Timo Broström

KYBERRIKOLLISUUS DIGITAALISEN TERVEYDEN-HUOLLON UHKANA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Broström, Timo
Kyberrikollisuus digitaalisen terveydenhuollon uhkana
Jyväskylä: Jyväskylän yliopisto, 2021, 34 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Halttunen, Veikko

Tulevaisuuden terveydenhuoltoa tarjotaan digitaalisesti. Terveydenhuollossa käytettävien digitaalisten laitteiden määrä kasvaa, ja ihmiset käyvät lääkärin vastaanotolla etänä internetin välityksellä, hakevat terveystietoa internetistä sekä käyttävät mobiilisovelluksia seuratakseen terveyttään. Terveydenhuollon digitalisoituminen vähentää kustannuksia sekä parantaa sen saatavuutta. Kaikki tämä kuitenkin kerää paljon tietoa potilaista, joka puolestaan houkuttelee kyberrikollisia. Terveydenhuoltoon kohdistuvat kyberrikokset uhkaavat palveluiden saatavuutta sekä potilaiden yksityisiä tietoja, ja pahimmassa tapauksessa myös potilaan henki voi olla vaarassa. Tämä tutkielma kartoitti digitaalisen terveydenhuollon uhkakuvia keskittyen kyberrikollisuuteen, jonka lisäksi myös rikoksista saatujen tietojen käyttöä sekä digitaalisen terveydenhuollon heikkoja kohtia tuotiin esille. Tutkielma toteutettiin kirjallisuuskatsauksena, ja lähteiksi valikoitui luotettavia, korkean tason tieteellisiä julkaisuja ja kirjoja. Tutkielmasta kävi ilmi, että digitaalinen terveydenhuolto kohtaa useita eri kyberrikollisuuden muotoja, kuten haittaohjelmien eri muotoja, palvelunestohyökkäyksiä, tietomurtoja ja hakkerointia sekä tulevaisuudessa mahdollisesti kokonaan uuden uhan, ihmishaittaohjelmat. Kyberrikolliset käyttävät varastettuja tietoja lääketieteellisissä identiteettivarkauksissa, myyvät ne eteenpäin, hankkivat niillä itse terveyspalveluita tai tehtailevat petoksia. Terveydenhuolto ei selvästikään ollut valmis kyberrikoksien aaltoon, sillä investoinnit kyberturvallisuuteen on edelleen vähäistä. Terveydenhuollon turvallisuuskulttuuri on välinpitämätöntä, korostaen mukavuutta ja helppoutta turvallisuuden yli. Lisäksi ihmiset, jotka käyttävät terveyttä parantavia laitteita tai sovelluksia suhtautuvat varsin välinpitämättömästi omien laitteidensa kyberturvallisuuteen. Digitaalisen terveydenhuollon mahdollisuudet ovat mittavat, mutta tulevaisuuden digitaalinen terveydenhuolto on turvallista vain, jos kaikki panostavat siihen.

Asiasanat: digitaalinen terveydenhuolto, terveydenhuolto, kyberrikollisuus, haittaohjelmat

ABSTRACT

Broström, Timo
Cybercrime as a threat to digital health
Jyväskylä: University of Jyväskylä, 2021, 34 pp.
Information Systems Science, Bachelor's Thesis
Supervisor(s): Halttunen, Veikko

The healthcare of the future will be provided digitally. The number of digital devices used in healthcare is growing, and people are conducting their doctors' appointments remotely via the internet, searching health information from the internet, and using mobile apps to monitor their health. The digitalization of healthcare will reduce costs and improve its accessibility. All of this, however, gathers a lot of information about patients, which in turn attracts cybercriminals. Cybercrime in healthcare threatens access to services as well as patients' private information, and in the worst case, the patient's life may also be at risk. This bachelor thesis maps the threats to digital health with a focus on cybercrime, in addition to which the use of stolen data and information and the weaknesses of digital health were also highlighted. The bachelor thesis has been carried out as a literature review, and reliable, high-level scientific publications and books were selected as sources. The study found that digital health faces several different forms of cybercrime, such as different forms of malware, denial-of-service attacks, hacking and data breaches and possibly a completely new threat in the future, human malware. Cybercriminals use stolen information for medical identity theft, sell it, obtain health services themselves or commit frauds. Clearly, healthcare was not ready for a wave of cybercrime, as investment in cybersecurity remains low. The safety culture in healthcare is nonchalant, emphasizing comfort and ease over safety. In addition, people who use health-enhancing devices or applications are quite nonchalant to the cybersecurity of their own devices. The potential for digital health is prodigious, but the digital health of the future will only be safe if everyone invests in it.

Keywords: digital health, healthcare, cybercrime, malware

KUVIOT

KUVIO 1 Digitaaliseen terveydenhuoltoon kohdistuvat kyberrikokset 24

TAULUKOT

TAULUKKO 1 Kyberrikollisuuden luokat 15
TAULUKKO 2 Tietojen käyttökohteet 25

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT
TAULUKOT

1 JOHDANTO 6

2 DIGITAALINEN TERVEYDENHUOLTO JA KYBERRIKOLLISUUS 9
2.1 Digitaalinen terveydenhuolto 9
2.2 Kyberrikollisuus 13

3 KYBERRIKOLLISUUDEN AIHEUTTAMAT UHAT DIGITAALISELLE TERVEYDENHUOLLOLLE 18
3.1 Digitaaliseen terveydenhuoltoon kohdistuvat kyberrikokset 18
3.2 Rikoksista saatujen tietojen käyttökohteet 21
3.3 Digitaalisen terveydenhuollon haavoittuvuudet 22
3.4 Tulokset ja johtopäätökset 23

4 YHTEENVETO 26

LÄHTEET 29

1 JOHDANTO

Terveydenhuolto toimii tulevaisuudessa yhä enemmän verkon välityksellä, varsinkin kun väestö ikääntyy. Potilaisiin on helpompaa ottaa yhteyttä etänä sen sijaan, että potilaan pitäisi itse saapua sairaalaan tai hoitajan käydä potilaan luona paikan päällä. Ihmiset voivat itse ennaltaehkäisevästi parantaa ja seurata terveyttään erilaisten sovelluskaupoista saatavien terveyttä edistävien sovellusten avulla. Kaikki terveydenhuollossa käytettävä teknologia kuitenkin kerää paljon tietoa potilaasta, mikä houkuttelee rikollisia. Potilastietojen vaarantuminen voi aiheuttaa erilaisia ongelmia potilaalle, esimerkiksi tietojen väärinkäyttö voi haitata potilaan elämää. Terveydenhuollon ammattilaisten kuin myös terveyspalvelujen käyttäjienkin pitää siis olla hereillä sekä ajan tasalla kyberrikoksista, jotka uhkaavat nykyistä digitaalista terveydenhuoltoa.

Terveydenhuolto on suurin ja nopeimmin kasvava ala maailmassa ja sen odotetaan vain kasvavan tulevaisuudessa (Thümmler, 2015). Terveydenhuollon palveluja tarjotaan nykyisin digitaalisten ratkaisujen avulla. Digitaalinen terveydenhuolto sisältää monia eri teknologioita ja menetelmiä, kuten itsevalvontalaitteita, terveyssovelluksia, kehoon asetettavia laitteita, terveydenhuollon tietoverkkoja ja -järjestelmiä, sähköposti, virtuaalitodellisuudet sekä useita muita ratkaisuja (Lupton, 2017).

Erilaiset kyberrikollisuuden muodot, kuten kiristyshaittaohjelmat, palvelunestohyökkäykset, tietojenkalastelu, hakkerointi sekä tietovuodot aiheuttavat kuitenkin vakavia ongelmia terveydenhuollolle. Ne estävät palveluiden saatavuutta sekä aiheuttavat haittaa ihmisille, kun omat henkilökohtaiset terveystiedot päätyvät ulkopuolisten käyttöön.

Tutkielmani tarkoituksena on kartoittaa kyberrikollisuuden uhkaa digitaaliselle terveydenhuollolle sekä selvittää, miten kyberrikolliset käyttävät saamiansa tietojaan sekä löytää digitaalisen terveydenhuollon heikkoja kohtia.

Tutkimuskysymykset on muodostettu seuraavasti:

- Mitkä kyberrikollisuuden muodot uhkaavat digitaalista terveydenhuoltoa?
- Miten kyberrikolliset ovat käyttäneet tietoja, joihin he ovat päässeet käsiksi?

- Millaisia heikkouksia liittyy digitaaliseen terveydenhuoltoon?

Tutkielma on toteutettu kirjallisuuskatsauksena. Lähdekirjallisuus koostuu tieteellisistä artikkeleista, kirjoista sekä kokoelmateoksista. Lähdemateriaalin keräämiseen käytettiin Google Scholar-, ResearchGate-, Scinapse- ja JYKDOK hakukoneita. Hakusanoina toimivat ”digital health”, ”cybercrime”, ”electronic health”, ”ehealth”, ”medical device”, ”cyber threat” sekä edellisten yhdistelmät. Lähdekirjallisuutta etsittiin vain englannin kielellä, koska suomenkielisiä, hyvän tason lähteitä on vielä vähän ja lisäksi kyberrikollisuus on vähän tutkittu aihe suomen kielellä. Lähteiksi valittiin julkaisuja, jotka julkaisufoorumi oli arvioinut olevan tasolla 1–3. Lisäksi arvioitiin lähteiden kirjoittajien tunnettuutta ja arvostettuutta, lähteen uskottavuutta ja kustantajan arvovaltaa. Lisäksi lähteiksi kelpuutettiin nettisivu sekä raportti, koska niissä käsiteltiin tutkielman kannalta relevanttia tietoa. Lähteiksi on pyritty valitsemaan varsin tuoreita julkaisuja, muutamia poikkeuksia kuitenkin löytyy.

Seuraavaksi on hyvä selittää auki lyhyesti muutamia käsitteitä, jotka esiintyvät tutkielmassa mutta joihin ei keskitytä syvällisemmin:

- *Kyberturvallisuudella* tarkoitetaan menettelytapoja, joita käytetään tietokoneiden, palvelinten, mobiililaitteiden, tietojärjestelmien, verkkojen ja datan puolustamiseen haitallisilta hyökkäyksiltä (Giansanti, 2021).
- *Kyberavaruus* on vuorovaikutusympäristö, joka on luotu yhdistämällä tietokoneet tietoliikenneverkkoon (Yar & Steinmetz, 2019).
- *Pimeällä verkolla* tarkoitetaan foorumeita, jotka ovat sellaisessa osassa internetiä, joihin pääsee vain tiettyjen salausohjelmien ja selainprotokollien avulla (Holt, Bossler & Seigfried-Spellar, 2017).

Tutkielman tarkoituksena on antaa lukijalle hyvä yleiskuva kyberrikoksista, jotka uhkaavat digitaalista terveydenhuoltoa, sekä siitä, mihin rikolliset käyttävät varastettuja tietoja sekä digitaalisen terveydenhuollon haavoittuvuuksista. Yleensä kirjallisuus on keskittynyt vain tiettyihin rikoksiin, jotka uhkaavat terveydenhuoltoa, jonka lisäksi rikoksista saatujen tietojen käyttöä ei ole laajasti tutkittu.

Tutkielmassa selvisi, että digitaalinen terveydenhuolto kohtaa useita eri kyberrikoksen muotoja, muun muassa kiristyshaittaohjelmia, lääketieteellisiä identiteettivarkauksia, palvelunestohyökkäyksiä, petoksia, tietojenkalastelua, tietovuotoja sekä hakkerointia. Rikolliset puolestaan käyttävät näitä tietoja itse, joko hoidon saamiseen tai lääkkeiden ostamiseen tai myyvät ne eteenpäin. Digitaalisen terveydenhuollon haavoittuvaisuuksia ovat puolestaan riittämättömät investoinnit kyberturvallisuuteen, digitaalisten laitteiden huono suojaus, sekä itse ihmiset.

Tutkielma jakaantuu neljään lukuun: johdantoon, kahteen sisältölukuun ja yhteenvetoon. Ensimmäisessä sisältöluvussa selitetään, mitä on digitaalinen terveydenhuolto, käydään läpi siihen liittyviä määritelmiä, ja avataan lukijalle mitä eri teknologioita sekä ratkaisuja kuuluu digitaaliseen terveydenhuoltoon.

Lisäksi ensimmäisessä sisältöluvussa käydään läpi mitä on kyberrikollisuus, avaamalla lukijalle internetin historiaa sekä kyberrikollisuuden historiaa, ja sen määritelmiä, luokkia sekä antamalla esimerkkejä rikoksista. Toisessa sisältöluvussa keskitytään kyberrikollisuuden aiheuttamiin uhkiin, jotka koskettavat digitaalista terveydenhuoltoa, sekä perehdytään siihen mihin rikolliset käyttävät saamiansa tietojaan. Lopussa käydään myös läpi digitaalisen terveydenhuollon haavoittuvuuksia ja lopulta tiivistetään tulokset ja vedetään johtopäätökset. Yhteenvedossa kerrataan sekä käydään läpi tutkielman keskeiset pääkohdat.

2 DIGITAALINEN TERVEYDENHUOLTO JA KYBERRIKOLLISUUS

Tässä luvussa käsitellään yleisesti mitä on digitaalinen terveydenhuolto sekä mitä on kyberrikollisuus. Alakappaleessa 2.1 kerrotaan digitaalisesta terveydenhuollosta ja alakappaleessa 2.2 esitellään kyberrikollisuutta.

2.1 Digitaalinen terveydenhuolto

Aluksi on syytä tehdä selväksi mitä tarkoitetaan digitaalisella terveydenhuollolla, sillä termillä on useampia määritelmiä. Sen lisäksi toinen termi, sähköinen terveydenhuolto, sekoittuu yleensä digitaalisen terveydenhuollon kanssa keskenään tai aiheuttaa muuten epäselvyyttä.

Digitaalinen terveydenhuolto ja sähköinen terveydenhuolto kohtaavat harvoin hyvin määriteltyinä termeinä tutkimuskirjallisuudessa. Yleensä artikkeleissa tai kirjoissa määritellään joko vain digitaalinen terveydenhuolto (Elenko, Underwood & Zohar, 2015; Fricker, Thümmler & Gavras, 2015; Lupton, 2017; Petersen, 2018; Rivas, & Wac, 2018; Wulfovich & Meyers, 2020) tai sähköinen terveydenhuolto (Boric-Lubecke ym., 2014; Gaddi, Capello & Manca, 2014; Iakovidis, Wilson & Healy, 2004; Mukherjee & McGinnis, 2007; Zeadally, Isaac & Baig, 2016), ja vain harvoin molemmat määritellään (Kukafka, 2019; Menvielle, Audrain-Pontevia & Menvielle, 2017), vaikka molemmat termit esiintyisivätkin samassa tutkimuksessa tai kirjassa. Digitaalisen terveydenhuollon on katsottu välillä myös olevan vain yksi sähköisen terveydenhuollon osa (Petersen, 2018). Kirjallisuudessa, jossa puhutaan digitaalisesta terveydenhuollosta, sähköinen terveydenhuolto yleensä mainitaan vain yhtenä digitaalisen terveydenhuollon teknologiana (Chu, Shah, Rouholiman, Riggare & Gamble, 2018) eikä sitä vaivauduta tarkemmin määrittelemään. Toisaalta voi olla, että sähköisellä ja digitaalisella terveydenhuollolla tarkoitetaan samaa asiaa (Petersen, 2018). On myös huomioitava, että sähköisestä terveydenhuollosta kertova kirjallisuus on hieman vanhempaa kuin digitaalisesta terveydenhuollosta kertova kirjallisuus.

Siksi onkin hyvin mahdollista, että termistö on muuttunut ajan kuluessa, kun digitalisaatio on nostanut päätään terveydenhuollossa.

Cunningham, Wake, Waller ja Morris (2014) määrittelevät sähköisen terveydenhuollon (engl. Electronic Health tai ”eHealth”) sellaisten terveyspalveluiden käytöksi, jotka voidaan toteuttaa käyttäen tietokonepohjaisia kommunikaatiovälineitä. Silber (2004) sekä Zeadally ym. (2016) kuvaavat sähköisen terveydenhuollon tieto- ja viestintätekniikan käytöksi terveydenhuollossa. Esimerkiksi potilas käyttää sähköisiä terveyspalveluita silloin, kun hän etsii tietoa internetistä tai käyttää itsehoitolaitteita (Silber, 2004). Cumming ym. (2017) kuvaavat sähköisen terveydenhuollon lyhyesti terveydenhuollon ja sen resurssien sähköisenä siirtona.

Digitaalinen terveydenhuolto (engl. Digital Health) on puolestaan laaja kattotermi, joka sisältää myös sähköisen terveydenhuollon (WHO, 2019). Rivas (2018) kuvaa digitaalisen terveydenhuollon perustuvan tieto- ja viestintätekniikan käyttöönottoon ja hyödyntämiseen terveydenhuollon tarjoamiseksi ja laajentamiseksi ihmisille. Wulfovich ja Meyers (2020) selittävät digitaalista terveydenhuoltoa tieto- ja viestintätekniikan käytöllä lääketieteellisen tiedon vaihtamiseen sairauksien diagnosoimiseksi ja hoitamiseksi sekä hoitoprosessien ja päätöksenteon parantamiseksi. Elenko ym. (2015) määrittelevät digitaalisen terveydenhuollon laajaksi termiksi, joka kattaa valtavan määrän tuotteita sisältäen esimerkiksi mobiilisovellukset, puettavat teknologiat, joilla voidaan seurata esimerkiksi sydämen sykettä sekä sellaiset teknologiat, joiden täyttä vaikutusta terveydenhuoltoon ei ole vielä ymmärretty. Mestres (2017) puolestaan määrittelee digitaalisen terveydenhuollon terveydenhuoltopalvelujen tarjoamiseksi tai terveyden parantamiseksi käyttäen tietotekniikkaa tai sähköisten viestintävälineiden palveluita ja prosesseja.

Tässä tutkielmassa käytetään termiä digitaalinen terveydenhuolto, koska se viittaa teknologisiin ratkaisuihin ja menetelmiin. Sähköinen terveydenhuolto puolestaan viittaa enemmän palveluihin, joita voidaan toimittaa esimerkiksi internetin välityksellä.

Ihmisten terveydenhuolto on digitalisoitunut hyvää vauhtia teknologian kehityksen mukana. Digitaalisen terveydenhuollon aloituspisteenä voidaan pitää Thümmlerin (2015) mukaan 1960-lukua, jolloin tietokoneet tulivat sairaaloiden hallinnon tueksi. Tietokoneiden avulla muun muassa henkilökunnan palkanmaksu helpottui. Väestön nopea kasvu 1960- ja 1970-luvulla nosti terveydenhuollon massojen hyödykkeeksi, ja tietokoneiden avulla voitiin käsitellä esimerkiksi potilastietoja nopeasti. 1980-luvulla tietotekniikan kehityksen myötä sairaaloiden digitalisaatio eteni nopeasti. 1990-luvulla mukaan tulivat mobiiliteknologia ja langattomat yhteydet. (Thümmler, 2015.)

Nykyisin termi ”digitaalinen terveys” viittaa teknologisiin ratkaisuihin, joiden tavoitteena on toimittaa terveydenhuoltoa, tarjota tietoa maallikoille ja auttaa heitä jakamaan heidän kokemuksiaan terveydentilastaan, valmentaa ja kouluttaa terveydenhuollon ammattilaisia, auttaa kroonisista sairauksista kärsiviä ihmisiä osallistumaan itsehoitoon sekä kannustaa muita osallistumaan

aktiviteetteihin, joissa jaetaan kokemuksia omasta hyvinvoinnista sekä sairauksien välttämisestä (Lupton, 2017).

Luptonin (2017) mukaan terveydenhuollossa käytetään useita eri digitaalisia teknologioita ja menetelmiä. Sähköpostin, audiovisuaalisen kommunikaation, sovelluksien ja muiden yhteydenpitopalveluiden avulla potilas ja terveydenhuollon tarjoaja voivat pitää yhteyttä. Terveyteen ja lääketieteeseen liittyvät verkkosivut, sosiaalinen media, internetfoorumit ja wikit tarjoavat tietoa, tukea ja tuotteita maallikoille sekä mahdollisuuksia asiantuntijoiden väliseen kommunikaatioon. (Lupton, 2017.) Hakukoneita voidaan käyttää terveys- ja lääketieteellisen tiedon etsimiseen. Digitaalisia laitteita käytetään lääkkeiden jakoon tai kehon toimintojen säätelyyn tai parantamiseen, ja tällaisia laitteita ovat esimerkiksi sisäkorvaistutteet, sydänmonitorit ja insuliinipumput. (Lupton, 2017.) Käytössä on itsevalvontalaitteita, potilaan itsehoitolaitteita, älypuhelinsovelluksia sekä "älykkäät" esineet, jotka ovat sulautettuina digitaalisiin biosensoreihin, jotka keräävät yksityiskohtaista informaatiota ihmiskehosta. Henkilökohtaiset hätäapujärjestelmät antavat hälytyksen hoitajille tai terveydenhuollon ammattilaisille, jos käyttäjällä on kotona terveyteen liittyvä hätätilanne. (Lupton, 2017.) Digitaaliset kuvantamisjärjestelmät auttavat diagnoosin muodostamisessa, ja näitä kuvantamisjärjestelmiä ovat esimerkiksi ultraääni, genomianalyysityökalut, tietokonetomografia ja magneettikuvaus. Terveydenhuollon tietotekniikka ja tietojärjestelmät sisältävät puolestaan esimerkiksi sähköiset potilastiedot, luokittelu- ja päätöksenteko-ohjelmistot, verkkomaksut ja henkilöstöjärjestelmät. (Lupton, 2017.) Virtuaalitodellisuuden ja lisätyn todellisuuden menetelmillä koulutetaan potilaita, tehdään diagnooseja, hoidetaan mielenterveyttä ja liikkuvuusolosuhteita, tehdään leikkaussimulaatioita ja koulutetaan terveydenhuollon ammattilaisia. Lisäksi terveydenhuollossa käytetään Luptonin (2017) mukaan seuraavia teknologioita ja menetelmiä:

- Digitaaliset tautien seurantajärjestelmät.
- Biolääketieteelliset tutkimusohjelmistot.
- Pelikonsoliteknologiat ja sovellukset kuntoa ja terveyttä edistäviin aktiviteetteihin.
- Robottileikkaukset.
- Robottien avustama vanhustenhoito.
- Kolmiulotteiset tulostustekniikat kirurgiaan, proteesit ja potilaiden koulutus.
- Sensoripohjainen ympäristönseuranta, yhteisökehitys ja kansalaisten tieteelliset aloitteet.

Internetistä etsitään paljon terveystietoa ja terveyteen liittyvät nettisivut ovat erittäin suosittuja. Google on maininnut, että terveystietoon liittyvät haut ovat yksi Googlen suosituimmista hakuaiheista. (Lupton, 2017.) Sosiaalista mediaa käytetään myös aktiivisesti terveyteen liittyvän tiedon jakamiseen ja esimerkiksi Facebookista löytyy useita eri sivuja tietyille sairauksille (Bender, Jimenez-Marroquin & Jadad, 2011; Zhang, He & Sang, 2013). YouTube on tehokas väline terveystietojen jakamiseen (Liu, Zhang, Susarla & Padman, 2020). YouTube tar-

joaa myös lääketieteelliseen koulutukseen tarkoitettuja videoita (Lupton, 2017). Sosiaalisen median alustoilla ihmiset jakavat tietoa muun muassa heidän kehostaan, hoidoistaan sekä terveydenhuoltokokemuksistaan (Lupton, 2017).

Etälääketiede tarkoittaa kirjaimellisesti ”etänä harjoitettua lääketiedettä.” Etälääketieteen merkitys on kasvanut ja on nykyisin tärkeässä asemassa terveydenhuoltopalveluiden tarjonnassa. (Lupton, 2017.) Alun perin etälääketieteeseen kuuluivat puhelimet sekä erilaiset seinään kytkettävät laitteet, mutta nykyisin mukaan ovat tulleet videoyhteydet, langattomat laitteet, ohjelmistot ja applikaatiot. Nykyinen etälääketiede tarjoaa jatkuvaa reaaliaikaista monitorointia, langatonta tiedonsiirtoa ja pilvipalveluiden käyttöä. (Lupton, 2017.) Etälääketieteessä käytettyjen digitaalisten laitteiden ja sovellusten kirjo on laaja. Potilas voi esimerkiksi käyttää kotonaan puhelimeen ladattavaa sovellusta, joka on yhdistettynä verenpaineenmittauslaiteeseen, ja sovellus kerää tarvittavat tiedot mittauksen aikana, jonka jälkeen se lähettää tiedot langattomasti potilaan lääkärille. Älypuhelimiin voi myös hankkia lisälaitteita, joiden avulla älypuhelin voi monitoroida potilaan sydämen toimintaa. (Lupton, 2017.)

Potilaan hoidossa käytettävät digitaaliset laitteet voivat Luptonin (2017) mukaan integroitua kehon kanssa eri tavoin. Älypuhelimien ja kannettavien laitteiden tapauksessa ne ovat kehon ulkopuolella. Jotkin laitteet asetetaan kehoon vain tietyksi aikaa esimerkiksi mittaamaan jotain tietyn toimenpiteen ajaksi. (Lupton, 2017.) Osa laitteista, kuten sydämentahdistimet, sisäkorvaistutteet ja insuliinipumput puolestaan asetetaan leikkauksella kehoon, ja niistä tulee enemmän tai vähemmän osa kehoa. Lisäksi käytetään myös digitaalista lääkitystä, jossa potilas nielaisee pillerin, joka sisältää mikrosiruja, jotka reagoivat potilaan vatsassa olevien kemikaalien kanssa, tuottaen pienen jännitteen, joka välittyy potilaan laastariin ja siihen tulevat tiedot puolestaan lähetetään potilaan lääkärille. (Lupton, 2017.)

Terveyssovellukset ja puettavat itsehoitolaitteet ovat Luptonin (2017) ja Lanzingin (2016) mukaan suosittuja ihmisten keskuudessa. Terveyssovelluksia ladataan älypuhelimiin sovelluskaupoista ja niitä käytetään esimerkiksi jonkin fyysisen itsehoitolaitteen kanssa. Puettavat itsehoitolaitteet voivat mitata esimerkiksi verensokeria, kehon painoa, painoindeksiä, fyysistä aktiivisuutta, energian kulutusta, mielialaa, kehon lämpötilaa, hengitysnopeutta, ja jopa aivotoimintaa. (Lanzing, 2016; Lupton, 2017.) Näitä tietoja mittaavat itsehoitolaitteiden anturit, joita voi löytyä esimerkiksi rannekkeista, päänauhoista, kengistä tai ne voivat olla myös vaatteissa. Itsehoitolaitteet tuottavat paljon yksityiskohtaista tietoa, ja ne voidaan jakaa helposti esimerkiksi sosiaalisessa mediassa. (Lanzing, 2016; Lupton, 2017.)

Terveydenhuollossa käytettävät järjestelmät keräävät paljon erilaista tietoa potilaasta. Usein esimerkiksi sairaaloissa potilaista merkataan ylös potilaiden perustietoja, kuten nimi ja ikä, sekä tietoja terveydentilasta, määrätyistä lääkkeistä ja hoitohistoriasta (Lupton, 2017).

2.2 Kyberrikollisuus

Alkuun on syytä tarkastella hieman internetiä, sillä ilman sitä myöskään kyberrikollisuutta ei olisi. Internethän tarjoaa elektronisen ympäristön, jossa kyberrikoksia toteutetaan (Yar & Steinmetz, 2019). Internet on Castellsin (2002) mukaan tietokoneverkko, tai tarkemmin sanottuna ”verkkojen verkko.” Tämä verkko liittää tietokoneet yhteen mahdollistaen kommunikaation ja informaation vaihdon niiden välillä (Yar & Steinmetz, 2019). Internetin alun voi jäljittää 1960-luvulle, jolloin ARPA eli tutkimusprojektien virasto Yhdysvalloissa muodosti ARPANET:in (Castells, 2002). APRANET:in tavoite oli varmistaa sotilaiden turvallinen ja joustava tapa viestiä ja koordinoida (Yar & Steinmetz, 2019). Lukuisten eri kehitysvaiheiden jälkeen vuonna 1990 ARPANET poistettiin käytöstä. Tämä ei kuitenkaan merkinnyt internetin katoamista, vaan lukuisat eri internet-palveluntarjoajat rakensivat omat tietoverkostonsa kaupallisin perustein. (Castells, 2002.) Tämä johti lopulta internetin kasvuun globaaliksi tietoverkoksi. Vaikka internet onkin helpottanut esimerkiksi ihmisten välistä kommunikaatiota sekä elämää, internetin mukana tuli kuitenkin myös varjopuolia, ja yksi niistä on kyberrikollisuus.

Kyberrikollisuuden määrittely on hankalaa, eikä asiaa auta yhtään se, että pelkästään jo ”kyber-” etuliite on ongelmallinen (Yar & Steinmetz, 2019). Kybersanalla on monimutkainen historia. Sana alun perin syntyi 1940-luvulla, kun Norbert Wiener ja Arturo Rosenblueth pohtivat sopivaa termiä kehittelemälleen alalle, joka tutki erilaisten järjestelmien palaute- ja ohjausmekanismeja, ja he valitsivat nimeksi ”kybernetiikka” (Wiener, 1948). Kyber-sanaa käytettiinkin alun perin vain kybernetiikan alalla, eikä sillä ollut tietotekniikan kanssa mitään tekemistä, mutta ajan myötä termi ajautui yhä kauemmaksi alkuperäisestä tarkoituksestaan (Steinmetz & Nobles, 2018). Kyber-sana kuulosti futuristiselta ja sai paljon suosiota 1980-luvulla, kun kirjailija William Gibson (1984) esitteli tietokoneita ja tietokoneiden luomia tiloja käsittelevässä tieteisnovellissaan termin ”kyberavaruus”, ja kyber tulikin sen jälkeen nopeasti etuliitteeksi kaikille substantiiveille ja verbeille, joilla oli jotain tekemistä tietokoneiden tai internetin kanssa. 1980- ja 1990-luvuilla ”kyber-” etuliite tulikin mukaan moniin sanoihin populaarikulttuurin innoittamana, muun muassa kyberavaruus, kyberseksi, kybershoppailu, unohtamatta tietysti kyberrikollisuutta. (Steinmetz & Nobles, 2018; Yar & Steinmetz, 2019.) Vaikka kyber-sanalla onkin hankala historia, niin kyberrikollisuudesta on tullut kuitenkin tullut hallitseva termi, jolla kuvataan tietokoneverkkoon liittyviä rikoksia (Yar & Steinmetz, 2019).

Kyberrikollisuudella ei kuitenkaan ole vieläkään yksimielistä määritelmää, ei edes niillä viranomaisilla, jotka tutkivat kyseisiä rikoksia (Yar & Steinmetz, 2019). Tällä hetkellä toimivin määritelmä (Yar & Steinmetz, 2019) on Thomasin ja Loaderin (2000, s. 3) määritelmä. He kuvailevat kyberrikollisuuden ”tietokonevälitteisenä toimintana, joka on joko laitonta tai mitä jotkut osapuolet voivat pitää laittomina ja joita voidaan toteuttaa maailmanlaajuisten sähköisten verkkojen kautta.” Toisiakin määritelmiä löytyy, ja esimerkiksi Bernik (2014) määrit-

telee kyberrikollisuuden tieto- tai viestintätekniikan käyttönä rikollisten, haitallisten ja moraalittomien tekojen toteuttamiseen kyberavaruudessa. Walden (2007) puolestaan toteaa, että kyberrikollisuus on tietokonerikollisuuden alakategoria, eikä tietokoneen tarvitse olla yhdistettynä internetiin, jotta sillä voisi tehdä rikoksia ja jotta se olisi kyberrikos. Gillespie (2015) esittää vastakkaisen näkemyksen, jonka mukaan rikos on kyberrikollisuutta vain silloin, jos se on tehty internetissä tai sen avulla. Kyberrikollisuutta on myös määritelty todella yksinkertaisesti viittaamaan vain teknologisesti helpotettuun rikollisuuteen (Holt, 2017). Osa tutkijoista on puolestaan hylännyt kyber-sanan kokonaan (Steinmetz & Nobles, 2018), ja käyttävät Leman-Langloisen (2013) muodostamaa termiä ”teknorikollisuus” kyberrikollisuuden sijasta, koska kuten jo aiemmin todettu, kyber-sanalla on hankala historia. Huolimatta kyber-sanan hankalasta historiasta, tässä tutkielmassa tullaan käyttämään termiä kyberrikollisuus, koska sillä on vakiintunut asema kyberrikollisuudesta kertovassa kirjallisuudessa. Tässä tutkielmassa käytetään Thomasin ja Loaderin (2000) sekä Yarin ja Steinmetzin (2019) teoksien pohjalta muodostettua määritelmää kyberrikollisuudesta: kyberrikollisuus on mitä tahansa laitonta toimintaa, joka tapahtuu internetissä.

Kyberrikollisuus on yleensä jaettu kahteen osaan, teknologiakeskeisiin ja ei-teknologiakeskeisiin tai tietokonekeskeisiin ja tietokoneavusteisiin (Clough, 2015; Gillespie, 2015; Gillespie, 2019; Kim, Jeong, Kim & So, 2011; Yar & Steinmetz, 2019). Clough (2015) lisää tähän vielä kolmannen osan, tietokonetuetut rikokset, joissa tietokoneen käyttö on vain pieni osa itse rikosta, mutta tietokone voi tarjota todisteita rikoksesta. Kyberrikollisuutta on myös yleensä lokeroitu eri tavoin. Shinder ja Cross (2008) ovat jakaneet kyberrikokset ensin kahteen laajaan osaan, väkivaltaisiin tai potentiaalisesti väkivaltaisiin rikoksiin sekä väkivallattomiin rikoksiin. Ensimmäiseen luokkaan kuuluvat esimerkiksi kyberterrorismi, uhkailu ja kyberseuranta (engl. Cyberstalking), ja toiseen luokkaan kuuluvat kybermurrot, kybervarkaudet- ja huijaukset, tuhoisat kyberrikokset sekä kaikki muut kyberrikokset, jotka eivät sisälly ensimmäiseen luokkaan (Shinder & Cross, 2008).

Kyberrikollisuus voidaan lokeroida informatiivisemmin neljään eri luokkaan ja kolmeen eri kehitysasteeseen (Wall, 2001; Wall, 2002). Ensimmäinen luokka on kybermurto, jossa rikollinen pääsee tietokonejärjestelmien kautta luvatta toisen henkilön verkossa olevaan omaisuuteen käsiksi. Toinen luokka on kyberpetos- ja varkaus, jossa rikollinen varastaa toisen rahaa tai omaisuutta kyberavaruudessa. Kolmas luokka on kyberpornografia, jossa rikolliset jakavat ja vaihtavat laitonta seksuaalista materiaalia kyberavaruudessa. Neljäs luokka on kyberväkivalta, jossa rikolliset aiheuttavat psykologista vahinkoa tai yllyttävät fyysiseen väkivaltaan toisia ihmisiä kohtaan. (Wall, 2001; Yar & Steinmetz, 2019.) Tässä tutkielmassa ei ole tarpeen käydä läpi kyberrikosten vaikutustasoja, joten ne sivuutetaan.

Alla olevaan taulukkoon (taulukko 1) on koottu kyberrikollisuuden neljä luokkaa sekä esitelty niiden määritelmät sekä annettu esimerkit kuhunkin luokkaan liittyvistä rikoksista. Taulukko on muodostettu yhdistelemällä kirjal-

lisuudessa mainittuja kyberrikollisuuden luokkia ja niiden määritelmiä sekä rikoksia, jotka kuuluvat näihin luokkiin (Shinder & Cross, 2008; Wall, 2001; Wall, 2002; Wall, 2003; Yar & Steinmetz, 2019).

TAULUKKO 1 Kyberrikollisuuden luokat

Kategoria	**Kybermurrot**	**Kyberpetokset- ja varkaudet**	**Kyberpornografia**	**Kyberväkivalta**
Määritelmä	Luvaton pääsy muiden ihmisten kyberavaruudessa olevaan omaisuuteen ja/tai vahinkojen aiheuttaminen	Kyberavaruudessa tapahtuvat varkaudet (raha, omaisuus)	Laittoman seksuaalisen materiaalin julkaisu tai vaihto kyberavaruudessa	Psykologisen vahingon aiheuttaminen, yllyttäminen fyysiseen väkivaltaan toisia kohtaan
Esimerkkejä	Hakkerointi, virukset, roskaposti, palvelunestohyökkäys, kybervandalismi, kyberterrorismi	Petokset, plagiointi, pyramidihuijaukset, sähköpostihuijaukset, liikesalaisuuksien varastaminen, identiteettivarkaus, tietojenkalastelu	Seksikauppa internetissä, kyberseksi, kyberprostituutio	Yleinen vihapuhe, toisen häirintä, kohdennettu vihapuhe

Seuraavaksi määritellään muutamia keskeisimpiä kyberrikoksia. Tässä tutkielmassa tullaan keskittymään kahteen ensimmäiseen kyberrikollisuuden luokkaan, kybermurtoihin ja kyberpetoksiin- ja varkauksiin, koska digitaaliseen terveydenhuoltoon kohdistuvat rikokset kuuluvat yleensä näihin kahteen edellä mainittuihin luokkiin. Kaikkia kyberrikoksia ei käydä läpi, mutta yleisimmät muodot on hyvä avata lukijalle.

Tietokonevirukset ovat yksi vanhimmista haittaohjelmien muodoista. Virukset tekevät kopioita itsestään ja leviävät saastuttamalla esimerkiksi tiedostoja tai ohjelmia. (Furnell, 2011; Holt ym., 2017.) Tietokonevirus tekee mitä se on ohjelmoitu tekemään, oli se viestin näyttö ponnahdusikkunalla, tietojen poisto tai muokkaus tai muiden haittaohjelmien, kuten troijalaisten asentaminen tietokoneelle (Clough, 2015).

Mato (engl. Worm) on haittaohjelman muoto, joka tekee kopioita itsestään (Shinder & Cross, 2008). Mato eroaa perinteisistä tietokoneviruksista siinä mielessä, että ne voivat levitä itsenäisesti, ilman että madon täytyisi saastuttaa toista ohjelmaa (Clough, 2015). Mato voi esimerkiksi käyttää tietokoneen muistia levitäkseen (Holt ym., 2017). Mato voi tulla tietokoneeseen esimerkiksi sähköpostin liitetiedoston mukana, jonka käyttäjä on aukaissut (Furnell, 2011).

Troijalainen (engl. Trojan horse) on vaarattoman näköinen ohjelma, joka toimii ilman että käyttäjällä on tietoa siitä, aiheuttaen yleensä ikäviä seurauksia. Tällaiset ohjelmat saattavat näyttää päällisin puolin luotettavilta, mutta todellisuudessa kyseessä onkin haittaohjelma, joka tekee taka-alalla muuta, ja troija-

laiset voivatkin asentaa tietokoneeseen esimerkiksi tietokoneviruksia, matoja tai kiristyshaittaohjelmia. (Clough, 2015; Furnell, 2011; Shinder & Cross, 2008.)

Kiristyshaittaohjelma (engl. Ransomware) on haittaohjelmatyyppi, joka lukitsee järjestelmiä ja tiedostoja, eikä niihin pääse käsiksi ennen kuin lunnaat on maksettu (Holt ym., 2017; Vuletić, 2018). Kiristyshaittaohjelmat muistuttavat troijalaisia, sillä ne leviävät ladattavien tiedostojen tai nettisivujen välityksellä (Holt ym., 2017). Kiristyshaittaohjelmat ovat yleistyneet viime vuosina ja ovatkin nykyisin kaikkein tuhoisin ja häiritsevin haittaohjelmamuoto, aiheuttaen suuria kustannuksia organisaatioille ja yrityksille vuosittain (Yar & Steinmetz, 2019).

Vakoiluohjelma (engl. Spyware) on ohjelma, joka pyrkii keräämään arkaluontoista tietoa käyttäjästä ja käyttäjän toimista hänen tietokoneellaan, ja nämä tiedot voivat mahdollisesti lopulta päätyä toisille osapuolille (Clough, 2015; Furnell, 2011). Vakoiluohjelmat voivat esimerkiksi tallentaa käyttäjän näppäimistön painalluksia tai aiheuttaa muunlaista häiriötä, kuten luomaan kirjainmerkkejä verkkosivuille, luomaan ponnahdusikkunoita, joissa on mainoksia tai ohjaamaan käyttäjä verkkosivuille, joille ei ole tarvetta mennä (Clough, 2015).

Roskaposti on yleinen riesa internetissä. Roskaposti viittaa ilmoituksiin tai postiin, jota saadaan yleensä sähköpostin välityksellä. Muita roskapostin muotoja ovat tekstiviestit ja toistuvat automaattiset puhelinsoitot. Roskapostin välityksellä pyritään usein huijaamaan vastaanottajaa tai levittämään haittaohjelmia, kuten tietokoneviruksia ja troijalaisia. (Clough, 2015; Kim, Jeong, Kim & So, 2011.)

Hakkerointi on muiden ihmisten tietokoneisiin tunkeutumista. Internet on mahdollistanut kyberrikollisille pääsyn toisten tietokoneisiin ilman fyysistä kontaktia itse tietokoneeseen. Hakkeroinnilla pyritään yleensä saamaan pääsy arkaluontoisiin tietoihin, varastamaan rahaa tai digitaalista omaisuutta, tuhoamaan tietoja tai aiheuttamaan ongelmia tietojärjestelmiin. (Clough, 2015; Kim, Jeong, Kim & So, 2011.)

Palvelunestohyökkäyksen (engl. Denial of Service, DoS) tarkoituksena on luoda suuri määrä tekaistuja pyyntöjä yhteen ja samaan tietokoneeseen tai serveriin, jotta se ei pystyisi tarjoamaan palvelujaan normaalisti tietokoneen käyttäjille ja palvelun omistajalle (Clough, 2015; Holt ym., 2017; Kim, Jeong, Kim & So, 2011; Yar & Steinmetz, 2019). Perinteisessä palvelunestohyökkäyksessä käytetään yleensä yhtä tietokonetta hyökkäyksen toteuttamiseen. Nykyisin kuitenkin on vaikeaa kuormittaa järjestelmiä vain yhdellä tietokoneella, koska käytössä ovat suuret tiedonsiirtonopeudet ja laskentateho sekä erilaiset palvelut palvelunestohyökkäyksien vähentämiseksi. (Yar & Steinmetz, 2019.) Siksi on yhä yleisempää, että palvelunestohyökkäyksiä toteutetaan hajautetusti, käyttäen useita eri tietokoneita. Hajautettu palvelunestohyökkäys (engl. Distributed Denial of Service, DDoS) toteutetaan bottiverkoksi kutsutun haittaohjelman avulla. Bottiverkot toimivat samantyylisesti kuin troijalaiset ja virukset, ja kun kyseinen haittaohjelma on aktiivinen tietokoneessa, hyökkääjä voi käyttää kyseistä tietokonetta etänä omalta päätelaitteeltaan. Jokainen saastunut tietokone ottaa yhteyttä rikollisen omaan päätelaitteeseen, ja näin rikollinen voi valjastaa nämä

tietokoneet hajautetun palvelunestohyökkäyksen toteuttamiseen. (Holt ym., 2017.) Bottiverkkoja voidaan käyttää myös haittaohjelmien ja roskapostin massajakeluun (Clough, 2015).

Tietojenkalastelulla (engl. Phishing) pyritään huijaamaan internetin käyttäjä sellaisille verkkosivuille, jotka ovat todellisuudessa vain hyvin tehtyjä kopioita oikeista verkkosivuista. Yleensä pankkien, luottokorttiyhtiöiden tai suosittujen sosiaalisten verkkosivustojen sivustoista tehdään oikean näköisiä kopioita. Näillä sivustoilla pyritään saamaan käyttäjä syöttämään arkaluontoisia tietoa kuten käyttäjänimiä, salasanoja ja pankkitunnuksia, jotka päätyvät rikollisten haltuun. (Kim, Jeong, Kim & So, 2011.) Toisaalta tietojenkalastelulla voidaan myös tarkoittaa toimintaa, jossa kyberrikollinen lähettää massoittain sähköpostiviestejä potentiaalisille uhreille saadakseen heiltä arkaluontoisia tietoja, joita voidaan käyttää esimerkiksi identiteettivarkauksiin tai petoksiin. Sähköpostissa voi olla myös linkki sivuille, jotka näyttävät oikeilta, mutta ovat tosiasiassa vain kopioita. (Holt ym., 2017; Yar & Steinmetz, 2019.) Tietojenkalastelua voidaan toteuttaa myös tekstiviestien ja puhelinsoittojen kautta (Yar & Steinmetz, 2019).

Identiteettivarkaudessa pyritään hankkimaan uhrin henkilökohtaisia tietoja, kuten nimi, syntymäaika, sosiaaliturvatunnus, henkilötunnus tai muu numerosarja, jolla voidaan tunnistaa ihminen, sekä muita tunnistetietoja. Identiteettivarkauden avulla pyritään yleensä tehtailemaan erilaisia petoksia. (Yar & Steinmetz, 2019.)

Nyt kun käsitteet ja määritelmät ovat tulleet tutuiksi, seuraavaksi voidaan siirtyä käsittelemään, miten kyberrikollisuus uhkaa digitaalista terveydenhuoltoa.

3 KYBERRIKOLLISUUDEN AIHEUTTAMAT UHAT DIGITAALISELLE TERVEYDENHUOLLOLLE

Tässä kappaleessa käsitellään uhkia, joita kyberrikollisuus aiheuttaa terveydenhuoltoalalle. Ensiksi käydään läpi, miksi terveydenhuoltoala on kyberrikollisten kohteena, ja esitellään myös muutamia rikoksia tarkemmin. Sen jälkeen käydään läpi sitä, miten kyberrikolliset käyttävät saamiaan tietoja. Niiden jälkeen käydään läpi digitaalisen terveydenhuollon haavoittuvaisuuksia, ja lopuksi tulokset tiivistetään sekä esitetään johtopäätöksiä.

3.1 Digitaaliseen terveydenhuoltoon kohdistuvat kyberrikokset

Terveydenhuollon ala on ollut jo muutaman vuoden ajan kasvavan kyberrikollisuuden kohteena. Sairaaloiden tietojärjestelmät ovat houkutteleva kohde kyberrikollisille, sillä ne sisältävät paljon arvokasta dataa ja ne ovat yleensä helppo kohde. Siinä missä esimerkiksi rahoituksen ja kaupan alat ovat olleet jo pitkään kyberrikollisuuden kohteena, ja ovat kehittäneet jo hyvät puolustuskeinot kyberrikoksia vastaan, niin terveydenhuoltoala on vasta viime vuosina joutunut kyberrikollisuuden uhriksi ja siten terveydenhuoltoalalla ei ole ollut riittävästi aikaa kehittää hyviä keinoja kyberhyökkäyksiä vastaan. (Argaw ym., 2020; Martin, Martin, Hankin, Darzi, Kinross, 2017; Vuletić, 2018.) Sen lisäksi kyberrikolliset ottavat sairaaloiden tietojärjestelmiä kohteikseen koska sairaalat yleensä maksavat lunnaat saadakseen tietonsa tai järjestelmänsä takaisin käyttöön (Vuletić, 2018). Sairaaloiden kyberturvallisuus ei ole ajan tasalla, ja siksi se onkin nyt yksi eniten kyberhyökkäyksiä saava ala (Argaw ym., 2020; Coventry & Branley, 2018; Martin ym., 2017). Lääkärit ovat pitäneet tietoteknisiä ongelmia yleensä vain tietotekniikkaan liittyvänä asiana. Yhteyksiin, käytettävyyteen ja lyhytaikaisiin, järjestelmän alhaalla oloon liittyvät tapahtumat vaikuttavat tehokkuuteen ja käyttäjätyytyväisyyteen, mutta niitä ei yleensä pidetä riskeinä potilaan hoidossa. (Jarrett, 2017.)

Kyberrikollisuuden aiheuttamat uhat voidaan jakaa neljään eri osaan: tietomurtoihin, taloudellisiin tappioihin, hyökkäykset terveydenhuollossa käytettäviä laitteita vastaan ja hyökkäykset terveydenhuollon infrastruktuuria vastaan (Perakslis, 2014).

Potilasrekisterit sisältävät paljon erilaisia potilastietoja, joihin rikolliset haluavat päästä käsiksi. Näitä tietoja ovat muun muassa potilaan nimi, puhelinnumero, sähköpostiosoite, tiedot menneistä leikkauksista ja diagnooseista, veriryhmä sekä muut henkilökohtaiset terveystiedot (Argaw ym., 2020; Mishra, Ghosh & Mishra, 2019). Potilastietoihin pääsy aiheuttaa monenlaista päänvaivaa potilaille, sillä terveystiedot ovat henkilökohtaisia ja korvaamattomia, eikä niitä voi vaihtaa samalla tavalla kuin varastettua luottokorttia tai ajokorttia. Siinä missä luottokortin voi kuolettaa ja hankkia sen jälkeen uuden luottokortin, niin esimerkiksi veriryhmää ei voi vaihtaa. (Argaw ym., 2020; Kwon & Johnson, 2015; Luh & Yen, 2020.)

Tietovuodot ovat yleinen tapa, jolla rikolliset pääsevät käsiksi potilastietoihin. Tietovuotoja tapahtuu yleensä, jos sairaalan tietoverkkoon pääsee käyttäjätietoja keräävä haittaohjelma tai jos sairaalan työntekijä kadottaa kannettavan tietokoneensa (McLeod & Dolezel, 2018; Vuletić, 2018). On myös mahdollista, että sairaalan työntekijä itse vuotaa tietoja tai käyttää sairaalan tietoverkkoa palvelunestohyökkäyksen toteuttamiseen (Vuletić, 2018).

Rikolliset voivat saada käsiinsä potilaiden terveystietoja muualtakin kuin vain sairaaloiden tietojärjestelmistä. Internetin sosiaalisissa medioissa sekä terveyteen liittyvillä verkkosivuilla käyttäjät jakavat henkilökohtaisia terveystietojaan muiden kanssa. Nämä sosiaalisen median applikaatiot sekä muut verkkosivut ovat alttiita muun muassa tietojenkalasteluyrityksille, haittaohjelmille, viruksille, vakoiluohjelmille ja madoille (Li, 2015). Tämä johtuu yleensä palveluntarjoajien riittämättömästä käyttäjätietojen suojauksesta, ja tietojen salaus on yleensä puutteellista (Lupton, 2017). Verkkosivujen ja sosiaalisen median lisäksi ongelmia esiintyy myös terveys- ja kuntosovelluksissa, joita voi ladata älypuhelimiin. Näiden sovellusten salaus on puutteellista, ja vain harvat sovellukset salaavat käyttäjiensä viestit, kun he käyttävät sovellusta (McCarthy, 2013). Siksi kolmannet osapuolet voivat päästä helposti käsiksi käyttäjien tietoihin, jotka ovat tallennettuina terveyssovelluksiin (Lupton, 2017).

Kiristyshaittaohjelmat ovat suuri ongelma terveydenhuoltoalalla. Jo ensimmäinen tunnettu kiristyshaittaohjelma vuonna 1989 kohdistui terveydenhuoltoalaa vastaan (Jayanthi, 2016). Nämä ohjelmat voivat kaapata valtavia määriä dataa, mikä voi hidastaa potilaiden hoitoa pitkäksikin aikaa, jollei tietoja saada palautettua (Jarrett, 2017). Kiristyshaittaohjelmat voivat viivästyttää potilaiden leikkauksia, ja jos potilastiedot ovat lukittuina, lääkärit eivät pääse niihin käsiksi, eivätkä pysty tarkistamaan esimerkiksi potilaiden senhetkisiä allergioita tai lääkityksiä (Argaw ym., 2020). Potilaita voidaan joutua siirtämään toisiin sairaaloihin, jotta he saisivat hoitoa (Argaw ym., 2020; Jarrett, 2017). Kiristyshaittaohjelmia levittävät tavallisten rikollisten lisäksi rikollisorganisaatiot, jotka pyrkivät siten virtuaalisesti kiristämään yleensä lääkeyritystä tai sairaalaa mak-

samaan lunnaat vastineeksi tutkimustuloksista tai potilastiedoista (Monnet & Very, 2017).

Laajat palvelunestohyökkäykset voivat estää tehokkaasti lääkäreiden pääsyn sähköisessä muodossa oleviin terveystietoihin (Jarrett, 2017; Monnet & Very, 2017; Vuletić, 2018). Palvelunestohyökkäykset voivat estää myös potilaiden pääsyn esimerkiksi terveyspalveluntarjoajan verkkosivuille.

Erilaiset petokset aiheuttavat erisuuruisia kustannuksia terveydenhuollolle (Vuletić, 2018). Jos sairaalan työntekijä ei ole tarkkana sähköposteja lukiessaan, ja erehtyy vastamaan sähköpostiin tai tilaamaan lääkkeitä, voivat nämä aiheuttaa esimerkiksi taloudellisia tappioita, kun tilattuja lääkkeitä ei olekaan olemassa. Pahimmassa tapauksessa haittaohjelma voisi saastuttaa koneen ja levitä sitä kautta sairaalan tietoverkkoon, jos työntekijä avaa huolimattomuuttaan sähköpostin liitetiedoston.

Tulevaisuudessa siintää uusi potentiaalinen uhka, mitä Vuletić (2018) kutsuu nimellä ihmishaittaohjelma (engl. Human malware). Näissä tapauksissa ihmisen kehoon asennettuihin laitteisiin tulisi haittaohjelma, kuten troijalainen tai tietokonevirus, joka vaikuttaisi haitallisesti laitteen toimintaan. Kyberhyökkäykset puettaviin sekä kehoon implantoituihin laitteisiin voivat aiheuttaa vakavia turvallisuusongelmia (Li, Raghunathan & Jha, 2011; Perakslis, 2014), ja tällaisten digitaalisten laitteiden hakkerointi on mahdollista (Alexander, Haseeb & Baranchuk, 2019).

Kehoon asennettavat laitteet käyttävät yleensä langattomia yhteyksiä (Giansanti, 2021; Kramer & Fu, 2017), ja jos rikolliset pääsevät käsiksi esimerkiksi sellaiseen langattomaan verkkoon, johon kyseinen laite on yhdistetty, hyökkääjät voivat murtautua asennettuun laitteeseen ja siirtää tietokonevirus tai muu haittaohjelma kyseiseen laitteeseen (Milliken, Selis & Marshall, 2013; Vuletić, 2018). Rikolliset voisivat myös muuttaa laitteen tietoja tai syöttää tarkoituksella väärää dataa laitteeseen. Esimerkiksi sydämentahdistimen akku voidaan tyhjentää nopeasti tai sydämentahdistin voisi antaa aiheettoman elektronisen pulssin aiheuttaen vaarallista värinää sydämessä (Giansanti, 2021; Kintzlinger & Nissim, 2019; Kuehn, 2018). Automaattinen insuliininjakosysteemi voisi syöttää kehoon suuren määrän insuliinia, mikä johtaisi matalaan verensokeriin, johon ihmiskeho vastaisi puolestaan vapauttamalla glukagonia. Lopulta kierre alkaisi vaikuttamaan haitallisesti esimerkiksi aivotoimintaan. (Giansanti, 2021.) Seuraukset voivat olla vakavia ja johtaa jopa potilaan kuolemaan, jos potilaan laite, esimerkiksi sydämentahdistin, lakkaa toimimasta (AlTawy & Youssef, 2016; Giansanti, 2021; Vuletić, 2018). Ihmishaittaohjelmat voisivat häiritä esimerkiksi laitteen ohjelmiston päivittämistä turvallisuusaukon paikkaamiseksi. Toisaalta tällä hetkellä tunnetuilla teknologioilla esimerkiksi sydämentahdistimeen kohdistuvan hyökkäyksen todennäköisyys on varsin pieni, sillä hyökkääjän pitäisi olla lähietäisyydellä uhrin kanssa (AlTawy & Youssef, 2016; Kuehn, 2018). Yhtään onnistunutta hyökkäystä ihmiskehoon asetettuihin laitteisiin ei ole vielä onnistuttu loppuun asti toteuttamaan reaalimaailmassa, mutta useita onnistuneita hyökkäyksiä on toteutettu laboratorioissa (muun muassa Halperin ym., 2008b; Li ym., 2011). Ihmishaittaohjelmien uhka

onkin tällä hetkellä varsin vähäinen, mutta teknologian ja lääkinnällisten laitteiden langattomien yhteyksien kehittyessä tulee nämä uhkamahdollisuudet ottaa huomioon laitekehityksessä.

3.2 Rikoksista saatujen tietojen käyttökohteet

Onnistuneen tietomurron jälkeen rikolliset laittavat saadut tiedot käyttöön. Mutta mihin rikolliset keräävät tai käyttävät saamiansa tietojaan? Kyberrikolliset voivat esimerkiksi sairaalan tai apteekin tietojärjestelmään päästyään muuttaa potilaiden lääkkeiden annoskokoa, joka voi johtaa pahimmassa tapauksessa potilaan kuolemaan (Monnet & Very, 2017), jos väärä annos jaetaan potilaalle tai asiakkaalle. Yleensä rikolliset kuitenkin hakevat vain potilastietoja käyttöönsä.

Jos rikolliset onnistuvat saamaan käsiinsä potilastietoja, ne laitetaan yleensä myyntiin pimeään verkkoon (engl. Dark web), eli tällä tavalla pyritään samaan taloudellista hyötyä. Potilastiedot ovat haluttua tavaraa varsinkin Yhdysvalloissa, koska ne sisältävät monia vakituisia tunnistetietoja sekä taloudellisia tietoja (Martin ym., 2017). Niistä maksetaankin hyvin esimerkiksi verrattuna luottokorttitietoihin (Vuletić, 2018; Zeadally ym., 2016), jopa 10–20 kertaa enemmän (Argaw ym., 2020; Lupton, 2017; Williams, Chaturvedi & Chakravarthy, 2020).

Kun potilastietoja saadaan identiteettivarkaudessa, voidaan puhua lääketieteellisestä identiteettivarkaudesta (engl. Medical identity theft) (Camp & Johnson, 2012). Potilastiedot ostanut henkilö voi käyttää niitä hyväkseen saadakseen esimerkiksi terveydenhoitoa, johon henkilöllä itsellään ei ole varaa, mikä puolestaan voi muuttaa alkuperäisen potilaan hoitohistoriaa sekä muita tietoja kuten esimerkiksi allergioita tai reseptejä, minkä lisäksi myös hoitolasku jää yleensä uhrin maksettavaksi, joka ei ole terveyspalveluita käyttänytkään (Camp & Johnson, 2012; Coventry & Branley, 2018; Jarrett, 2017). Potilastietojen muuttuminen voi aiheuttaa vakavia seurauksia tietojen oikeille omistajille, jos ne jäävät huomaamatta, ja terveystietojen korjaaminen ennalleen on aikaa vievää ja työlästä (Camp & Johnson, 2012). Kyberrikolliset voivat myös käyttää tietoja väärennettyjen henkilöllisyystodistuksien tekemiseen, joiden avulla he voivat ostaa terveydenhoidossa käytettäviä digitaalisia laitteita tai lääkkeitä, jotka he laittavat myyntiin pimeään verkkoon tai he voivat tehdä väärennettyjä vakuutusvaatimuksia (Camp & Johnson, 2012; Coventry & Branley, 2018; Lupton, 2017). Lääketieteellisistä identiteettivarkauksista on tullut ongelma varsinkin Yhdysvalloissa, sillä näiden raportointi ja seuranta on vähäistä, toisin kuin esimerkiksi perinteisemmän identiteettivarkauden tapauksessa, joissa rikollinen käyttää yleensä uhrin luottokorttitietoja hankkiakseen voittoa. Terveystietojen avulla rikollinen voi puolestaan hankkia hoitoa ja hoitotarvikkeita tuhansien ja jopa miljoonien dollarien edestä, ennen kuin asia huomataan. (Camp & Johnson, 2012.)

Potilastiedot voivat kiinnostaa myös epäeettisesti toimivaa vakuutusyhtiötä, joka ostaa kyberrikolliselta potilastietoja ja pyrkii siten vaikuttamaan siihen, keitä yritys valitsee asiakkaikseen. Kilpailevat lääkeyritykset voivat myös ostaa kyberrikollisten varastamia, toisien lääkeyrityksien tieteellisiä tutkimustuloksia tai muuta dataa, jonka he katsovat hyödyttävän heitä. (Monnet & Very, 2017.)

Potilaiden puettavista sekä kehoon asetetuista laitteista saadut tiedot voivat myös aiheuttaa potentiaalisesti mielenkiintoisia seurauksia. Henkilökohtaiset kehoon asetetut laitteet, kuten sydämentahdistimet, yleensä sisältävät tietoja laitteesta sekä potilaasta. Potilaan nimi, tunnistenumero, hoitohistoria ja muita potilaan terveyteen liittyviä tietoja voi olla laitteen muistissa. Lisäksi laite tallentaa terveyteen liittyvää dataa, kuten sykettä sekä laitteen operointihistoriaa, kuten aikaa milloin automaattista defibrillaatiota on käytetty. (Gasson & Koops, 2013; Kintzlinger & Nissim, 2019.) Jos näiden laitteiden suojaus on huonosti suunniteltu, kyberrikolliset voivat henkilökohtaisten laitteiden kautta hankkia henkilökohtaisia tietoja. Lisäksi laitteesta on mahdollista kerätä laitetietoja, ja tällaisten tietojen hankinta voi olla arvokasta esimerkiksi kilpaileville laitevalmistajille (Kintzlinger & Nissim, 2019), jotka haluavat tietoonsa toisten laitevalmistajien laitteiden ominaisuuksia.

3.3 Digitaalisen terveydenhuollon haavoittuvuudet

Miksi terveydenhuoltoala kohtaa kasvavassa määrin kyberrikoksia? Suurin riskitekijä on se, ettei terveydenhuollossa ole investoitu riittävästi tietotekniseen infrastruktuuriin ja kyberturvallisuuteen (Coventry & Branley, 2018; Kwon & Johnson, 2015; Martin ym., 2017). Terveydenhuollon organisaatiot saattavat käyttää vain 1–2 % vuotuisesta budjetistaan tietotekniikkaan, ja käyttävät edelleen vanhoja järjestelmiä, joiden tuki on loppunut jo vuosia sitten, kuten Windows XP käyttöjärjestelmää, jonka tukemisen Microsoft lopetti vuonna 2014 (Coventry & Branley, 2018; Martin ym., 2017). Lisäksi esimerkiksi Yhdysvalloissa vallitsee epätietoisuus eri terveydenhuollon palveluntarjoajien investoinneista kyberturvallisuuteen, ja asiakas ei yleensä tiedä kuinka hyvin mikäkin terveyspalveluntarjoaja on panostanut kyberturvallisuuteen. Tämä epäsymmetrinen informaatio asiakkaiden ja terveyspalveluiden tarjoajien välillä antaa terveyspalveluntarjoajille mahdollisuuden olla investoimatta kyberturvallisuuteen, sillä asiakkaat eivät voi arvioida ja vertailla tehokkaasti terveyspalveluntarjoajien turvallisuutta. (Kwon & Johnson, 2015.) Lisäksi terveydenhuoltoalalla ei välttämättä ole yksinkertaisesti rahaa investoida riittävästi kyberturvallisuuteen, ja esimerkiksi kyberturvallisuuden ammattilaisten tarjoamat palvelut voivat olla hyvinkin kalliita (Martin ym., 2017).

Toinen ongelma on terveydenhuollossa käytettävien digitaalisten laitteiden turvallisuusongelmat. Näissä laitteissa on yleensä vain laitekohtaista ohjelmistoa (engl. Firmware), mikä eroaa normaaleista käyttöjärjestelmistä siten, että tällainen laiteohjelmisto tarjoaa vain tietyn tyyppisiä palveluita, eikä niitä usein suunnitella turvallisuus edellä (Kramer & Fu, 2017; Shwartz, Mathov,

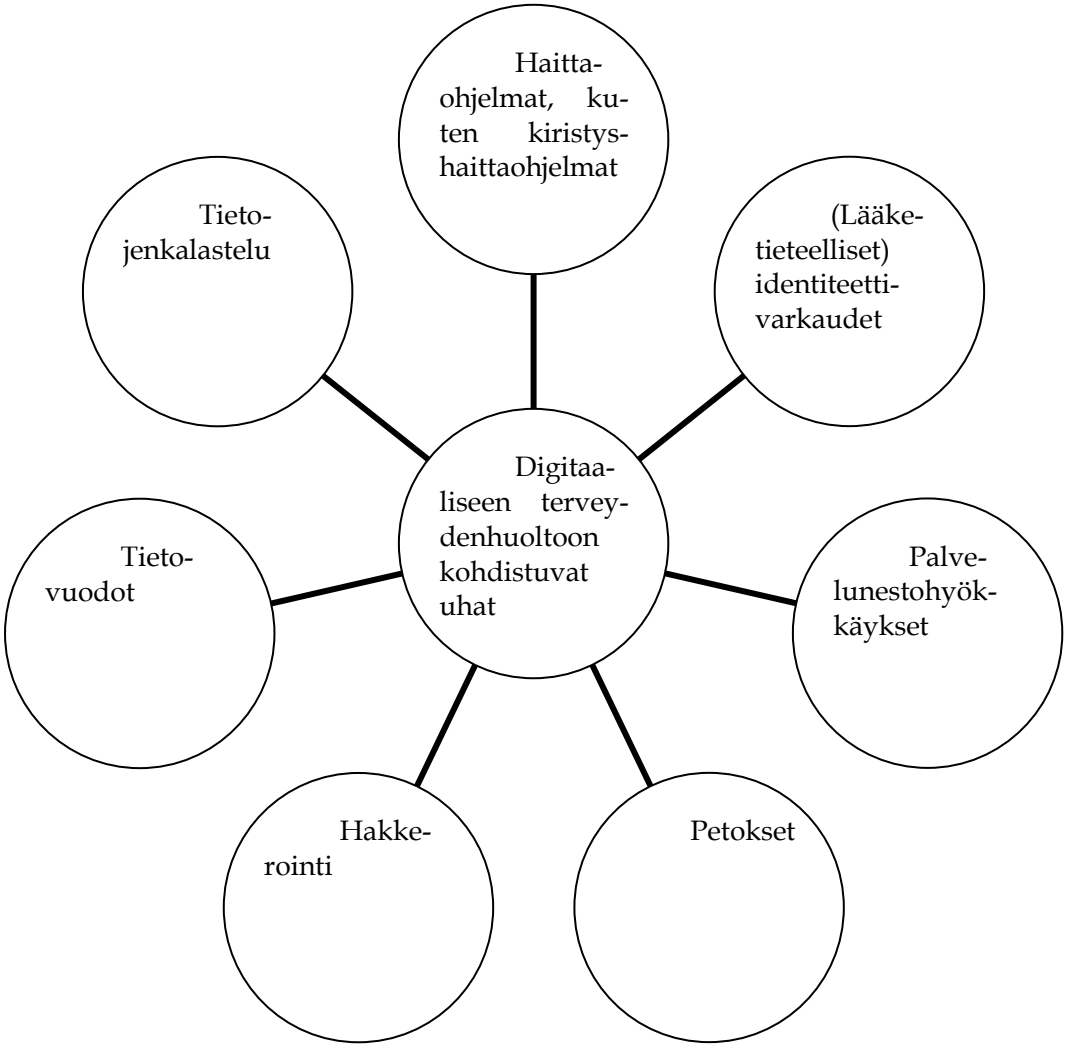
Bohadana, Elovici & Oren, 2017). Tämä johtuu yleensä siitä, että esimerkiksi laitteen akun elinikä vähenisi huomattavasti, jos laitteessa olisi sellaisia ominaisuuksia, kuten hyvä salaus tai haittaohjelmien tunnistaminen (Argaw ym., 2020; Halperin, Heydt-Benjamin, Fu, Kohno & Maisel, 2008a). Toisaalta vahvat salausmenetelmät voivat estää potilaan tunnistamisen sellaisissa tapauksissa, joissa potilas on tuotu tajuttomana ja yksin sairaalaan onnettomuuden jälkeen (Halperin ym., 2008a). Lisäksi terveydenhuollossa käytettävien internetiin yhdistettyihin laitteiden määrä vain kasvaa, ja jo yhden laitteen saastuminen voi vaarantaa esimerkiksi sairaalan tietoverkon. Potilaiden jatkuva monitorointi digitaalisten laitteiden avulla sairauksien ehkäisemiseksi aiheuttaa myös omat ongelmansa, sillä nämä laitteet keräävät paljon dataa. (Coventry & Branley, 2018.) Lisäksi laitteiden suojaus voi olla puutteellista, sillä sairaalat eivät välttämättä voi vaikuttaa näiden laitteiden turvallisuuteen, varsinkin jos laitteita ostetaan useilta eri laitevalmistajilta (Coventry & Branley, 2018; Fayans, Motro, Rokach, Oren & Moran-Gilad, 2020). Mobiililaitteiden lisääntynyt käyttö terveyden parantamisessa tai monitoroimisessa lisää myös omat ongelmansa, sillä älypuhelimien käyttäjät eivät välttämättä panosta laitteidensa turvallisuuteen (Coventry & Branley, 2018).

Ihmiset ovat kyberturvallisuuden heikoin lenkki, joten terveydenhuollossakin olisi hyvä ottaa käyttöön koulutustapahtumia, jotka lisäävät tietoisuutta kyberuhista (Argaw ym., 2020). Lisäksi olisi puututtava sairaaloiden turvallisuuskulttuuriin, sillä edelleen terveydenhuollon työntekijät jättävät liimattavia muistilappuja tietokoneiden ja digitaalisten laitteiden läheisyyteen (Koppel, Smith, Blythe & Kothari, 2015). Osassa sairaaloista muistilappuja kirjoitetaan myös lukittujen tilojen oviin, jotta hoitajat pääsevät tarvittaessa sisään tiloihin, eivätkä tuhlaa aikaa ovikoodien muistamiseen (Koppel ym., 2015).

3.4 Tulokset ja johtopäätökset

Digitaalista terveydenhuoltoa uhkaava kyberrikollisuus on potentiaalisesti vaarallista terveydenhuoltopalveluita käyttäville asiakkaille. Tässä tutkielmassa todettiin, että digitaaliseen terveydenhuoltoon kohdistuu useita eri kyberrikoksia. Argaw ym. (2020), Jarrett (2017) sekä Monnet ja Very (2017) havaitsivat kiristyshaittaohjelmia. Vuletić (2018) havaitsi petoksia. McLeod ja Dolezel (2018) sekä Vuletić (2018) havaitsivat tietovuotoja. Jarrett (2017), Monnet ja Very (2017) sekä Vuletić (2018) havaitsivat palvelunestohyökkäyksiä. Alexander ym. (2019) sekä Li ym. (2011) havaitsivat hakkerointia. Li (2015) sekä Lupton (2017) havaitsivat tietojenkalastelua ja Camp ja Johnson (2012), Coventry ja Branley sekä Lupton (2017) havaitsivat lääketieteellisiä identiteettivarkauksia. Tulevaisuudessa uusi potentiaalinen uhka, ihmishaittaohjelmat, voivat häiritä terveydenhoidossa käytettyjen digitaalisten laitteiden käyttöä vaarallisella, jopa kuolettavalla tavalla, jos laitteen toiminta estetään. Seuraavalla kuviolla (kuvio 1) voidaan paremmin havainnollistaa kyberrikoksia, jotka kohdistuvat digitaaliseen

terveydenhuoltoon. Kuvio on muodostettu luvussa 3.1 löydettyjen tuloksien pohjalta.



KUVIO 1 Digitaaliseen terveydenhuoltoon kohdistuvat kyberrikokset

Kyberrikosten kirjo on mittava, joita vastaan terveydenhuoltoalan on puolustauduttava. Tehokas keino vähentää edellä mainittujen uhkien realisoitumista olisivat terveydenhuollon ammattilaisten koulutustapahtumat, joissa selitettäisiin esimerkkien avulla, miten kyberrikokset yleensä tapahtuvat ja mitkä niiden seuraukset ovat.

Kyberrikolliset käyttävät varastamiaan tietojaan esimerkiksi lääketieteellisiin identiteettivarkauksiin, ja näiden tietojen avulla he voivat ostaa lääkkeitä tai jopa saada itse hoitoa. Kyberrikolliset voivat myös myydä tiedot eteenpäin pimeillä markkinoilla. Epäeettiset lääkeyritykset voivat ostaa lääkinnällisten laitteiden laitetietoja, joiden avulla he parantavat omia vastaavia laitteitaan, ja vakuutusyhtiöt voivat käyttää potilastietoja asiakkaidensa valikoimiseen. Seuraavalla taulukolla (taulukko 2) voidaan havainnollistaa tietojen käyttökohteita

sekä ketkä niitä hankkivat. Taulukko on muodostettu luvussa 3.2 käytettyjen lähteiden pohjalta (Camp & Johnson, 2012; Coventry & Branley, 2018; Kintzlinger & Nissim, 2019; Monnet & Very, 2017; Lupton, 2017).

TAULUKKO 2 Tietojen käyttökohteet

Käyttäjä	Rikollinen	Lääkeyritys	Vakuutusyhtiö
Miten hankittu	Hakkerointi, tietovuodot, kiristyshaittaohjelmat, tietojenkalastelu, pimeät markkinat	Pimeät markkinat	Pimeät markkinat
Mitä hankittu	Potilastietoja, laitetietoja, tutkimustuloksia	Tietoja kilpailijan digitaalisen laitteen ominaisuuksista, tutkimustuloksia	Potilastietoja, esimerkiksi nimi ja hoitohistoria
Mihin käytetään	(Lääketieteellinen) identiteettivarkaus, terveyspalvelujen hankinta, tietojen myynti, petokset, kiristys	Parannetaan oman vastaavan laitteen ominaisuuksia	Valikoidaan ”paremmin” asiakkaat

Tietojen väärinkäyttöä voisi vähentää vaatimalla jotain muitakin tunnistetietoja hoitoa tai lääkkeitä hankkiessa, kuin vain nimi ja sairausvakuutusnumero tai vastaava tunnistenumerosarja. Lisäksi ihmisten tulisi kiinnittää huomiota siihen, mitä tietoja he jakavat terveyssovelluksissa ja sosiaalisessa mediassa.

Digitaalinen terveydenhuolto on haavoittuvaista, eikä vähiten siitä syystä, että terveydenhuoltoala ei investoi tarpeeksi tietotekniikkaan ja kyberturvallisuuteen, kuten esimerkiksi Coventry ja Branley (2018), Kwon ja Johnson (2015) sekä Martin ym. (2017) totesivat. Jotta tulevaisuuden digitaalinen terveydenhoito olisi turvattu, tarvitaan aktiivisesti päivitettäviä suosituksia, ehkä jopa lainsäädäntöä, antamaan suuntaviivoja turvallisille terveydenhuollossa käytettäville digitaalisille laitteille ja tietojärjestelmille. Sairaaloiden olisi myös hyvä varmuuskopioida aktiivisesti järjestelmiään ja tiedostojaan. Lisäksi kyberhyökkäystilanteiden torjuntasuunnitelma, joka sisältää tarkat toimenpiteet, jotka otetaan käyttöön mahdollisen kyberhyökkäyksen jälkeen, olisi hyvä ottaa käyttöön jokaisessa terveydenhuollon organisaatiossa (Argaw ym., 2020). Terveyssovelluksien käyttäjillä tulisi olla hyvät tiedot omien laitteidensa suojaamiseksi sekä miten toimia, jos epäilee laitteensa joutuneen esimerkiksi haittaohjelman saastuttamaksi.

Kaikki edellä mainittu saattaa pelottaa esimerkiksi potentiaalista asiakasta hakeutumasta terveydenhuollon pariin, jos sitä tarjotaan vain digitaalisesti. Tulevaisuudessa onkin panostettava terveydenhuollossa käytettävien digitaalisten ratkaisujen turvallisuuteen, sekä kannustettava ihmisiä pitämään parempaa huoltoa omista internetiin kytketyistä laitteistaan.

4 YHTEENVETO

Terveydenhuoltoon kohdistuvat kyberrikokset ovat suuri huolenaihe niin potilaille kuin terveydenhuollon ammattilaisillekin. Tämän tutkielman tavoitteena oli valaista lukijalle, mitkä kyberrikokset uhkaavat digitaalista terveydenhuoltoa, miten rikolliset käyttävät saamiansa tietoja, ja mitkä ovat digitaalisen terveydenhuollon sudenkuopat. Tutkielma toteutettiin kirjallisuuskatsauksena, ja lähteiksi valittiin sopivaa kirjallisuutta, kuten tieteellisiä artikkeleita, ja kokoomateoksien artikkeleita. Korkeasti arvostetut julkaisijat olivat julkaisseet suuren osan lähteistä, ja julkaisujen kirjoittajat olivat usein tunnettuja omalla alallaan.

Tässä tutkielmassa haettiin vastauksia seuraaviin tutkimuskysymyksiin:

- Mitkä kyberrikollisuuden muodot uhkaavat digitaalisia terveydenhuoltoa?
- Miten kyberrikolliset ovat käyttäneet tietoja, joihin he ovat päässeet käsiksi?
- Millaisia heikkouksia liittyy digitaaliseen terveydenhuoltoon?

Tutkielma jaettiin neljään eri lukuun: johdantoon, kahteen sisältölukuun ja yhteenvetoon. Ensimmäisessä sisältöluvussa käytiin läpi käsitteitä, ja toisessa sisältöluvussa vastattiin tutkimuskysymyksiin.

Johdannossa lukija tutustutettiin aihepiiriin sekä syihin, miksi tämän aiheen tutkiminen on tarpeellista. Lukijalle avattiin muutamia tutkielmassa esiintyviä käsitteitä tarkemmin auki.

Toisessa luvussa määriteltiin digitaalisen terveydenhuollon, ja kyberrikollisuuden käsitteet. Ilmeni, että molempien käsitteiden määrittely on hankalaa, sillä niille on useita eri määritelmiä. Digitaalinen terveydenhuolto lisäksi sekoitetaan usein sähköisen terveydenhuollon kanssa. On kuitenkin muistettava, että digitaalinen terveydenhuolto on uudempi käsite kuin sähköinen terveydenhuolto, ja voi olla, että nimi on muuttunut kuvaavammaksi digitalisaation edetessä.

Kyberrikollisuus on myös määritelty eri tavoin vuosien varrella, ja sen lisäksi kyber-sana itsessään on joidenkin tutkijoiden mielestä ongelmallinen. Kyberrikollisuus on kuitenkin vakiintunut käsite kirjallisuudessa, ja sitä tullaan

luultavasti käyttämään jatkossakin, vaikka osa tutkijoista kritisoikin kyseisen sanan käyttöä tutkimuksissa. Luvussa käsiteltiin myös kyberrikollisuuden luokkia, ja itse kyberrikoksia.

Kolmannessa luvussa vastattiin tutkimuskysymyksiin omissa alaluvuissaan, ja lopuksi pohdittiin näitä tuloksia sekä vedettiin johtopäätöksiä. Ensimmäisessä alaluvussa todettiin, että digitaalista terveydenhuoltoa uhkaavat monet erilaiset haittaohjelmat, kuten kiristyshaittaohjelmat. Terveydenhuoltoon kohdistetaan kyberhyökkäyksiä, koska se on helppo kohde ja se on investoinut huonosti kyberturvallisuuteen. Kyberrikosten uhkaa voisi vähentää esimerkiksi terveydenhuollon henkilöstön koulutuksella, sekä kannustamalla tavallisia ihmisiä pitämään parempaa huolta digitaalisista laitteistaan.

Toisessa alaluvussa ilmeni, että rikolliset käyttävät saamiansa tietojaan esimerkiksi lääketieteellisiin identiteettivarkauksiin, jonka lisäksi he voivat myydä näitä tietoja eteenpäin pimeillä markkinoilla. Rikollisten lisäksi epäeettiset lääkeyritykset ja vakuutusyhtiöt voivat ostaa potilastietoja tai tutkimustuloksia, joita rikolliset ovat hankkineet.

Kolmannessa alaluvussa havaittiin, että digitaalisen terveydenhuollon heikkoja kohtia ovat muun muassa vähäiset investoinnit yleiseen kyberturvallisuuteen. Lisäksi digitaalisten laitteiden kasvava määrä ja niiden turvallisuusongelmat aiheuttavat ongelmia, jos niiden suojaukseen ei ole panostettu tarpeeksi. Ihmiset itse aiheuttavat myös turvallisuusongelmia, sillä tavallisten käyttäjien mobiililaitteiden suojaus voi olla heikkoa, esimerkiksi jos laitteiden suojaus laiminlyödään tai ladataan epäilyttäviä sovelluksia internetistä. Sairaaloiden turvallisuuskulttuuri aiheuttaa myös riskejä, kun salasanoja ja koodeja jätetään muistilapuilla näkyville paikoille.

Tämän tutkielman tavoitteena on ollut antaa lukijalle hyvä yleiskatsaus siitä, mikä digitaalista terveydenhuoltoa uhkaa, keskittyen kyberrikoksiin. Laaja katsaus digitaalisen terveydenhuollon kohtaamien kyberrikosten laajuuteen, sekä rikollisten saamien potilastietojen käyttöön, ja digitaalisen terveydenhuollon haavoittuvuuksiin antaa syyn ottaa nämä uhat vakavasti.

Kuten jokaisessa tutkielmassa, myös tässä tutkielmassa on rajoitteita. Tämän tutkielman rajoitteita on muun muassa se, että tutkielma on toteutettu täysin kirjallisuuskatsauksena, eikä empiiristä tutkimusta ole toteutettu. Tutkimuskysymykset ovat varsin laajoja, eikä tutkielmassa perehdytty syvällisemmin mihinkään tiettyyn osa-alueeseen, kuten tiettyyn terveydenhuollossa käytettävän laitteen ongelmiin. Lisäksi rikollisten käsiinsä hankkimista potilastiedoista kertova kirjallisuus keskittyi maantieteellisesti enimmäkseen Yhdysvaltoihin, eikä se ole terveydenhuoltojärjestelmänsä erilaisuuden vuoksi suoraan verrattavissa esimerkiksi Pohjoismaihin. Lisäksi tutkielmaan haettu kirjallisuus oli vain englanninkielistä. Tarpeen on myös huomioida, ettei tässä tutkielmassa keskitytty mihinkään maantieteelliseen alueeseen, vaan käsiteltiin kyberrikollisuuden uhkaa digitaaliselle terveydenhuollolle yleisellä tasolla.

Tulevaisuudessa olisi hyvä tutkia lisää terveydenhuollon kyberturvallisuutta, erityisesti tietoverkkojen- ja järjestelmien sekä digitaalisten laitteiden suojaamista. Lisäksi tulisi kiinnittää lisää huomiota kyberrikoksiin ja miten ne

muuttuvat, sillä esimerkiksi uusia haittaohjelmia ja keinoja levittää haittaohjelmia kehitellään jatkuvasti. Epäeettisten lääkeyrityksen sekä vakuutusyhtiöiden osuutta kyberrikoksien toteuttamisessa olisi myös syytä tutkia.

LÄHTEET

Alexander, B., Haseeb, S., & Baranchuk, A. (2019). Are implanted electronic devices hackable?. *Trends in cardiovascular medicine, 29(8),* 476–480.

AlTawy, R., & Youssef, A. M. (2016). Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access, 4,* 959–979.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making, 20(1),* 1–10.

Bender, J. L., Jimenez-Marroquin, M. C., & Jadad, A. R. (2011). Seeking Support on Facebook: A Content Analysis of Breast Cancer Groups. *Journal of medical Internet research, 13(1),* e16.

Bernik, I. (2014). *Cybercrime and cyber warfare*. John Wiley & Sons.

Boric-Lubecke, O., Gao, X., Yavari, E., Baboli, M., Singh, A., & Lubecke, V. M. (2014). E-healthcare: Remote monitoring, privacy, and security. Teoksessa *2014 IEEE MTT-S International Microwave Symposium (IMS2014), (1–3).* IEEE.

Camp, L. J., & Johnson, M. E. (2012). Identity Theft in Healthcare. Teoksessa Camp, L. J., & Johnson, M. E. (toim.), *The Economics of Financial and Medical Identity Theft (s. 61–67).* Springer Science & Business Media.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society.* Oxford University Press on Demand.

Chu, L. F., Shah, A. G., Rouholiman, D., Riggare, S., & Gamble, J. G. (2018). Patient-centric strategies in digital health. Teoksessa Rivas H., Wac K. (toim.), *Digital Health. (s. 43–54).* Springer, Cham.

Clough, J. (2015). *Principles of cybercrime* (2. painos). Cambridge University Press.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. *Maturitas, 113,* 48–52.

Cumming, G. P., French, T., Hogg, J., McKendrick, D., Gilstad, H., Molik, D., & Luciano, J. S. (2017). Trust and provenance in communication to ehealth consumers. Teoksessa Menvielle, L., Audrain-Pontevia, A. F., & Menvielle,

W. (toim.), *The Digitization of Healthcare (s. 189–203).* Palgrave Macmillan, London.

Cunningham, S. G., Wake, D. J., Waller, A., & Morris, A. D. (2014). Definitions of eHealth. Teoksessa Gaddi, A., Capello, F., & Manca, M. (toim.), *eHealth, care and quality of life (s. 15–30).* Springer, Milano.

Elenko, E., Underwood, L., & Zohar, D. (2015). Defining digital medicine. *Nature biotechnology, 33(5),* 456–461.

Fayans, I., Motro, Y., Rokach, L., Oren, Y., & Moran-Gilad, J. (2020). Cyber security threats in the microbial genomics era: implications for public health. *Eurosurveillance, 25(6),* 1900574.

Fricker, S. A., Thümmler, C., & Gavras, A. (toim.). (2015). *Requirements engineering for digital health.* Springer, Cham.

Furnell, S. (2011). Hackers, viruses and malicious software. Teoksessa Jewkes, Y., & Yar, M. (toim.), *Handbook of Internet crime. (s. 173–193).* Routledge.

Gaddi, A., Capello, F., & Manca, M. (toim.). (2014). *eHealth, Care and Quality of Life.* Springer, Milano.

Gasson, M. N., & Koops, B. J. (2013). Attacking human implants: a new generation of cybercrime. *Law, Innovation and Technology, 5(2),* 248–277.

Giansanti, D. (2021). Cybersecurity and the Digital-Health: The Challenge of This Millennium. *Healthcare 9(1),* 62.

Gibson, W. (1984). *Neuromancer.* HarperCollins.

Gillespie, A. A. (2015). *Cybercrime: Key issues and debates.* Routledge.

Gillespie, A. A. (2019). *Cybercime: Key issues and debates* (2. painos). Routledge.

Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008a). Security and privacy for implantable medical devices. *IEEE pervasive computing, 7(1),* 30–39.

Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., ... & Maisel, W. H. (2008b). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. Teoksessa *2008 IEEE Symposium on Security and Privacy (sp 2008)* (129–142).

Holt, T. J. (2017). Situating the problem of cybercrime in a multidisciplinary context. Teoksessa Holt, T. J. (toim.), *Cybercrime Through an Interdisciplinary Lens. (s. 1–14).* Routledge.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). *Cybercrime and Digital Forensics: An Introduction.* (2. painos). Routledge.

Iakovidis, I., Wilson, P., & Healy, J. C. (toim.). (2004). *E-health: current situation and examples of implemented and beneficial e-health applications (Vol. 100).* Ios Press.

Jarrett, M. P. (2017). Cybersecurity—a serious patient care concern. *Jama, 318(14),* 1319–1320.

Jayanthi A. (2016, 11. toukokuuta). First known ransomware attack in 1989 also targeted healthcare. Haettu 4.4.2021 osoitteesta https://www.beckershospitalreview.com/healthcare-information-technology/first-known-ransomware-attack-in-1989-also-targeted-healthcare.html

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information systems, 36(3),* 675–705.

Kintzlinger, M., & Nissim, N. (2019). Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. *Journal of biomedical informatics, 95,* 103233.

Koppel, R., Smith, S., Blythe, J., & Kothari, V.H. (2015). Workarounds to Computer Access in Healthcare Organizations: You Want My Password or a Dead Patient? *Studies in health technology and informatics, 208,* 215–220.

Kramer, D. B., & Fu, K. (2017). Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. *Jama, 318(21),* 2077–2078.

Kuehn, B. M. (2018). Pacemaker Recall Highlights Security Concerns for Implantable Devices. *Circulation, 138(15),* 1597–1598.

Kukafka, R. (2019). Digital health consumers on the road to the future. *Journal of medical Internet research, 21(11),* e16359.

Kwon, J., & Johnson, M. E. (2015). Protecting patient data-the economic perspective of healthcare security. *IEEE Security & Privacy, 13(5),* 90–95.

Lanzing, M. (2016). The transparent self. *Ethics and Information Technology, 18(1),* 9–16.

Leman-Langlois, S. (2013). Introduction, Technocrime. Teoksessa Leman-Langlois, S. (toim.), *Technocrime: Technology, crime and social control. (s. 1–13).* Willan.

Li, C., Raghunathan, A., & Jha, N. K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. Teoksessa

2011 IEEE 13th International Conference on e-Health Networking, Applications and Services. (150–156). IEEE.

Li, J. (2015). A privacy preservation model for health-related social networking sites. *Journal of medical Internet research, 17(7),* e168.

Liu, X., Zhang, B., Susarla, A., & Padman, R. (2020). Go to youtube and call me in the morning: Use of social media for chronic conditions. *MIS Quarterly, 44(1),* 257–283.

Luh, F., & Yen, Y. (2020). Cybersecurity in Science and Medicine: Threats and Challenges. *Trends in Biotechnology, 38(8),* 825–828.

Lupton, D. (2017). *Digital health: critical and cross-disciplinary perspectives.* Routledge.

McCarthy, M. (2013). Experts warn on data security in health and fitness apps. *BMJ: British Medical Journal, 347.*

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems, 108,* 57–68.

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. *BMJ: British Medical Journal, 358.*

Menvielle, L., Audrain-Pontevia, A. F., & Menvielle, W. (toim.) (2017). *The Digitization of Healthcare*. Palgrave Macmillan, London.

Mestres, J. C. (2017). State of the art of health care: The cubism period. Teoksessa Menvielle, L., Audrain-Pontevia, A. F., & Menvielle, W. (toim.) *The digitization of healthcare (s. 3–21).* Palgrave Macmillan, London.

Milliken, J., Selis, V., & Marshall, A. (2013). Detection and analysis of the Chameleon WiFi access point virus. *EURASIP Journal on Information Security, 2013(1),* 1–14.

Mishra, A., Ghosh, S., & Mishra, B. K. (2019). Cybersecurity: A Practical Strategy Against Cyber Threats, Risks with Real World Usages. Teoksessa Le, D. N., Kumar, R., Mishra, B. K., Chatterjee, J. M., & Khari, M. (toim.), *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies. (s. 207–220).* John Wiley & Sons.

Monnet B., Very P. (2017). Cyber Threats in the Health-Care Industry. Teoksessa Menvielle L., Audrain-Pontevia AF., Menvielle W. (toim.), *The Digitization of Healthcare. (s. 371–379).* Palgrave Macmillan, London.

Mukherjee, A., & McGinnis, J. D. (2007). E-healthcare: an analysis of key themes in research. *International Journal of Pharmaceutical and Healthcare Marketing, 1(4),* 349–363.

Perakslis, E. D. (2014). Cybersecurity in health care. *The New England journal of medicine, 371(5),* 395–397.

Petersen, A. (2018). *Digital health and technological promise: A sociological inquiry.* Routledge.

Rivas H. (2018) Creating a Case for Digital Health. Teoksessa Rivas H., Wac K. (toim.), *Digital Health. (s. 1–13).* Springer, Cham.

Rivas, H., & Wac, K. (toim.). (2018). *Digital Health: Scaling Healthcare to the World.* Springer, Cham.

Shwartz, O., Mathov, Y., Bohadana, M., Elovici, Y., & Oren, Y. (2017). Opening Pandora's box: effective techniques for reverse engineering IoT devices. Teoksessa Eisenbarth, T., & Teglia, Y. (toim.), *Smart Card Research and Advanced Applications, CARDIS 2017, (s. 1–21).* Springer, Cham.

Shinder, D. L., & Cross, M. (2008). *Scene of the Cybercrime.* Elsevier.

Silber, D. (2004). The case for eHealth. Teoksessa Iakovidis, I., Wilson, P., & Healy, J. C. (toim.), *E-health: current situation and examples of implemented and beneficial e-health applications (Vol. 100). (s. 3–27).* Ios Press.

Steinmetz, K. F., & Nobles, M. R. (2018). Introduction. Teoksessa Steinmetz, K. F., & Nobles, M. R. (toim.), *Technocrime and criminological theory. (s. 1–10).* Routledge.

Thomas, D., & Loader, B. D. (2000). Introduction. Teoksessa Thomas, D., & Loader, B. D. (toim.), *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. (s. 1–14).* Routledge.

Thümmler, C. (2015). Digital Health. Teoksessa Fricker, S. A., Thümmler, C., & Gavras, A. (toim.), *Requirements engineering for digital health. (s. 1–23).* Springer, Cham.

Vuletić, I. (2018). Data-Driven Healthcare and Cybercrime: A Threat We Are Not Aware Of?. *Asia Pacific Journal of Health Law & Ethics, 11(2),* 16–32.

Walden, I. (2007). *Computer crimes and digital investigations.* Oxford: Oxford University Press.

Wall, D. S. (2001). Cybercrimes and the Internet. Teoksessa Wall, D. S. (toim.), *Crime and the Internet. (s. 1–17).* Routledge.

Wall, D. S. (2002). Insecurity and the policing of cyberspace. Teoksessa Crawford, A. (toim.), *Crime and insecurity (s. 186–209).* (3. painos). Routledge.

Wall, D. S. (2003). Mapping out Cybercrimes in a Cyberspatial Surveillant Assemblage. Teoksessa Webster, F., & Ball, K. (toim.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age (s. 112–136).* Pluto Press.

World Health Organization. (2019). WHO Guideline: recommendations on digital interventions for health system strengthening. Haettu 31.3.2021 osoitteesta https://www.who.int/reproductivehealth/publications/digital-interventions-health-system-strengthening/en/

Wiener, N. (1948). *Cybernetics: Or Control and Communication in the Animal and the Machine.* MIT press.

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research, 22(9),* e23692.

Wulfovich, S., & Meyers, A. D. (toim.). (2020). *Digital health entrepreneurship.* Springer, Cham.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society.* (3. painos). SAGE Publications Ltd.

Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (e-health) systems. *Journal of medical systems, 40(12),* 1–12.

Zhang, Y., He, D., & Sang, Y. (2013). Facebook as a platform for health information and communication: a case study of a diabetes group. *Journal of medical systems, 37(3),* 1–12.