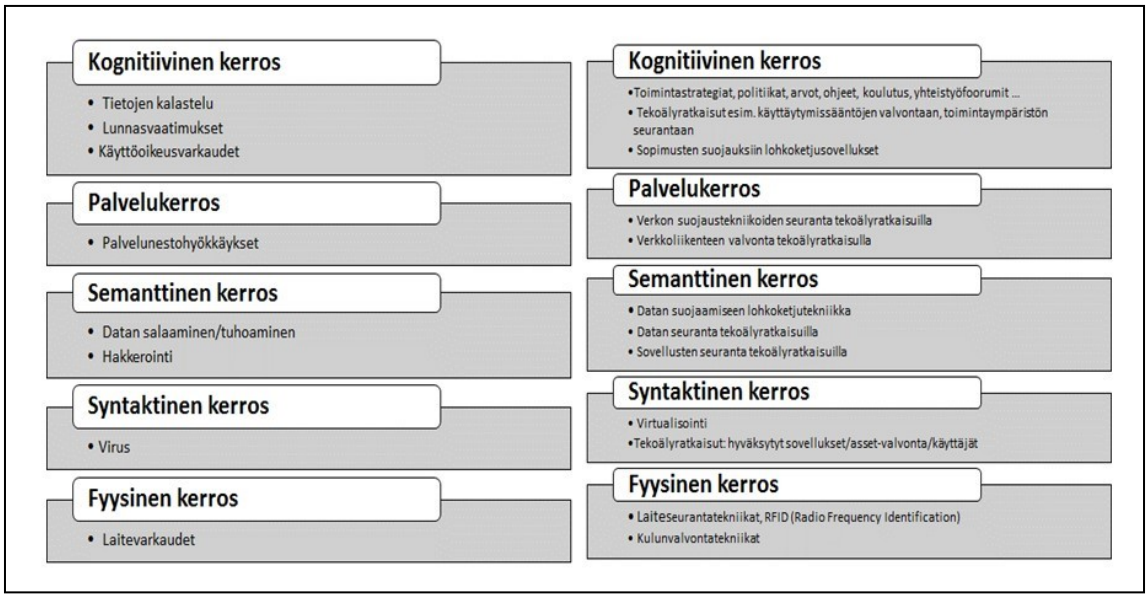
7.2 Systeemitason suojauksen teknillinen kehittäminen

Suojauksen kehitystä edistävät tekniikat

Kyberfyysisissä järjestelmissä verkon avulla yhteen liitetyt laitteet ohjelmistoineen kontrol-



Kuva 18: IBM:n integroitu kyberturvallisuuskonsepti ja sen sovellukset.



KUVA 19: Sairaalajärjestelmien uhkakuvat ja uudet suojaustekniikat.

loivat fyysisiä prosesseja. Sairaalan toimintaan liittyy merkittävä määrä teknillisiä laitteita ja niistä koostuvia toiminnallisia kokonaisuuksia ja 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:n 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 suojauskehiinperustuvat turvallisuusratkaisut eivät vastaa enää riittävästi tämän päivän kehittyneisiin uhkiin, jotka tulevat laajalta alueelta joko organisaation ulkoa tai sisältä (Suomen Automaatioseura ry Turvallisuusjaosto, 2010, 69). 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 tekoäly-sovelluksen 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.

Kuvassa 19 edellisellä sivulla 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 (ks. luku 5.3). Ratkaisut voidaan rakenteessa kohdistaa sen eri kerroksille, jolloin niiden yhteisvaikutuksella ns. systeemitason teknillistä suojausta voidaan tavoitella.

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.

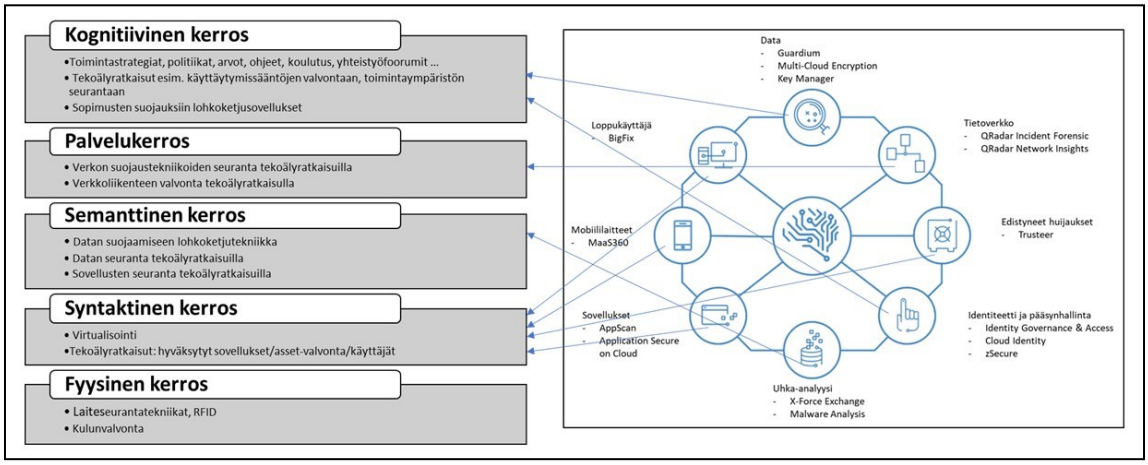
Sairaalan älykkäässä alustassa tulee huomioida erityisesti langattomiin yhteyksiin pohjautuvien laitteiden vianilmaisu ja niiden käytön mallinnukseen perustuva vianhavaitsemisjärjestelmä. Virtualisointitekniikan avulla voitaneen suojautua tai puolustautua hyökkääjiä vastaan käyttämällä osoitealueita, 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 mm. 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.

IBM Watson systeemitasolla

IBM kyberturvallisuuskonseptin kahdeksan eri osaa voidaan liittää viisikerroksiseen ICT-rakenteeseen oheisen kuvan 20 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



KUVA 20: Suojaustekniikat ja niihin liittyvät IBM kyberturvallisuuskonseptin osat.

(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.

7.3 Systeemitason suojauksen yhteenveto

Systeemitason suojauksen lähtökohtana on yhdistelmä strategisen päätöksentekotason toimenpiteitä, jotka täyttävät arkkitehtuurin (kuva 15) 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 (ks. kuva 12) 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 (ks. taulukko 4 ja taulukko 5). 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 kuvan 15 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.

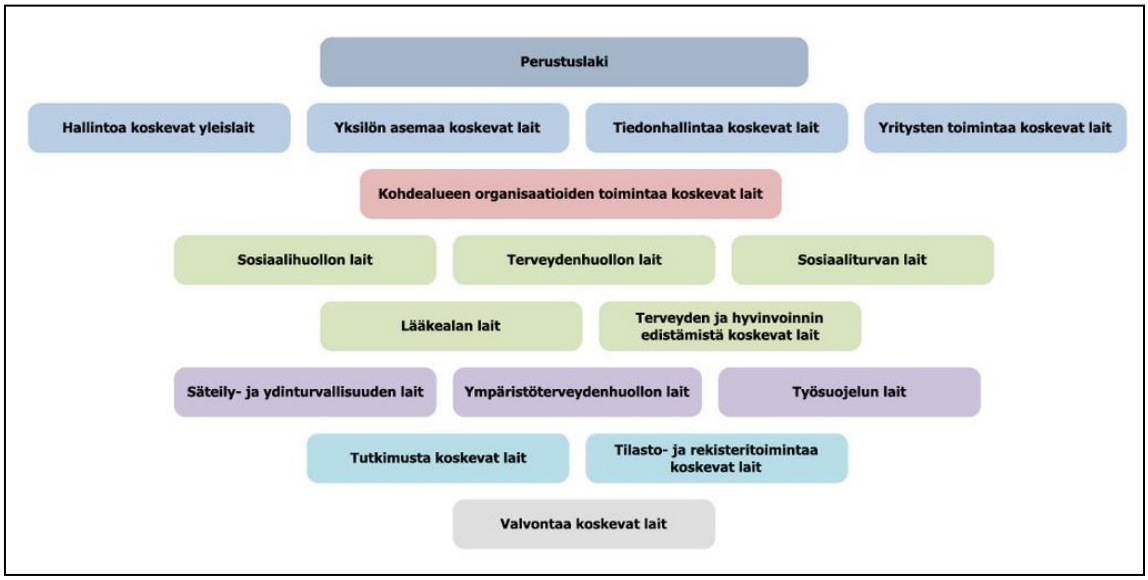
LUKU 8

SOTE-lainsäädäntö sekä terveys– ja hyvinvointidata

Terveyden ja hyvinvoinnin alueen lainsäädännön kokonaisuus on laaja ja asiakastiedon hyödyntämisestä säädetään eri näkökulmista. Kohdealuetta koskeva lainsäädännön analyysi on tehty koko kohdealutta kuvaavassa kokonaisarkkitehtuurikuvauksessa. Terveyden ja hyvinvoinnin kohdealueen lainsäädännön kokonaisuus on esitetty kuvassa 21.

8.1 Potilasasiakirjamerkinnät

Terveydenhuollon ammattihenkilöistä annetun lain (559/1994) mukaan terveydenhuollon ammattihenkilön tulee laatia ja säilyttää potilasasiakirjat sekä pitää salassa niihin liittyvät tiedot sen mukaan, mitä laissa potilaan asemasta ja oikeuksista säädetään (785/1992). Sosiaali- ja terveysministeriön antamassa asetuksessa potilasasiakirjoista (298/2009, jäljempänä potilasasiakirja-asetus) on säädetty potilaskertomukseen kirjattavista perustiedoista ja hoitoa koskevista merkinnöistä. Potilasasiakirja-asetus asettaa vaatimuksia potilasasiakirjojen sisällölle. Potilasasiakirjoihin on terveydenhuollon ammattihenkilön tai hänen ohjeistuksensa mukaisesti muun hoitoon osallistuvan henkilön merkittävä potilaan hoidon järjestämisen, suunnittelun ja toteuttamisen seurannan turvaamiseksi tarpeelliset ja laajuudeltaan riittävät tiedot. Merkintöjen tulee olla selkeitä ja ymmärrettäviä ja niitä tehtäessä on käytettävä yleisesti tunnettuja ja hyväksyttyjä käsitteitä ja lyhenteitä. Jokaisen terveydenhuollon toimintayksikön ja itsenäisesti ammattiaan harjoittavan terveydenhuollon



KUVA 21: Terveyden ja hyvinvoinnin kohdealueen lainsäädännön kokonaisuus (Virkkunen ym. 2015).

ammattihenkilön tulee pitää jokaisesta potilaasta jatkuvaan muotoon laadittua, aikajärjestyksessä etenevää potilaskertomusta. Potilaskertomuksessa on oltava potilaan perustiedot, esimerkiksi potilaan nimi, syntymäaika, henkilötunnus, kotikunta ja yhteystiedot, ja siihen tulee tehdä merkinnät jokaisesta potilaan palvelutapahtumasta. Näistä tiedoista tulee käydä ilmi tulosyy, esitiedot, nykytila, havainnot, tutkimustulokset, ongelmat, taudinmääritys tai terveysriski, johtopäätökset, hoidon suunnittelu, toteutus ja seuranta, sairauden kulku sekä loppuarvio. Sosiaali- ja terveysministeriö on julkaissut potilasasiakirja-asetukseen perustuvan oppaan (STM 2012). Siinä kuvataan tarkemmin potilasasiakirjojen laatimista ja muuta potilastietojen käsittelyä.

8.2 Yksityisyys ja potilastietojen käsittely

Potilastietojen käsittely perustuu henkilötietolakiin (523/1999). Sen tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Lisäksi laissa potilaan asemasta ja oikeuksista (785/1992), laissa sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000), laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007) ja laissa viranomaisen toiminnan julkisuudesta (621/1999) tarkennetaan potilastiedon käyttöä ja rekisterinpitoa. (Virkkunen ym. 2015)

Suomessa on lainsäädännöllä määrätty, kuinka potilaskertomusmerkintöjä tehdään, kuinka asiakirjoja on säilytettävä ja kenellä on oikeus lukea niitä. Aiemmin potilaskertomukset säilytettiin sairaalakohtaisesti, mutta vuonna 2010 terveydenhuoltolaki mahdollisti sairaanhoitopiirin laajuisen yhteisen potilastietorekisterin. Valtakunnallinen potilastiedon arkisto (Kanta) on otettu käyttöön 2013. Julkisen terveydenhuollon palvelunantajilla on velvollisuus liittyä sen käyttäjiksi syyskuuhun 2014 mennessä ja yksityisten palvelujenantajienkin syyskuuhun 2015 mennessä. Ainoastaan sellaisen palvelunantajan, jolla ei ole sähköistä potilaskertomusjärjestelmää ei tarvitse siihen liittyä. (Virkkunen ym. 2015)

Valtakunnalliseen arkistoon tallennettava tietosisältö lisääntyy vaiheistusasetuksen määräysten mukaan. Potilailla on mahdollisuus katsoa valtakunnallisessa arkistossa olevia omia tietojaan. Potilaat voivat Omakannan avulla hallita sitä, mitä tietoja valtakunnallisen arkiston kautta välitetään muille palvelunantajille. Lisäksi potilaat voivat tehdä Omakannan kautta elinluovutusta koskevan tahdonilmaisun tai hoitotahdon. (Virkkunen ym. 2015)

Potilasasiakirjat muodostavat henkilötietolaissa tarkoitetun loogisen henkilörekisterin. Samaan henkilö- rekisteriin kuuluvat kaikki ne potilasta koskevat tiedot, jotka ovat rekisterinpitäjän hallussa ja joita käytetään samaan käyttötarkoitukseen riippumatta tietojen tallentamistavasta, -ajankohdasta tai -paikasta. Rekisterinpitäjänä toimii terveydenhuollon toimintayksikkö tai itsenäisesti ammattiaan harjoittava terveydenhuollon ammattihenkilö. (STM 2012) Potilas- tai asiakastiedon käyttö edellyttää aina asiakas- tai potilassuhdetta ja asiayhteyttä. Henkilötietolaki edellyttää, että henkilörekisterin käyttötarkoitus määritellään siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään, mistä henkilötietoja säännönmukaisesti hankitaan ja mihin niitä säännön-

mukaisesti luovutetaan. Samoin kaikki muut käsittelyvaiheet ja prosessin eri vaiheet määritellään ja kuvataan, jotta tietojärjestelmät ja niiden rakenteet voidaan suunnitella ja toteuttaa kaikkien käsittelyvaiheiden osalta toiminnallisten, teknisten ja oikeudellisten vaatimusten kannalta asianmukaisesti. (Virkkunen ym. 2015)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007, jäljempänä asiakastietolaki) tuli voimaan heinäkuussa 2007 ja muutettiin 2014 (250/2014). Laki sisältää säännökset sosiaali- ja terveydenhuollon asiakastietojen sähköisen käsittelyn yleisistä vaatimuksista mm. potilastiedon käyttöä säätelevien potilaan informoinnin, suostumuksen ja kieltojen suhteen. Sen tarkoituksena on turvata näiden tietojen käytettävyys, eheys ja säilyminen sekä asiakkaan yksityisyyden suoja. Asiakastietojen käsittelylle asetettavien yleisten vaatimusten avulla luodaan perusta asianmukaiselle sähköiselle tietojenkäsittelylle, jossa edellytetään yhtenäisen tietoturvatason toteutumista kaikissa asiakkaan tietojen käsittelyn vaiheissa. (Virkkunen ym. 2015)

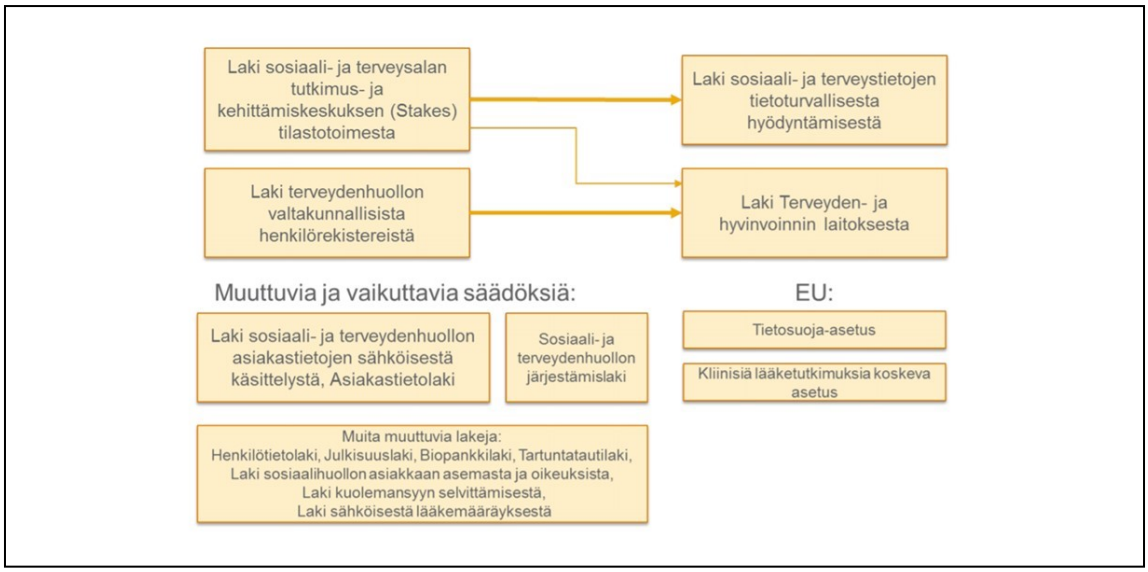
Sosiaalihuollon nykyinen tiedonkeruu perustuu lakiin sosiaali- ja terveysalan tutkimus- ja kehittämiskeskuksen tilastotoimesta (409/2001). Lakia kutsutaan myös Stakesin tilastolaiksi.

Terveydenhuollon laitos- ja avohoidon tiedonkeruu perustuu lakiin (556/1989) ja asetukseen (774/1989) terveydenhuollon valtakunnallisista henkilörekistereistä. Edellä mainitut lait tullaan korvaamaan laeilla:

- Laki sosiaali- ja terveystietojen tietoturvallisesta hyödyntämisestä.

- Laki sosiaali- ja terveydenhuollon valtakunnallista henkilörekistereistä.

Edellä mainitut lait koskevat nimenomaan kansallista tiedonkeruuta (Stakesin tilastolaki ja laki terveydenhuollon valtakunnallisista henkilörekistereistä). Terveyden ja hyvinvoinnin lainsäädännön muutoskokonaisuus on esitetty kuvassa 22.



KUVA 22: Terveyden ja hyvinvoinnin lainsäädännön muutoskokonaisuus (Sosiaali- ja terveystietojen tietoturvallisen hyödyntämisen kokonaisarkkitehtuuri, luonnos 2017).

Lainsäädäntö ohjaa potilas- ja hoitotietojen kirjaamista ja käsittelyä:

* Laki potilaan asemasta ja oikeuksista (785/1992, potilaslaki).

* STM:n asetus lääkkeen määräämisestä (1088/2010).

* Henkilötietolaki (523/1999).

* Laki viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki).

* STM:n asetus potilasasiakirjoista (298/2009, potilasasiakirja asetus), joka ohjaa mm. rakenteista kirjaamista.

* Laki sähköisestä lääkemääräyksestä.

* Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä.

* Biopankkilaki (688/2012).

Laki sähköisestä lääkemääräyksestä (eResepti-laki) säätää sähköisen reseptin käyttöönoton pakolliseksi apteekeille, terveydenhuollon toimintayksiköille ja terveydenhuollon toimintayksikön tiloissa vastaanottoa pitäville ammatinharjoittajille. Käyttöönotto on vapaaehtoista terveydenhuollon toimintayksiköille Ahvenanmaalla sekä itsenäisinä ammatinharjoittajina muualla kuin terveydenhuollon toimintayksikön tiloissa toimiville lääkäreille ja hammaslääkäreille.

Sähköisestä lääkemääräyksestä annetun lain tavoitteena on potilas- ja lääketurvallisuuden parantaminen sekä lääkkeen määräämisen ja toimittamisen helpottaminen ja tehostaminen.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (Asiakastietolaki) velvoittaa julkiset terveydenhuollon organisaatiot tallentamaan potilastiedot valtakunnallisesti keskitettyyn arkistoon. Yksityisille terveydenhuollon organisaatioille keskitetyn arkiston käyttöönotto on pakollista, jos potilasasiakirjojen pitkäaikaissäilytys toteutetaan sähköisesti. Käyttöönotto on vapaaehtoista terveydenhuollon toimintayksiköille Ahvenanmaalla. Asiakastietolain tavoitteena on edistää potilastietojen tietoturvallista käsittelyä, potilaiden tiedonsaantimahdollisuuksia sekä terveydenhuollon palveluiden potilasturvallista ja tehokasta tuottamista.

Biopankkilaki (688/2012)

Sairaanhoitopiirien ja yliopistollisten sairaaloiden yhteydessä toimivilla biopankeilla on hallussaan näytteitä ja näytteisiin liittyviä tietoja, joiden kerääminen perustuu ensisijaisesti suostumukseen. Biopankkitoimintaa sääntelevän biopankkilain tarkoitus on tukea tutkimusta, jossa hyödynnetään ihmisperäisiä näytteitä, ja samalla turvata yksityisyydensuoja ja itsemääräämisoikeus. Kuitenkin ns. vanhoja kliinisiä näytteitä ja tutkimusnäytteitä voidaan siirtää biopankkiin, ellei näytteen antaja sitä erikseen kiellä (nk. ilmoitusmenettely). (Tarja Martti, Viitanen Jaakko, 2016) Laki tuli voimaan 1.9.2013 (tähän mennessä perustettu 6 biopankkia).

Lain tarkoituksena on tukea tutkimusta, jossa hyödynnetään ihmisperäisiä näytteitä, edistää näytteiden käytön avoimuutta sekä turvata yksityisyyden suoja ja itsemääräämisoikeus näytteitä käsiteltäessä.

Biopankin toiminnan aloittamisen edellytyksenä on tukijan puoltava lausunto, ilmoitus valtakunnalliseen biopankkirekisteriin ja biopankista vastaava henkilön nimeäminen. Biopankkitoiminnassa on kyse henkilötietojen käsittelystä eli lisäksi sovelletaan usein myös henkilötietolakia (523/1999) ja julkisuuslakia (621/1999).

Henkilötietojen käsittelyyn liittyviä säädöksiä ja säännöksiä

Henkilötietolaki:

* Rekisterinpitäjän velvollisuudet ja henkilötietojen käsittelyn perusteet.

* 11 § Arkaluonteisten tietojen käsittelykielto.

* 12 § Oikeus käsitellä SOTE:n omassa toiminnassa.

Laki viranomaisten toiminnan julkisuudesta:

* 24 § 25 kohta SOTE-tiedot salassa pidettäviä säännöksiä tietojen käsittelystä + asetuksenantovaltuus.

Laki sosiaalihuollon asiakasasiakirjoista (Asiakasasiakirjalaki):

* Velvollisuus kirjata määrämuotoisiin asiakasasiakirjoihin + määräystenantovaltuus THL:lle.

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (Sosiaalihuollon asiakaslaki):

* 16–19, 27 § salassapitovelvoitteet ja oikeus poiketa niistä.

* 11, 3 § alaikäisen oikeus määrätä palveluistaan ja tiedoistaan.

Laki potilaan asemasta ja oikeuksista (Potilaslaki):

* 7.1 ja 9.2 § Alaikäisen oikeus määrätä hoidostaan ja tiedoistaan.

* 12 § Velvollisuus kirjata potilastiedot + asetuksenantovaltuus.

Potilasasiakirja-asetus:

* Potilastietojen kirjaamista ja muuta käsittelyä koskevat säännökset.

* 13 § Salassapitovelvoitteet ja poikkeusperusteet, sivullisen määritelmä.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (Asiakastietolaki):

* Kanta- (ja Kansa-) arkistoa koskevat säännökset.

* Sähköisten asiakastietojen tallentamista, säilytystä, luovutusta ja muuta käsittelyä koskevat säännökset.

8.3 Tietojen luovutus

Valtakunnallisten rekistereiden tietoja voidaan luovuttaa tieteelliseen tutkimukseen. Eniten tutkimuspyyntöjä on kohdistettu erikoissairaanhoidon hoitoilmoitusrekisterin tietoihin ja syöpärekisteriin. Rekistereiden tietojen hyödyntäminen tutkimustoimintaan edellyttää tutkimussuunnitelmaa ja aineiston käyttölupaa. THL voi antaa luvan rekisteritietojen saamiseen. Kun rekistereiden tietoa halutaan yhdistää muiden rekisterinpitäjien tietoihin, lupa anotaan erikseen eri rekisterinpitäjiltä. THL voi antaa luvan tietojen saamiseen yksittäistapauksessa, kun tieteellistä tutkimusta varten tarvitaan tietoja useamman kuin yhden SOTE-organisaation asiakas- tai potilastiedoista. (Tarja Martti, Viitanen Jaakko, 2016)

Osaa valtakunnallisten rekisterien tiedoista voidaan hyödyntää SOTE-organisaatioiden päivittäisessä työssä, esimerkkinä Tartuntatautirekisteri, johon tietoja välitetään suoraan myös näytteitä analysoivista laboratorioista. Valtakunnallista tartuntatautirekisteriä hyödynnetään erityisesti valtakunnallisessa tartuntatautien vastustamistyössä. Käyttö paikallisessa ja alueellisessa päätöksenteossa lienee rajoitettu. (Ibid.)

Henkilöillä ei ole pääsyä THL:n valtakunnallisten terveydenhuollon eikä sosiaalihuollon rekistereiden itseä koskeviin tietoihin, ei mah-

dollisuutta määrätä tietojen käytöstä eikä tarkistaa tietojen oikeellisuutta. Yksinomaan tilastointia taikka historiallista tai tieteellistä tutkimusta varten olevien rekistereiden henkilötietojen tarkastusoikeuden rajoitukset on säädetty henkilötietolaissa. (Ibid.)

Terveydenhuollon ammattilaiset käyttävät tarvittaessa Kanta-palveluja suoraan potilastietojärjestelmän tai Kanta-arkiston selainkäyttöliittymän kautta. Henkilöt voivat katsella itse omia potilasasiakirjansa tietojaan ja hallinnoida omien potilastietojen käyttöä Omakanta-palvelulla. (Ibid.)

Kanta-palvelujen Potilastiedon arkistoon tallennettuja potilastietoja ei voi nykyisen lainsäädännön mukaan hyödyntää tutkimuksiin. Tutkimusten potilastietoaineistoja on poimittava yksittäisistä potilastietojärjestelmistä tai THL:n hoitoilmoitusrekistereistä. Asiakas- ja potilastietojen hyödyntämiseen valtakunnallisten rekistereiden kautta on viiveellistä johtuen tietojen keruutavoista, laaduntarkastuksesta, julkaisuaikatauluista, lupakäsittelystä ja käytettävissä olevista aineistojen poimintaresursseista. Tiedon saamiseen voi kulua aikaa jopa vuosi ja luovutettu tieto koskee yleensä edellistä kalenterivuotta.

Kanta-palvelujen Reseptikeskuksen tietojen käyttö tutkimustoimintaan on lainsäädännöllä mahdollistettu. Kela saa luovuttaa Reseptikeskuksessa ja Reseptiarkistossa olevia tietoja tieteelliseen tutkimukseen. Luovutus edellyttää kuitenkin aina Terveyden ja hyvinvoinnin laitoksen lupaa. (Ibid.)

8.4 Tilastolaki

Tämän lain tarkoituksena on yhteiskunnallista päätöksentekoa ja suunnittelua varten tarvittavan luotettavan tilastotiedon saannin varmistamiseksi sekä kansainväliseen tilastoyhteistyöhön liittyvien velvoitteiden toteuttamiseksi yhtenäistää ja tehostaa tietojen keruussa, käsittelyssä, käytössä, luovuttamisessa ja säilyttämisessä sovellettavia periaatteita ja menettelytapoja, edistää hyvän tilastotavan noudattamista valtion tilastotoimessa sekä varmistaa, että niiden oikeudet toteutuvat, jotka luovuttavat tietoja tilastointia varten tai joita tiedot koskevat. Lain tarkoituksena on myös edistää tilastotarkoituksia varten kerättyjen tietojen käyttöä tieteellisissä tutkimuksissa ja yhteiskuntaoloja koskevissa tilastollisissa selvityksissä.

Tietojen antaminen tilastojen laatimista varten on tiedonantajille vapaaehtoista, jollei tiedonantovelvollisuudesta ole laissa säädetty. Hankittaessa tietoja tilastojen laatimista varten tulee ensi sijassa käyttää hyväksi julkishallinnon tehtävien hoitamisessa kertyneitä sekä elinkeinon- ja ammatinharjoittajien, yhteisöjen ja säätiöiden tavanomaisen toiminnan seurauksena syntyneitä tietoja.

Tilastoja laativan viranomaisen on huolehdittava siitä, että tiedonantajilta pyydetään vain tilastojen laatimisen kannalta välttämättömät tiedot. Tiedot tulee kerätä ja tallettaa ilman tunnistetietoja aina, kun se tilastojen laatimisen kannalta on mahdollista. Tunnistetietoja voidaan kerätä ja tallettaa ainoastaan silloin, kun se on välttämätöntä tietoaineistojen yhdistämiseksi tai kun se on muutoin välttämätöntä yhteiskuntaolojen kehityspiirteitä kuvaavien luotettavien ja vertailukelpoisten tilastojen tuottamiseksi.

Tilastotarkoituksia varten kerättyjä tietoja yhdistettäessä, säilytettäessä, hävitettäessä ja muutoin käsiteltäessä on huolehdittava siitä, ettei kenenkään yksityiselämän tai henkilötietojen suoja taikka liike- tai ammattisalaisuus

vaarannu. Tietoja on käsiteltävä hyvää tilastotapaa noudattaen ja tilastoalalla yleensä sovellettavien kansainvälisten suositusten ja menettelytapojen mukaisesti. Tilastoja laativan viranomaisen on huolehdittava siitä, että tiedot on tilastotuotannon kaikissa vaiheissa asianmukaisesti suojattu siten kuin erikseen säädetään.

Tilastoviranomainen voi luovuttaa tilastotarkoituksiin keräämiään salassa pidettäviä tietoja:

1. Tieteellistä tutkimusta ja yhteiskuntaoloja koskevaa tilastollista selvitystä varten.

2. Toiselle tilastoviranomaiselle sen toimialaan kuuluvan tilaston kehittämistä, tuottamista ja laadunparannusta varten.

3. Muulle Euroopan tilastojärjestelmään kuuluvalle viranomaiselle sen vastuulla olevan Euroopan tilaston kehittämistä, tuottamista ja laadunparannusta varten.

4. Suomen Pankille sen vastuulla olevan Euroopan tilaston kehittämistä, tuottamista ja laadunparannusta varten.

5. Toiselle tilastoviranomaiselle tieteelliseen tutkimukseen ja yhteiskuntaoloja koskevaan tilastolliseen selvitykseen käytettävän tutkimusaineiston teknistä muodostamista varten.

8.5
EU:n tietosuoja-asetus

Tietosuoja-asetuksen tarkoituksena on ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta voidaan vastata teknologian kehitykseen ja globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin. Asetuksen tarkoituksena on myös tukea digitaalitalouden kehitystä sisämarkkinoiden alueella yhdenmukaistamalla jäsenvaltioiden tietosuojaa koskevat säännökset sekä rakentamalla luottamusta. Henkilötietojen asianmukainen käsittely vahvistaa rekisteröidyn oikeuksia sekä lisää avoimuutta ja läpinäkyvyyttä. Keskeistä on muun muassa:

* Henkilötietojen käsittelyn lainmukaisuuden painottaminen.

* Kerättävien henkilötietojen minimointi ja niiden virheettömyys.

* Avoimen informoinnin lisääminen.

(Tietosuojavaltuutetun toimisto, 2017)

Tietosuoja-asetuksen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. Asetuksen velvoitteiden noudattamista tuetaan tehokkaalla täytäntöönpanolla: asetuksessa on säädetty henkilötietolakia tiukemmat seuraamukset asetuksen vastaisesta henkilötietojen käsittelystä. Valvontaviranomainen voi esimerkiksi määrätä henkilötietojen käsittelyyn liittyviä korjaavia toimenpiteitä ja hallinnollisia sakkoja. (Ibid.)

Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia henkilötietoja käsitteleviä organisaatioita, niin rekisterinpitäjiä kuin henkilötietojen käsittelijöitä. Asetuksen soveltamisalaa rajaavat sen aineellista ja alueellista soveltamisalaa koskevat säännökset. Sitä sovelletaan tietyissä asetuksessa määritellyissä tilanteissa myös EU:n ulkopuolelle sijoittautuneisiin organisaatioihin. Asetusta sovelletaan niin yksityisellä kuin julkisella sektorilla riippumatta esimerkiksi henkilötietojen käsittelyn laajuudesta, käsiteltävien henkilötietojen luonteesta tai käytetystä teknologiasta. (Ibid.)

Tietosuoja-asetusta sovelletaan automaattiseen henkilötietojen käsittelyyn sekä henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat rekisterin osan. Asetuksessa hen-

kilötiedon käsite on määritelty vastaavalla tavalla kuin henkilötietolaissa. Asetuksen mukainen henkilötiedon määritelmä on henkilötietolakia yksityiskohtaisempi ja se sisältää konkreettisia esimerkkejä henkilötiedoiksi määriteltävistä tiedoista. (Ibid.)

Viimeaikaisia GDPR-perusteisia ratkaisuja Euroopassa (Sortti, 2019):

* Iso-Britannian viranomainen antoi kyytipalvelu Uberille 385 000 punnan sakon siitä, ettei se onnistunut suojaamaan asiakkaiden tietoja kyberhyökkäyksen aikana.

* Ruotsissa tietosuojavaltuutetun tarkastuksen kohteena oli ensivaiheessa 66 eri organisaatiota joista 57:lle annettiin huomautus ja kahdelle varoitus (tutkittujen yritysten joukossa mukana mm. Tele2, Telia, Resurs Bank, eri viranomaisia, liikenneyhtiöitä, vakuutusyhtiöitä).

* Saksassa viranomainen antoi 20.000 euron suuruisen sakon sosiaalisen median palveluja tarjoavalle yritykselle, joka ei ollut asianmukaisesti suojannut käyttäjien salasanoja (salasanat olivat tallessa tavallisena tekstinä, niitä ei oltu pseudonymisoitu tai muutoin asianmukaisesti suojattu).

* Portugalissa paikallinen tietosuojaviranomainen (CNDP) antoi GDPR:n nojalla sairaalalle 400 000 euron suuruisen sakon sen vuoksi, että sairaalan järjestelmästä oli pääsy potilastietoihin tekaistuilla profiililla. Vaikka sairaalassa oli noin 300 lääkäriä, ”lääkäriprofiileita” oli käytössä lähes 1000.

8.6 Sosiaali- ja terveydenhuollon asiakas- ja potilastiedon toissijaista käyttöä koskeva lainsäädäntö

Hallituksen esityksessä (159/2017 vp.) ehdotetaan säädettäväksi uusi laki sosiaali- ja terveystietojen toissijaisesta käytöstä. Lisäksi esityksessä ehdotetaan muutettaviksi Terveyden ja hyvinvoinnin laitoksesta (THL) annettua lakia, potilaan asemasta ja oikeuksista annettua lakia, sosiaalihuollon asiakkaan asemasta ja oikeuksista annettua lakia, sähköisestä lääkemääräyksestä annettua lakia, lääkelakia, sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettua lakia, tartuntatautilakia ja kuolemansyyn selvittämisestä annettua lakia sekä kumottavaksi terveydenhuollon valtakunnallisista henkilörekistereistä annettu laki ja sosiaali- ja terveysalan tutkimus- ja kehittämiskeskuksen tilastotoimesta annettu laki. Ehdotetuilla laeilla saatetaan tämän lainsäädäntöalueen säännökset vastaamaan 25.5.2018 alkaen sovellettavana olevaa EU:n yleisen tietosuoja-asetuksen vaatimuksia. (HE, 2017)

Eduskunta hyväksyi ensimmäisessä käsittelyssä 13.3.2019 em. hallituksen esityksen laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä sekä eräiksi siihen liittyviksi laeiksi. Uuden lain tavoitteena on mahdollistaa sosiaali- ja terveydenhuollon toiminnassa sekä sosiaali- ja terveysalan ohjaus-, valvonta-, tutkimus- ja tilastotarkoituksessa tallennettujen henkilötietojen tehokas ja tietoturvallinen käsittely sekä niiden yhdistäminen Kansaneläkelaitoksen, Väestörekisterikeskuksen, Tilastokeskuksen ja Eläketurvakeskuksen henkilötietoihin. (Ibid.) Laki astuu voimaan 1.4.2019.

Lain tarkoituksena on luoda ajanmukaiset ja yhdenmukaiset edellytykset sosiaali- ja terveydenhuollon palvelutoiminnassa syntyvien henkilötasoisten asiakastietojen sekä muiden terveyteen ja hyvinvointiin liittyvien henkilötietojen käytölle tilastointiin, tutkimukseen, kehittämis- ja innovaatiotoimintaan, opetukseen, tietojohtamiseen, viranomaisohjaukseen ja -valvontaan sekä viranomaisten suunnittelu- ja

selvitystehtäviin. Lailla yhtenäistetään sosiaali- ja terveydenhuollon asiakastietojen sekä muiden terveyteen ja hyvinvointiin liittyvien henkilötietojen käyttöä ohjaava lainsäädäntökokonaisuus. Lain mukaan tällaisten tietojen käyttöluvat myöntäisi jatkossa keskitetysti Sosiaali- ja terveysalan käyttölupaviranomainen, lupakäsittelyä ja tietopyyntöjen käsittelyä varten luotaisiin keskitetty tietopyyntöjen hallintajärjestelmä ja luvan nojalla luovutettaville tiedoille luotaisiin tietoturvalliset käyttöympäristöt ja käyttöyhteydet. Lain keskeisenä tavoitteena on sujuvoittaa ja nopeuttaa olennaisesti tietojen käyttölupiin liittyvää käsittelyä ja keventää siihen liittyvää, rinnakkaisista lupamenettelyistä aiheutuvaa hallinnollista taakkaa. Laissa on otettu huomioon sosiaali- ja terveydenhuollon integraatio sekä digitalisaation voimakas vaikutus asiakastietojen sähköiseen käsittelyyn ja sen edellyttämiin tietosuoja- ja tietoturvavaatimuksiin. Samanaikaisesti tekninen kehitys on luonut uudenlaiset mahdollisuudet käsitellä arkaluonteisia asiakastietoja ja yhdistää niitä sallituissa käyttötarkoituksissa muihin henkilötietoihin tavalla, joka aiempaa paremmin turvaa asiakkaiden henkilötietojen- ja luottamuksen suojan. (Ibid.)

Lain tarkoituksena on luoda ajanmukaiset ja yhdenmukaiset edellytykset sosiaali- ja terveydenhuollon palvelutoiminnassa syntyvien henkilötasoisten asiakastietojen sekä muiden terveyteen ja hyvinvointiin liittyvien henkilötietojen käytölle tilastointiin, tutkimukseen, kehittämis- ja innovaatiotoimintaan, opetukseen, tietojohtamiseen, viranomaisohjaukseen ja -valvontaan sekä viranomaisten suunnitteluja selvitystehtäviin. (Ibid.)

Lainsäädännön muutosten myötä voidaan olennaisesti tehostaa Suomen poikkeuksellisen kattavien ja laadukkaiden tietovarantojen käyttöä, joita ei ole tähän mennessä hyödynnetty riittävästi. Tavoitteiden toteuttamiseksi on lisäksi uudistettava merkittävässä määrin tietojen toissijaista käyttöä koskevia käyttölupaprosesseja sekä kehitettävä tietoturvalliset, yhteen toimivat rekisteriviranomaisten tietojärjestelmät. Luovutettujen tietojen asianmukaisen käsittelyn varmistamiseksi tarvitaan myös tietoturvalliset sähköiset käyttöyhteydet sekä käyttöympäristöt, jotka turvaavat arkaluonteistenkin henkilötietojen tietosuojan. (Ibid.)

LUKU 9

Käyttäjien kokemuksia terveystietojen yksityisyydestä

9.1 Tutkimuksen lähtökohtia ja perusteita

Tässä luvussa esitellään tutkimustuloksia kuluttajien kokemuksista hyvinvointiin liittyvien kuluttajalaitteiden (tässä tutkimuksessa aktiivisuusranneke) yksityisyyteen liittyvistä riskeistä ja huolenaiheista. (Lehto Miikael, 2016; Lehto Miikael, Lehto Martti, 2017)

Aktiivisuusrannekkeet ovat yleistyneet ja ne mahdollistavat tietojen keräämisen henkilön fyysisestä aktiivisuudesta ja terveydestä. Henkilön terveystiedot ovat perinteisesti olleet vain terveydenhuollon tietokannoissa, mutta nykyään terveystietoja tallennetaan moniin palveluihin. Tämä muutos on tuonut uusia teknologian hyödyntämismahdollisuuksia terveyden ja hyvinvoinnin alueella, mutta samalla on herännyt kysymyksiä henkilöiden yksityisyyteen liittyen.

Tutkimuksessa selvitettiin käyttäjien subjektiivisia kokemuksia aktiivisuusrannekkeilla kerätyn terveystiedon yksityisyydestä ja arkaluontoisuudesta. Tutkimuksessa selvitettiin myös tutkittavien ajatuksia terveystiedon yksityisyydestä yleisesti ja heidän halukkuudestaan jakaa heistä kerättyjä tietoja eri osapuolille.

Tutkimuksen empiirinen aineisto kerättiin käyttämällä laadullista tutkimusmenetelmää ja työkaluna teemahaastatteluita. Kuluttajalaitteiden yksityisyyden vaikutusten ja niihin liittyvien tietosuojaongelmien ymmärtäminen on tunnistettu alueeksi, joka tarvitsee lisätutkimuksia (Motti & Caine, 2015). Privacy calculus -mallia käytettiin tutkimuksen teoreettisena viitekehyksenä, joka myös ohjasi tuloksien analysointia ja luokittelua.

Aiemmat tutkimukset ovat osoittaneet, että käyttäjät jakavat paljon enemmän terveys- ja henkilötietojaan palveluntarjoajien kanssa kuin he itseasiassa ymmärtävät (Patterson, 2013). Käytettävissä olevien laitteiden ja niihin liittyvien palvelujen ongelma on se, että yksilöt eivät ymmärrä tarkasti, miten heidän tietojaan tallennetaan ja käsitellään.

Käytettävissä olevien laitteiden tutkimuksessa on havaittu, että käyttäjät ovat huolissaan sijaintitietojensa keräämisestä GPS:n kautta ja huolissaan tietojen paljastumiseen liittyvistä riskeistä (Patterson, 2013). Samaan aikaan tutkimukset ovat osoittaneet, että yksilöt eivät ole huolissaan henkilökohtaisilla kannettavilla laitteilla kerättyjen tietojen paljastumisesta (Motti & Caine, 2015).

Tutkimus tehtiin haastattelemalla henkilöitä, joilla oli aktiivisuusranneke tutkimushetkellä käytössä. Haastattelussa käytettiin teemoja, jotka ovat keskeisiä Privacy calculus-teoriassa. Haastatteluissa luotiin sellaiset olosuhteet, jossa yksilö voi ilmaista todellisia mielipiteitään suhteessa tiedon yksityisyyteen ja sensitiivisyyteen.

Tutkimukseen osallistuneiden käyttämät laitteet keräävät erilaisia tietoja terveyteen ja yleiseen toiminnallisuuteen. Kerätyt tiedot koostuvat askelmääristä, etäisyydestä, liikkumisnopeudesta, sydämensykkeestä, sijainnista, unes-

ta, ajasta, aktiivisuustasosta, poltetuista kaloreista ja maksimaalisesta hapenkulutuksesta. Useimmat osallistujat käyttävät laitteitaan koko päivän, mutta ottavat sen pois yön aikana, koska unen seurantaan sen ei havaittu olevan hyödyllinen. Laitteita käytetään usein rannekelloina ja niitä käytetään aktiivisesti harjoitusten tai muiden aktiviteettien aikana. Laitteet keräävät passiivisesti tietoja ja laskevat aktiivisuustasot, jotka näkyvät käyttäjälle numeroina tai prosentteina.

Käyttäjät arvostivat laitteita ja pitivät hyödyllisenä saada palautetta tai tietoa harjoitusten aikana ja monille tämä oli tärkein syy laitteen ostamiseen. Pystyäkseen näkemään sykkeensä (HR) harjoituksen aikana oli tärkein ominaisuus ja syy, miksi laitteet ostettiin. Kädessä pidettäviä pidettiin parempina kuin niitä, joissa käyttöön tarvittiin rintahihnaa. Yksikään tutkimukseen osallistujista ei ollut ostanut laitetta motivoidakseen itseään liikkumaan enemmän. Laitteen antamat tiedot auttoivat jotakin tekemään pidempiä juoksumatkoja tai harjoituksia, mutta monille laite paransi harjoituksen laatua paljon enemmän kuin sen määrä. Harjoituksista saatu tieto oli eniten mainittu etu laitteiden käytössä.

Tutkimukseen osallistuja eivät käyttäneet laitteiden antamia tietoja oman terveydentilansa arvioimiseen vaan kuntotasonsa arvioimiseen. Monet esittivät huolta siitä, että laitteiden keräämät tiedot eivät ole riittävän tarkkoja tai relevantteja, jotta niistä voisi arvioida omaa terveyttään. Osallistujilta kysyttiin, haluaisivatko he kerätä lisää tietoa terveydestään, kuten happisaturaatiosta, verenpaineesta tai muusta terveydentilasta, joko ranteeseen asetetun laitteen tai jonkin muun lääkinnällisen laitteen kanssa kotona. Monet eivät pitäneet näitä tietoja itselleen suoranaisesti hyödyllisinä, mutta niitä pidettiin kiinnostavina. Mahdollinen pitkäaikainen sairaus muutti heidän mielipidettään, jolloin he olivat halukkaampia ja kiinnostuneempia keräämään näitä tietoja myös itse.

9.2 Halukkuus jakaa hyvinvointitietoja

Tutkimukseen osallistuneille kysyttiin heidän halukkuutensa jakaa tietoja, joita he ovat keränneet laitteillaan eri tarkoituksiin. Taulukossa 6 esitetään havainnot halukkuudesta jakaa näitä tietoja eri kohteille.

Sosiaalinen media

Suurin osa ei nähnyt minkäänlaista hyötyä jakaa tietoa omista harjoittelutuloksistaan sosiaalisessa mediassa (ks. taulukko 6). He kyllä keskustelevat terveydestään ja hyvinvoinnistaan perheenjäsenten ja lähimpien ystävien kanssa, mutta säännöllistä keskustelua sosiaalisessa mediassa ei pidetty tarpeellisena. Lisäksi huolta aiheutti sosiaalisen median luonne ja sen turvallisuus. Osaa huolestutti näiden tietojen jakamisen sosiaalinen hyväksyttävyys. Epätietoisuus tietojen toissijaisesta käytöstä

Halukkuus jakaa tietoja	Kyllä %	Ei %
Sosiaalinen media	10	90
Lääkäri	100	0
Lääketieteellinen tutkimus	100	0
Työterveyshuolto	80	20
Laitteiden valmistajat	70	30

TAULUKKO 6: Halukkuus jakaa oman aktiivisuusrannekkeen tietoja.

esitettiin myös syynä haluttomuuteen jakaa tietoja, koska niiden käytöstä ei ollut varmuutta.

Lääkäri

Yksikään tutkimukseen osallistujista ei ollut jakanut tietojaan lääkäreille, mutta ne kaikki olivat valmiita tekemään niin oikeissa olosuhteissa (ks. taulukko 6 edellisellä sivulla). He eivät kuitenkaan olleet valmiita suoralta kädeltä tarjoamaan tietojaan, vaan tekisivät niin lääkärin pyytäessä. Heidän mielestään tämä olisi hyvä tapa toimia vuorovaikutuksessa terveydenhuollon ammattilaisten kanssa. Osallistuneita arvelutti tietojen käytettävyys, mutta näkivät niillä olevan ehkä käyttöä myöhemmässä vaiheessa, kun tietoja on kerätty pidemmän aikaa ja henkilön terveydentilassa tapahtuu muutoksia.

Osallistujien mielestä, sairaana oleva henkilö voisi hyötyä tietojen keräämisestä näiden laitteiden tai muiden lääkinnällisten laitteiden avulla ja tietojen luovuttamisesta hoitavan lääkärin käyttöön. Osallistujat ilmaisivat halukkuutensa kerätä lisää terveystietoja itsestään ja toimittaa niitä lääkärille, jos heidän terveydenhoitonsa hyötyisi lisätiedoista. Tämäntyyppinen lääkärille siirrettävä tieto saattaisi heidän mielestään vähentää lääkärikäyntien määrää. Tämä todettiin olevan hyödyllinen erityisesti niille henkilöille, joiden sairaus vaatii mittauksia usein.

Terveyskeskuksessa tai sairaalassa tulisi olla henkilö, joka aktiivisesti tarkastelisi näitä itse- ja omahoidon kautta tulevia tietoja, jotta palaute tietoja lähettäneelle olisi saatavissa välittömästä ja mahdolliset mittausvirheet huomattaisiin. Erityisesti vanhuksilla mittausvirheiden tekemisen riskiä pidettiin suurena. Väärät mittausarvot voivat johtaa virheelliseen diagnoosiin, mikä voi pahimmillaan johtaa potilaan tilan huononemiseen.

Mahdollista tekoälyyn perustuvan ohjelmistorobotin käyttöä näiden kotoa tulevien mittaustietojen käsittelyyn pidettiin ongelmallisena. Kuitenkin vain harva osallistuja ilmaisi huolensa sosiaalisen vuorovaikutuksen puutteesta lääkärin kanssa, jos terveydenhuoltomalli siirtyisi enemmän itsemittauksiin ja vuorovaikutukseen verkkopalvelujen kautta.

Lääketieteellinen tutkimus

Tutkimuksessa tarkasteltiin halukkuutta antaa tietoja lääketieteelliseen tutkimukseen, joita he ovat keränneet kannettavalla laitteellaan. Osallistujat saivat esimerkkinä tietoa sydän- ja verisuonitautien tutkimuksesta ja siitä, miten tietoa voitaisiin käyttää uusien hoitojen löytämiseen. Kaikki olivat hyvin halukkaita toimittamaan tietojaan käytettäväksi tällä tavalla (ks. taulukko 6).

Tietosuojariski ja mahdollisuus, etteivät tiedot pysyisi yksityisinä ja luottamuksellisina herättivät huolta osallistujien keskuudessa. Harva osallistujista oli halukas antamaan tietojaan, jos pyynnön esitti organisaatio, virkamies tai alan yritys, mutta olisivat epäröimättä antaneet tietonsa yksittäiselle tutkijalle. Ts. yksittäinen tutkija nähtiin luotettavammaksi kuin virallinen toimija tai yritys. Tietoja ei haluttu päätyvän käytettäväksi liiketoiminnallisiin tarkoituksiin, tilanteessa, jossa tutkimusta tekisi jokin SOTE-alan yritys. Yleensä haluttiin, että henkilökohtaisia tietoja tarkasteltaisiin anonyymeinä, eikä henkilökohtaisella tasolla.

Osalle osallistujista henkilökohtaisten tietojen joutuminen liikeyritysten käyttöön arvelutti samalla, kun oltiin valmiit ottamaan riskejä tiedonjakamisessa auttaakseen muita ihmisiä. Tärkeäksi koettiin myös se, että tutkimukseen osallistuva henkilö olisi osa laajaa tutkimusaineistoa, eikä vain hänen yksittäisiä tietojaan tarkasteltaisi. Suuressa tietojoukossa yksilöt eivät erottuisi.

Työterveyshuolto

Tutkimuksessa osallistujilta kysyttiin, olisivatko he halukkaita käyttämään työnantajansa tarjoamaa aktiivisuusseurantalaitetta, jos laitteen tiedot siirretään työterveyshuollon tarjoajalle. Useimmat osallistujat olivat valmiita käyttämään tällaista aktiivisuusseurantaan tai ainakin harkitsemaan sitä joissakin olosuhteissa (ks. taulukko 6), mutta he ilmaisivat myös monia huolenaiheita ja negatiivisia näkökohtia, joita kyseinen toimintamalli toisi.

Yksilöiden kannalta tärkeä tekijä oli se, että tiedot lähetetään vain työterveyshuollon tarjoajalle, koska ne jo nykyisellään käsittelevät työntekijöiden terveystietoja. Osallistujat ilmaisivat luottamuksensa terveyspalvelujen tarjoajiin ja uskoivat, etteivät ne tietoisesti paljastaisi potilastietoja työnantajalle. Epävarmojen keskeisin huoli oli juuri se, että tällaiset tiedot päätyisivät työnantajan käyttöön ja siksi he eivät välttämättä käyttäisi tarjottua laitetta. Tällaiset laitteet saattaisivat synnyttää työpaikalla kaksi ryhmää, joista fyysisesti aktiivisia työnantaja suosisi tavalla tai toisella ja syrjisi huonosti liikkuvia. Tämä voisi näkyä erityisesti saneeraus- ja irtisanomistilanteissa. Kokonaisuutena em. kuvattuja riskejä pidettiin erittäin epätodennäköisinä ja järjestelmän etuja pidettiin suurempina kuin mahdollisia riskejä. Osallistujat näkivät arvon siinä, että työnantajan tarjoamat laitteet voisivat motivoida yksilöitä olemaan liikunnallisempia.

Laitteiden valmistajat

Tutkimuksen mukaan halukkuus jakaa yksilön keräämiä terveystietoja laitevalmistajille jakaa mielipiteitä. Osa laitevalmistajista kerää jo nyt tietoja, mutta tilanteessa, jossa henkilöt itse voisivat valita, suurin osa oli halukas niin tekemään (ks. taulukko 6). Useimmat olivat halukkaita saamaan yritykseltä vastineena tiedon jakamisesta parempia palveluita ja yritykselle annettuja tietoja tulisi käyttää laitteiden kehittämiseen. Jotkut osallistujat olettivat, että juuri näin yritykset todennäköisesti tekevät nyt, vaikka he eivät ole tietoisia siitä.

Kolmasosan mielestä he eivät todennäköisesti anna tietojaan laitevalmistajan käyttöön tai antavat vain pakolliset tiedot palveluun ja laitteen käyttöön liittyvän rekisteröinnin yhteydessä He eivät haluan antaa laitevalmistajalle oikeutta käyttää asiakkaan tietoja muihin tarkoituksiin. Keskeisin huolenaihe oli, että laitevalmistajalle annetut tiedot päätyisivät tietoisesti ja tahattomasti kolmannelle osapuolelle. Osallistujat edellyttivät, että suhteessa laitevalmistajiin tarvitaan parempaa läpinäkyvyyttä tällaiselle tietojen käytölle.

9.3 Tietojen sensitiivisyys

Haastattelun aikana osallistujia pyydettiin miettimään, minkä tyyppistä tietoa heidän kannettava laitteensa kerää, ja arvioimaan, miten henkilökohtainen, yksityinen tai herkkä kerätty tieto on. Osallistujat kuvailivat laitteidensa keräämiä tietoja vähemmän sensitiivisiksi, ei-salaisiksi, vähemmän luottamuksellisiksi ja yleensäkin melko yleisiksi. Näillä laitteilla kerätyillä tiedoilla ei nähty vahvaa yhteyttä yksilöön, mikäli näihin numeerisiin tietoihin ei yhdistetä henkilötunnisteita. Yleisesti ottaen laitteiden keräämää tietoa ei pidetty kovin sensitiivisenä, mutta joitakin huolenaiheita kuitenkin esitettiin. Vaikka henkilöön sitomattomia tietoja pidettiin hyödyttöminä, esimerkiksi rikollisille, henkilöt eivät kuitenkaan halunneet tietojen joutuvan ulkopuolisten käsiin tai niitä leviteltäisiin julkisesti.

Vertaamalla henkilöiden henkilökohtaisten aktiivisuusrannekkeiden ja muiden laitteiden

Henkilökohtaisten laitteiden tiedot	Potilastietojärjestelmän tiedot
Yleisiä	Yksityiskohtaisia
Numeerisia	Tekstimuotoisia
Ei henkilökohtaisia	Identifioitavissa
Liikuntatapoja kuvaavia	Terveydentilaa kuvaavia
Ei-yksityisiä	Yksityisiä
Ei-sensitiivisiä	Sensitiivisiä

TAULUKKO 7: Henkilökohtaisten laitteiden tiedot suhteessa potilastietojärjestelmän tietoihin.

keräämää tietoa sairaalan potilastietojärjestelmissä (PTJ) oleviin sähköisiin potilastietoihin saatiin haastateltavilta tutkimuksessa oheinen taulukko 7. Henkilöt näkivät eri tietojärjestelmiin kerättyjen tietojen välillä merkittäviä eroja suhteessa niiden sensitiivisyyteen ja luottamuksellisuuteen.

Potilastietojärjestelmän tiedot sisältävät tarkempia ja yksilöidympiä tietoja potilaan terveydentilasta ja mahdollisista sairauksista. Nämä tiedot ovat sairauteen liittyviä historiatietoja, kun taas aktiivisuuslaitteista tai muista kotona olevista mittauslaitteista tuleva tieto on lähes reaaliaikaista, ja siten osin kuvaavat paremmin henkilön nykyistä terveydentilaa tai sairautta. Tässä suhteen nämä henkilökohtaiset laitteet tuottavat uutta tietoa ja parantavat henkilön terveystilannekuvaa.

Henkilöt suhtautuivat eri tavoin erityyppisiin tietoihin. Osaa numeerisista tiedoista ei pidetty kovin sensitiivisinä mutta esimerkiksi veriryhmä- ja muita laboratoriotuloksia pidettiin sellaisina. Kaikkein sensitiivisimpinä ja yksityisyyttä lähellä olevia tietoja olivat potilaskertomukset (epikriisi) ja muut sanalliseen muotoon tehty aineisto potilaan ja lääkärin välisestä keskustelusta. Henkilöiden mielestä heidän terveystiedoillaan ei ole samaa taloudellista hyödynnettävyyttä kuin heidän talouteensa liittyvillä tiedoilla (tilitiedot, tulot, verot, lainat). Henkilön terveys- ja lääketieteelliset tiedot ovat sensitiivisiä ja kertovat enemmän henkilön yksityisyydestä kuin taloudelliset tiedot. Terveystiedot paljastavat enemmän henkilön tilasta erityisesti silloin, jos hänellä on pitkäaikaisia tai vaikeita sairauksia ja erityislääkitystä, jotka paljastuessaan voivat vaikuttaa henkilön sosiaalisiin suhteisiin tai suhtautumiseen työpaikalla.

9.4 Tietosuojaongelmat

Tutkimuksessa nousi esille osallistujien huoli yksityisyydestä käsiteltäessä terveystietoja eri laitteilla sekä itse laitteisiin liittyvistä riskeistä. Yleensä osallistujat pitivät omia tietojaan turvallisesti suojattuna ja epäilivät, oliko kukaan yleensäkään kiinnostunut heidän tiedoistaan. Pääsyä tietoihin oman laitteen kautta pidettiin mahdollisena riskinä, mutta sitä vähennettiin käyttämällä mm. sormenjälkitunnistusta laitteen lukituksen avaamiseen.

Tutkimuksessa tuotiin esille kolme organisaatiota, jotka saattaisivat toimia väärin, jos heillä olisi käytössä henkilökohtaisia terveystietoja. Pankkeja ja vakuutusyhtiöitä pidettiin organisaatioina, jotka voisivat hyödyntää lääketieteellisiä tietoja lainaa päätettäessä tai määritettäessä vakuutusmaksuja, vakuutusten kattavuutta tai vakuutuskorvauksia.

Kolmannen ryhmän muodostivat työnantajat, jotka voisivat käyttää terveystietoja palkatessa

tai irtisanoessaan henkilöstöä tai päättäessään kenen uraa yrityksessä edistetään.

Osallistujien keskuudessa herätti myös huolenaiheita se, että olemme yksilöinä ja yhteiskuntana niin riippuvaisia sähköisistä järjestelmistä SOTE-alalla, pankkitoiminnassa ja yleensä maksuliikenteessä, koska paperisia tallenteita tai analogisia toimintamalleja ei enää ole käytössä. Huolimatta edellä kuvatuista riskeistä, tietojen mahdollisista värinkäytöksistä ja hakkeroinneista tietojärjestelmiin, osallistujien piirissä vallitsi laaja yksimielisyys siitä, että uudet digitaaliset järjestelmät tarjoavat yksityisyyden suojaan liittyviä riskejä enemmän käytännön etuja.

Tutkimuksessa selvitettiin sitä, miten osallistujat kokisivat tilanteen, jossa yritykseen, joista heillä on aktiivisuusranneke, kohdistuisi tietomurto. Yksikään osallistujista ei sanonut, että he lopettaisivat laitteen käyttämisen, vaikka heidän tietojaan olisi varastettu yrityksen tietojärjestelmistä, mutta osan tuleviin ostopäätöksiin em. kuvattu tietomurto vaikuttaisi. He näkivät kyberturvallisuustapaukset ikään kuin väistämättöminä nykyisessä digitaalisessa toimintaympäristössä, vaikka yritykset toimisivatkin mahdollisimman turvallisesti ja siksi riskejä pidettiin hyväksyttävinä. He kuitenkin odottavat, että yritys korjaa ongelmansa välttääkseen uusia ongelmia, mutta erityisen oli tärkeää, että yritys ei tarkoituksellisesti tai tahallisesti väärinkäytä asiakastietoja tai myy niitä ulkopuolisille.

Yrityksen epäeettinen käyttäytyminen tai yritys piilottaa turvallisuuspoikkeamia todettiin vaikuttavan merkittävästi, kuinka ihmiset suhtautuvat jatkossa yritykseen.

Osallistujien mielestä heidän olisi rajoitettava jokapäiväistä elämäänsä monin tavoin, jos he eivät hyväksyisi näitä turvallisuusriskejä. Esimerkiksi tietomurto yhteen pankkiin ei vaikuttaisi ihmisten suhtautumiseen pankkisektoriin yleisesti. Sama logiikka soveltuu aktiivisuusrannekkeiden valmistajiin ja terveystietojen tallentamiseen. Tietomurtotapausten nähtiin vaikuttavan suuriin ihmisryhmiin kerrallaan, joten yksittäinen henkilö ei tällaisissa tapauksissa tunne henkilökohtaisesti tilannetta niin uhkaavana tai vaarallisena, jonka vuoksi käyttäytymistä tai toimintatapoja pitäisi muuttaa.

Monissa kannettavissa laitteissa on GPS-valmiuksia, jotka ovat joko sisäänrakennettuja laitteeseen tai ne hyödyntävät käyttäjän älypuhelimen GPS:ää. Tämä toiminto herätti huolta osalle osallistujista, koska he ajattelivat, että näin heitä voitaisiin seurata tai paikantaa. Uhkana pidettiin mahdollisuutta, että heidän sijaintitietojaan voitaisiin kerätä asianomaisen tietämättä ja salaa ja heidän liikkeitänsä voitaisiin seurata. Tätä uhkaa ei kuitenkaan pidetty hyvin todennäköisenä. Henkilön sijaititiedon joutuminen rikollisten käsiin voisi antaa näille esimerkiksi mahdollisuuden päätellä, milloin asunto olisi tyhjä ja toteuttaa tällöin asuntomurto. Tätäkään skenaariota ei pidetty kovin todennäköisenä riskinä. Yleensä ihmiset ajattelevat, ettei kukaan ole kiinnostunut, missä he käyvät lenkillä. Paikka- ja sijaintitiedoista tulisi merkittäviä, mikäli henkilö olisi merkittävässä asemassa politiikassa, liike-elämässä tai julkisella sektorilla.

Tutkimuksessa ilmeni yleinen luottamus yrityksiä ja organisaatiota kohtaan. Niiden ajateltiin tekevän hyvää työtä ihmisten tietojen suojaamiseksi. Osa tutkimukseen osallistuneista koki epävarmuutta siitä, missä olisi turvallista tallentaa tietojaan, kuinka kontrolloida omia tietojaan ja tietää kuinka niitä mahdollisesti käytetään eri tarkoituksiin. Harvat osallistujat sanoivat rajoittavansa online-palvelujen rekisteröintiprosessin aikana antamiensa tietojen

määrää ja sisältöä. Esille nousi huoli siitä, että useimmat palvelut keräävät tietoja käyttäjästä ilman, että ne olisivat nimenomaisesti ilmoittaneet keräävänsä tietoja.

Ilmaisia palveluita ja sovelluksia, jotka keräävät käyttäjätietoja mainostajille, pidettiin ärsyttävänä, mutta ei uhkana yksityisyyden suojalle. Yleisesti todettiin, että monilla henkilöillä ei ole suuria yksityisyyttä koskevia huolenaiheita, koska he eivät ymmärrä, mikä on kybermaailmassa mahdollista tai mitä heidän tiedoilleen voi tapahtua, jos ne varastetaan. Kysymys on ihmisten tiedon ja ymmärryksen puutteesta.

Ihmiset tuntevat kyynisyyttä kolmansia osapuolia kohtaan, joille heidän käyttäjätietojaan välitetään, vaikka se tapahtuisikin palvelun käyttösopimuksen mukaisesti. Heillä oli huoli siitä, miten ja mihin heidän tietojaan käytettiin. Verkkopalveluiden käyttäjinä he jättävät jälkeensä kaikkialla, missä he käyvät verkossa (digitaalinen jalanjälki), ja myös tietoja paikoista, joissa he fyysisesti käyvät. Identiteettivarkaudet tunnistettiin, ia niitä pidettiin usein tapahtuvina, mutta nämä huolenaiheet ja riskit eivät vaikuttaneet merkittävästi yksilöiden käyttäytymiseen.

Parhaaksi tavaksi vähentää yksityisyyttä koskevia huolia, oli osallistujien mielestä mahdollisuus omien tietojen kontrollointiin ja avoimuus niiltä, jotka heidän tietojaan käyttävät. Ihmiset arvostavat mahdollisuutta valita, mitä tietoja kuhunkin palveluun tulee antaa ja mitkä ovat todella välttämättömiä tietoja palveluun rekisteröitymisen kannalta. Ihmiset haluavat paremman näkymän palveluihin ja kuinka heidän tietojaan kerätään ja käytetään.

Tällaisten toimintatapamallien puute ei kuitenkaan merkittävästi vaikuta ihmisten käyttäytymiseen ja palveluiden käyttämiseen, mutta näillä menettelytavoilla yritys voi lisätä asiakkaiden luottamusta yritykseen ja parantaa yrityskuvaa.

JOHTOPÄÄTÖKSIÄ

Teknologiamarkkinoiden kasvu vaikuttaa siihen, kuinka yksilöt keräävät ja säilyttävät terveystietojaan. Ennen nykyisiä tekniikoita terveystieto tallennettiin vain lääketieteellisiin tiedostoihin, jotka olivat saatavilla vain terveydenhuollon ammattilaisille. Nyt terveystietoja tallennetaan useisiin eri paikkoihin, mukaan lukien henkilökohtaiset kannettavat laitteet, älypuhelimet, kannettavat tietokoneet ja pilvipalvelut, joita eri organisaatiot tarjoavat. Koska terveystietopalvelut ovat hajautuneet ja yksilöillä on helpompi pääsy tietoihinsa, tämä on tuonut esiin uusia yksityisyyden suojaa koskevia kysymyksiä ja riskejä.

Taulukko 8 seuraavalla sivulla esittää synteesin tutkimuksen keskeisistä havainnoista luettelemalla ne kolmeen osaan, jotka on tunnistettu Privacy calculus -teoriasta.

Tutkimuksen tuloksena ilmeni, että henkilöt eivät pidä aktiivisuusrannekkeiden tietoja yksityisinä tai arkaluontoisina vaan enemmän yleisinä. Toisaalta henkilöiden mielestä heidän lääkäreillänsä olevat terveystietonsa ovat hyvin yksityisiä ja sensitiivisiä. Lääkäreillä olevat tiedot koettiin yksityiskohtaisiksi, koska ne sisältävät henkilökohtaista tietoa sekä numeerisessa että kirjallisessa muodossa. Tutkimuksessa selvisi, että käyttäjät eivät jaa aktiivisuusrannekkeidensa tietoja sosiaalisessa mediassa.

Käyttäjät olivat valmiita antamaan keräämiään tietoja lääkärille, mikäli niistä olisi hyötyä heidän terveydenhoidossaan sekä työterveyshuollon käyttöön. Käyttäjät olivat myös valmiita antamaan tietojaan lääketieteelliseen tutkimukseen sekä antamaan laitevalmistajan käyttää heidän tietojaan tuotteiden ja palveluiden kehittämiseen.

Tulosten perusteella terveydenhuoltopalveluiden tarjoajat ja lääketieteellinen tutkimus voivat hyötyä suuresta määrästä ihmisiä, jotka ovat keränneet tietoja kannettaviin laitteisiinsa. Yksilöiden luovuttamien tietojen käyttö on kuvattava selkeästi ja läpinäkyvästi, jotta yksilöiden yksityisyyttään koskevia huolenaiheita voidaan lieventää. Ihmiset ovat halukkaita keräämään jopa ylimääräisiä terveystietoja, jota niitä voidaan käyttää terveydenhuollossa, mutta hyödyn saamiseksi ja yksityisyyden suojan turvaamiseksi on luotava selkeät, läpinäkyvät ja turvalliset toimintaprosessit.

Ihmisten omia käyttämiään laitteita ei pidetä lääkärin korvikkeena, vaan keinona täydentää nykyisiä terveydenhuoltopalveluja. Siirtyminen enemmän kunkin itsensä tekemiin mittauksiin terveydenhuollossa aiheuttaa yksilöille joitakin huolenaiheita tietojen oikeellisuudesta ja siitä, miten tietoja käytetään diagnosoinnissa.

Tutkimuksen mukaan yksilöillä on yksityisyyttä koskevia huolenaiheita, jotka koskevat terveystietojen paljastumista ulkopuolisille. He tunnistavat terveystietojen mahdolliset riskit, jotka liittyvät tietojen keräämiseen, väärinkäyttöön ja ulkopuolisten pääsyn heidän tietoihinsa. Tietojen keräämistä ja väärinkäyttöä pidetään riskeinä, jotka ovat aina läsnä käytettäessä online-palveluita. Riskien toteutumisen todennäköisyyttä pidetään kuitenkin erittäin alhaisena.

Koska yksilöt eivät ymmärrä, että mahdolliset riskit voisivat aiheuttaa heille merkittävää vahinkoa, nämä huolenaiheet eivät vaikuta merkittävästi tuotteiden ja palvelujen käyttöön. Henkilöt käyttävät edelleen tuotteita, joita he pitävät hyödyllisinä tai saavat hyötyä, mutta

Koetut yksityisyyden riskit ->	Koetut yksityisyyden huolenaiheet ->	Halukkuus tarjota henkilökohtaisia terveystietoja
Tietovarkaus	Tulee seuratuksi tai paikannetuksi	Ei sosiaaliseen mediaan
Tiedon katoaminen	Pankit eivät myönnä lainaa	Lääketieteellistä tutkimusta varten
Tiedon väärinkäyttö	Ei saa työ paikkaa	Terveydenhuollon tarpeisiin
Tiedon joutuminen kolmannelle osapuolelle	Vakuutusyhtiö kieltäytyy korvauksista	Kannettavien laitteiden kehittämiseen
Oikeudeton pääsy tietoihin	Tietoja käytetään markkinointiin	Työterveyshuollon tarpeisiin

TAULUKKO 8: Synteesi tutkimuksen keskeisistä havainnoista.

pyrkivät rajoittamaan luovuttamiensa tietojen määrää. Pääasialliset syyt ottaa kannettavia mittalaitteita käyttöön olivat tietoisuuden lisääminen omasta kuntoharjoittelusta ja mahdollisuus parantaa harjoittelun laatua. Näiden etujen katsottiin olevan suurempia kuin mahdolliset riskit tai yksityisyyden suojaan liittyvät huolenaiheet.

Laitevalmistajien on harkittava, miten ja milloin käyttäjien paikannustietoja kerätään, koska tämä on merkittävä huolenaihe käyttäjillä, mikä voi vaikuttaa näiden palveluiden käyttöön ja käyttöönottoon. Laitevalmistajien tulisi tutkia mahdollisuutta, että laitteiden GPS-toiminnot ovat käytössä vain harjoitusten aikana ja pois käytöstä muina aikoina. Tulosten perusteella yksityisyyden riskit kasvavat, koska laitteiden keräämät tiedot liittyvät terveyteen ja hyvinvointiin. Yritysten tulisi harkita, mitkä tiedot ovat hyödyllisiä ja merkityksellisiä kerättäviksi. Nämä yksityisyyden suojaan liittyvät kysymykset ilmenevät myös silloin, kun käytettävät laitteet on liitetty potilastietojärjestelmiin.

Jatkotutkimuksen yksi lähtökohta olisi haastatella yksilöitä, joilla on ollut kokemuksia identiteettivarkaudesta tai muusta henkilökohtaisten tietojen väärinkäytöstä ja tutkia, onko tällä vaikutusta tietojen sensitiivisyyteen, yksityisyyden suojaan ja kuluttajien käyttäytymiseen.

Tämä tutkimus laajentaa aiempaa tutkimustietoa esittämällä uuden kontekstin, johon Privacy Calculus -teoriaa voidaan hyödyntää. Tutkimuksen tuloksista on käytännön hyötyä, koska aktiivisuusrannekkeiden keräämiä tietoja voidaan tulevaisuudessa hyödyntää terveydenhuollossa ja tutkimuksissa, koska käyttäjät ovat valmiita jakamaan niiden tietoja.

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/

Chew Jonathan. 2016. One in Five Employees Would Sell Their Work Passwords, Fortune Tech, Mar 30, 2016

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

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

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. 2017. Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends

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/

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

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 affec-

ted. 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

HE. 2017. Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveystietojen toissijaisesta käytöstä sekä eräiksi siihen liittyviksi laeiksi. HE 159/2017 vp. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_159+2017.pdf

Health Care Industry. 2017. Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry, June 2017

HealthIT Security. 2016. Cybersecurity Attacks Leading 2016 Data Breach Cause, 19.12.2016

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

HIPAA. 2019, Healthcare Data Breach Statistics, HIPAA Journal. Saatavilla 12.3.2019 https://www.hipaajournal.com/healthcare-data-breach-statistics/

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. o. & 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

Kalli S., Nikanne E., Pitkänen S., Häyrinen E., Harvia P., Varvikko K., Suurnäkki J. 2015. KSSHP ICT Strategia ja kehittämissuunnitelma - lähtökohta ja tavoitteet, 13.4.2015

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

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

Lehto, Martti. 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 Martti. Neittaanmäki P. 2016. Digitalisaatio muuttaa yhteiskunnan ja yksilöiden tapaa toimia. Tiedepolitiikka 1/2016, 56–64

Lehto Miikael. 2016. User Perceptions on the Privacy of Health Information, Jyväskylän yliopisto, Informaatioteknologian tiedekunta, kyberturvallisuuden Pro gradu, 2016

Lehto Miikael, Lehto Martti. 2017. Health Information Privacy of Activity Trackers, Proceedings of the 16th European Conference on Cyber Warfare and Security, University College Dublin, Dublin, Ireland, 29.30.6.2017, pages 243–251

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.-2.7.2010, pages 177 - 182.

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

Martti T., Viitanen J. 2016. Asiakas- ja potilastietojen toissijaisen käytön kokonaisarkkitehtuurin nykytila, 7.7.2016

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/

Motti, V. G., & Caine, K. (2015). Users' Privacy Concerns About Wearables: impact of form factor, sensors and type of data collected. In Financial Cryptography and Data Security Conference.

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

Mulero A. 2017. Must-know healthcare cybersecurity statistics, HealthcareDIVE, Feb. 27, 2017

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

Neuvoston direktiivi 93/42/ETY, annettu 14 päivänä kesäkuuta 1993, lääkinnällisistä laitteista

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

Patterson, H. (2013). Contextual expectations of privacy in self-generated health information flows. In TPRC, 2013.

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: 6.2.2019 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. 2018. 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

Protenus, Breach Barometer Report 2017, https://www.protenus.com/2017-breach-barometer-annual-report

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

Rubenfire A. 2017. A Smarter Anti-Hacker Defense, Modern Healthcare, 21.1.2017

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

Smith. Ms. 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

Sortti P. 2019. Tietosuojalaki ja EU:n tietosuoja-asetus ovat nyt voimassa – mikä on muuttunut? 17.01.2019 https://www.eilakaisla.fi/blogi/tietosuojalaki-ja-eun-tietosuoja-asetus-ovat-nyt-voimassa-mika-on-muuttunut

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

Sosiaali- ja terveydenhuollon asiakas- ja potilastiedon toissijaista käyttöä koskevaa lainsäädäntöä valmistelevan työryhmän väliraportti, 4.7.2016

Sosiaali- ja terveystietojen tietoturvallisen hyödyntämisen kokonaisarkkitehtuuri, Luonnos 0.3 16.6.2017

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 Corporation. 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

Talus A., Autio E., Hänninen A., Pihamaa H-T., Kantonen S. 2017. Miten valmistautua EU:n tietosuoja asetukseen? Tietosuojavaltuutetun toimisto, Selvityksiä ja ohjeita 4/2017, 27.1.2017. Saatavilla 7.3.2019 https://tietosuoja.fi/documents/6927448/9666681/Miten+valmistautua+tietosuoja-asetukseen/8c5b9a96-a8ce-4c91-ad06-6e36130bd0e5/Miten+valmistautua+tietosuoja-asetukseen.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

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.

Viestintävirasto. 2016. Terveydenhuoltoalan kyberuhkia, Saatavilla: 6.2.2019 https://

www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf

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

Virkkunen H., Mäkelä-Bengs P., Vuokko R. (toim.) 2015. Terveydenhuollon rakenteisen kirjaamisen opas Osa I, THL, 2015

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

Yhteiskunnan turvallisuusstrategia. 2017 Valtioneuvoston periaatepäätös, Turvallisuuskomitea 2.11.2017. saatavilla 7.3.2019 https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

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).

Verkkosivuja

www.cisecurity.org

www.sitra.fi/hyvinvointi/hyvinvointidata

www.vahtiohje.fi/web/guest/kuinka-valttaa-tartunta

LIITTEET

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

Lähde: World Health Organization, Core Medical Equipment, 2011, 1–2.

LIITE 2

Euroopan neuvoston direktiivi lääkinnällisistä laitteista

Tässä direktiivissä tarkoitetaan:

a) lääkinnällisellä laitteella tarkoitetaan kaikkia instrumentteja, laitteistoja, välineitä, ohjelmistoja, materiaaleja tai muita tarvikkeita, joita käytetään joko yksinään tai yhdistelminä, mukaan luettuina valmistajansa erityisesti diagnosointi- ja/tai hoitotarkoituksiin tarkoittamat ja lääkinnällisen laitteen asianmukaiseen toimintaan tarvittavat ohjelmistot ja joita valmistaja on tarkoittanut käytettäviksi ihmisten:

* Sairauden diagnosointiin, ehkäisyyn, tarkkailuun, hoitoon tai lievitykseen.
* Vamman tai vajavuuden diagnosointiin, tarkkailuun, hoitoon, lievitykseen tai kompensointiin.
* Anatomian tai fysiologisen toiminnon tutkimiseen, korvaamiseen tai muunteluun.
* Hedelmöitymisen säätelyyn.

Kyse on samasta kokonaisuudesta, kun laitteiden pääasiallista aiottua vaikutusta ihmiskehossa tai -kehoon ei saavuteta farmakologisin, immunologisin tai metabolisin keinoin, mutta joiden toimintaa voidaan tällaisilla keinoilla edistää.

Tätä direktiiviä sovelletaan lääkinnällisiin laitteisiin ja niiden lisälaitteisiin. Tässä direktiivissä lisälaitteita pidetään sellaisenaan lääkinnällisinä laitteina. Laitteita ja niiden lisälaitteita kutsutaan jäljempänä ’laitteiksi’.

b) ’lisälaitteella’ kaikkia tarvikkeita, vaikka ne eivät olisi laitteita, joita valmistaja on erityisesti tarkoittanut käytettäväksi laitteen kanssa mainitun laitteen käyttämiseksi tämän laitteen valmistajan aikomuksen mukaisesti,

c) ’in vitro -diagnostiikkaan tarkoitetulla lääkinnällisellä laitteella’ lääkinnällistä laitetta, joka on reagenssi, reagenssituote, kalibraattori, vertailumateriaali, testipakkaus, instrumentti, laite, laitteisto tai järjestelmä joko yksin tai yhdessä muiden kanssa käytettynä ja jonka valmistaja on tarkoittanut käytettäväksi in vitro ihmiskehosta otettujen näytteiden, mukaan lukien veren ja kudosten luovutukset, tutkimisessa yksinomaisena tai pääasiallisena tarkoituksena saada tietoa:

* fysiologisesta tilasta, patologisesta tilasta tai
* synnynnäisestä epämuodostumasta tai
* turvallisuuden ja yhteensopivuuden määrittämiseksi mahdollisten saajien kannalta tai
* hoitotoimenpiteiden tarkkailemiseksi.

Näytteenottoastioiden katsotaan olevan in vitro -diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita. Näytteenottoastiat, tyhjiöllä tai ilman tyhjiötä, ovat laitteita, joiden nimenomainen tarkoitus niiden valmistajan mukaan on sisältää ja säilyttää ihmiskehosta otettuja näytteitä välittömästi näytteenoton jälkeen in vitro -diagnostista tutkimusta varten.

Yleiseen laboratoriokäyttöön tarkoitettuja tuotteita ei pidetä in vitro -diagnostiikkaan tarkoitettuina laitteina, ellei valmistaja ole niiden ominaisuudet huomioon ottaen erityisesti tarkoittanut niitä käytettäväksi in vitro -diagnostisessa tutkimuksessa.

d) ’yksilölliseen käyttöön valmistetulla laitteella’ kaikkia laitteita, jotka on erityisesti valmistettu asianmukaisesti pätevän lääkärin kirjallisen määräyksen mukaisesti, jossa tämän vastuulla annetaan laitteen yksityiskohtaiset suunnitteluominaisuudet, ja jotka on tarkoitettu käytettäviksi ainoastaan tietylle potilaalle.

Edellä mainitun määräyksen voi laatia myös muu henkilö, joka on siihen ammatillisen pätevyytensä perusteella oikeutettu.

Jatkuvalla tai sarjatuotantomenetelmällä valmistettuja laitteita, joita on muunnettava lääkärin tai muun ammattikäyttäjän erityistarpeita varten, ei saa pitää yksilölliseen käyttöön valmistettuina laitteina;

e) 'kliinisiin tutkimuksiin tarkoitetulla laitteella' kaikkia laitteita, jotka on tarkoitettu asianmukaisesti pätevän lääkärin käytettäviksi tehtäessä liitteessä X olevassa 2.1 kohdassa tarkoitettuja tutkimuksia ihmisille asianmukaisissa kliinisissä olosuhteissa.

Kliinisten tutkimusten toteuttamisessa asianmukaisesti pätevään lääkäriin rinnastetaan muut henkilöt, jotka ammatillisen pätevyytensä perusteella ovat oikeutettuja suorittamaan näitä tutkimuksia;

f) 'valmistajalla' luonnollista henkilöä tai oikeushenkilöä, joka on vastuussa laitteen suunnittelusta, valmistuksesta, pakkaamisesta ja merkitsemisestä sen markkinoille saattamiseksi omalla nimellään, nämä toimet voi suorittaa tämä sama henkilö tai kolmas henkilö tämän lukuun.

Tässä direktiivissä valmistajille asetettavia velvollisuuksia sovelletaan yhtäläisesti luonnolliseen henkilöön tai oikeushenkilöön, joka kokoaa, pakkaa, käsittelee, täysin kunnostaa ja/tai merkitsee yhden tai useamman valmiin tuotteen ja/tai antaa niille laitteena käyttötarkoituksen markkinoille saattamiseksi omalla nimellään. Tätä ei sovelleta henkilöön, joka olematta ensimmäisen alakohdan mukainen valmistaja, kokoaa tai muuntaa käyttötarkoituksen mukaan jo markkinoille saatettuja laitteita yksittäisen potilaan käyttöön;

g) 'käyttötarkoituksella' käyttöä, johon laite valmistajan merkinnöissä, käyttöohjeessa ja/tai myynninedistämistä koskevassa aineistossa annettavien tietojen mukaan on tarkoitettu;

h) 'markkinoille saattamisella' laitteen ensimmäistä käyttöön saattamista maksua vastaan tai ilmaiseksi, ei kuitenkaan kliinisiin tutkimuksiin tarkoitettuja laitteita, sen jakelemiseksi ja/tai käyttämiseksi yhteisön markkinoilla, riippumatta siitä, onko laite uusi tai täysin kunnostettu;

i) 'käyttöönottamisella' vaihetta, jossa laite on loppukäyttäjän saatavilla ja valmis käytettäväksi yhteisön markkinoilla ensimmäistä kertaa käyttötarkoituksensa mukaisesti;

j) 'valtuutetulla edustajalla' yhteisöön sijoittautunutta luonnollista henkilöä tai oikeushenkilöä, joka valmistajan nimenomaisesti nimeämänä toimii valmistajan puolesta ja jonka puoleen yhteisön viranomaiset ja elimet voivat kääntyä valmistajan asemesta valmistajalle tämän direktiivin mukaisesti kuuluvien velvoitteiden osalta;

k) 'kliinisillä tiedoilla' laitteen kliinisen käytön perusteella saatuja turvallisuutta ja/tai suorituskykyä koskevia tietoja. Kliinisten tietojen on oltava peräisin:

* asianomaista laitetta koskevasta yhdestä tai useammasta kliinisestä tutkimuksesta; tai

* samankaltaista laitetta, jonka vastaavuus asianomaisen laitteen kanssa voidaan osoittaa, koskevasta yhdestä tai useammasta kliinisestä tutkimuksesta tai muista tutkimuksista, joista on raportoitu tieteellisessä kirjallisuudessa; tai

* asianomaisesta laitteesta tai samankaltaisesta laitteesta, jonka vastaavuus asianomaisen laitteen kanssa voidaan osoittaa, saatuja muita kliinisiä kokemuksia

kuvaavista julkaistuista ja/tai julkaisemattomista raporteista;

l) ’laitealaryhmällä’ sellaisten laitteiden kokonaisuutta, joilla on yhteisiä käyttötarkoitusaloja tai joissa on yhteistä tekniikkaa;

m) ’geneerisellä laiteryhmällä’ sellaisten laitteiden kokonaisuutta, joilla on sama tai vastaava käyttötarkoitus tai yhteistä tekniikkaa, minkä johdosta ne voidaan luokitella yleisesti erityispiirteitä kuvaamatta;

n) ’kertakäyttölaitteella’ laitetta, jota on tarkoitus käyttää vain kertaalleen yhtä potilasta varten.

Lähde: Neuvoston direktiivi 93/42/ETY, annettu 14 päivänä kesäkuuta 1993, lääkinnällisistä laitteista.

LIITE 3

Lääkintälaitteiden kyberominaisuuksia

Viitetutkimuksessa 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.

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.

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.

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. Myös ultraäänilaitteissa on USB-portteja, joita voidaan hyödyntää hyökkäysvektoreina.

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.

Muista tutkimuksessa olleista laitteista voidaan todeta seuraavaa:

* Liikuteltavia röntgenlaitteita (Ziehman RFD ja Fuji FDR Go) voidaan myös yhdistää langattomaan verkkoon erillisillä adaptereilla, mutta tutkimuk-

sessa mukana olleista laitteiden salausmenetelmistä ei ollut käytettävissä ohjekirjatietoa.

* Radiometerin verikaasuanalysaattori (ABL90 FLEX) ei yhdisty langattomaan verkkoon, mutta LAN verkkoon kyllä-kin. 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

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 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.

TAULUKKO 9: Mahdollisia MRI-kuvantamislaitteeseen kohdistuvia hyökkäyksiä (Ayala, 2016, 21).

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.

Taulukossa 9 havainnollistuvat mahdolliset MRI-laitteeseen kohdistuvat kyberfyysiset hyökkäykset.

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.

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.

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 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.

TAULUKKO 10: Potentiaaliset PET-skannerin hakkerointimahdollisuudet (Ayala, 2016, 21–22).

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. Esimerkkejä potentiaalisista PET-skannerin hakkeroinneista on esitelty taulukossa 10.

Röntgengeneraattori

Lääketieteellisiä röntgenlaitteita käytetään ottamaan kuvia tiheistä kudoksista. Laitteiden 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.

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 suosituksia korkeammaksi, mikä 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 säteilyaltistumisessa.
Saa röntgenlaitteen tekemään satunnaisia hälytyksiä.	Häiritsee röntgenoperaatioita.
Saa röntgenlaitteen käynnistymään uudelleen.	Pyyhkii konfiguraatioasetukset.
Yhdistää jonkun potilaan kuvantamistiedosto toisen potilaan vastaavaan.	Diagnoosi toimitetaan väärälle potilaalle.

TAULUKKO 11: Mahdollisia röntgenlaiteeseen kohdistuvia hyökkäyksiä (Ayala, 2016, 22).

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.

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.

Säteilystä aiheutuneet palovammat voivat olla akuutteja paikallisia altistuksia, jotka ovat seurausta suoralle 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. Taulukosta 11 havainnollistuu röntgenlaitteeseen kohdistuvia kyberfyysisiä hyökkäyksiä.

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

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.

TAULUKKO 12: Mahdollisia CT-skanneriin kohdistuvia hyökkäyksiä (Ayala, 2016, 26).

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 edellisellä sivulla taulukossa 12.

Robottikirurgiset koneet

Robottikirurgisia koneita on hyödynnetty useammanlaisissa kirurgisissa operaatioissa, ku-

ten 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.

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. Taulukossa 13 havainnollistetaan mahdollisia leikkauskirurgisiin robotteihin kohdistuvia kyberfyysisiä hyökkäyksiä.

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 14 havainnollistetaan potentiaalisia anestesiakoneisiin kohdistuvia kyberfyysisiä hyökkäyksiä. Sairaalat luottavat vahvasti kliinisiin tietovarastoihin, kliiniseen informatiik-

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

TAULUKKO 13: Mahdollisia kirurgisiin robotteihin kohdistuvia hyökkäyksiä (Ayala, 2016, 31).

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.

TAULUKKO 14: Mahdollisia anestesiakoneisiin kohdistuvia hyökkäyksiä (Ayala, 2016, 27).

kaan, terveystietojärjestelmiin ja potilastietueisiin. Hakkeri voi ilman vaadittavaa autentikointia 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. Esimerkkejä potentiaalisista hakkeroinneista on esitelty taulukossa 15.

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.

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.

Terroristihakkeri voi kyetä tuhoamaan näytteiden jäljitysohjelmiston ja saada viivakoodin

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 ylinannostus, 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.

TAULUKKO 15: Digitaalisiin potilastietueisiin 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.

TAULUKKO 16: Viivakoodin lukemisjärjestelmiin kohdistuvia hyökkäyksiä. (Ayala, 2016, 35–36.)

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. Esimerkkejä potentiaalisista viivakoodilukujärjestelmän hakkeroinneista on esitelty taulukossa 16.

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).

Esimerkkejä potentiaalisista lääketieteelliseen laboratorioon kohdistuvista hyökkäyksistä on mainittu taulukossa 17 seuraavalla sivulla.

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-keuhkokoneeseen, 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

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.

TAULUKKO 17: Lääketieteellisiin laboratorioihin kohdistuvia hyökkäyksiä. (Ayala, 2016, 28.)

mukaan. Taulukossa 18 on esimerkkejä potentiaalisista sydän-keuhko -koneeseen kohdistuvista hakkeroinneista.

LÄHTEET

Heli Kallio, Sairaalalaitteiden turvallisuudesta, julkaisematon Cyber Trust -hankeraportti 12.9.2016.

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

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.

TAULUKKO 18: Sydän-keuhkokoneeseen kohdistuvia hyökkäyksiä (Ayala, 2016, 28).

LIITE 4

Kyberhyökkäyksiä terveydenhuollossa lajityypin mukaan

1. Kiristysohjelmahyökkäykset

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.)

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.)

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.)

Lukas Hospital, Saksa 1.2.2016:

Röntgenlaitetta ei voitu käyttää. 15–20 prosenttia toimenpiteistä peruutettu. Samanlaiset ongelmat kahdessa muussa Saksan sairaalassa. (Steffen, 2016.)

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.)

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.)

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.)

Methodist Hospital, USA 18.3.2016:

Kiristyshaittaohjelma havaittu verkossa. Sairaala käytti varmuusjärjestelmäänsä, kun pääverkko oli lukittu. Organisaation sisäinen tila, joka rajoitti sähköisten webpohjaisten palvelujen käyttöä. (Monegain, 2016b.)

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.)

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.)

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.)

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.)

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.)

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.)

National Health Service, UK 12.5.2017:

Hyökkääjä käytti WannaCry-kiristyshaittaohjelmaa, 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.)

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.)

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.)

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.)

2. Hakkeroinnit

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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. Oikeusjuttu organisaatiota vastaan käynnissä laiminlyödystä tietoturvasta. (McGee, 2016.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

Central Ohio Urology Group, USA 1.8.2016:

Haitantekijät saivat haltuunsa 223 gigatavua dataa: 401 828 tiedostoa, jotka sisältä-

vät 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.)

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.)

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.)

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.)

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.)

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.)

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.)

Chase Brexton Health Care, USA 17.10.2017:

Haitantekijät saivat haltuunsa 16 562 potilaan tiedot, kun neljä työntekijää joutuivat tietojenkalastushyökkäyksen kohteeksi. Tietojenkalasteluviestit lähetettiin 2.–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.)

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.)

3. Muut hyökkäysmuodot

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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.)

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 julkistamatto-

man määrän ultraäänilaitteita. Varastettujen laitteiden palauttamisen yhteydessä selvisi, että laitteet sisälsivät potilastietoja kuten nimiä, lääketieteelliset tietoja ja kuvia. (LaPointe, 2016b.)

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.)

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.)

Red Cross Blood Service, Australia 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.)

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.)

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 Kelainverkkopalveluihin. Sähköisten reseptien käyttö estyi. (Finnish News Network, 2017.)

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.)

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.)

Lahden kaupunki, Suomi 9.2.2018:

Virtuaalivaluuttaa louhiva haittaohjelma saastutti Lahden kaupungin tietojärjestel-

> män – 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.)