FinJeHeW Finnish Journal of eHealth and eWelfare

OTHER ARTICLES

Terveydenhuolto ja kyberuhkat

Teija Norri-Sederholm[1], Tiina Laitinen[2], Martti Lehto[3], Martti J. Kari[3]

[1] Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Helsinki; [2] Kuopion yliopistollinen sairaala, Kuvantamiskeskus, Kuopio; [3] Jyväskylän yliopisto, Informaatioteknologian tiedekunta, Jyväskylä

Teija Norri-Sederholm, Johtamisen ja sotilaspedagogiikan laitos, Maanpuolustuskorkeakoulu, PL 7, 00861 Helsinki, FINLAND. Email: teija.norri-sederholm@mil.fi

Tiivistelmä

Kyberturvallisuusstrategian vision mukaan Suomen tulee kyetä suojaamaan elintärkeät toimintonsa kyberuhkaa vastaan kaikissa tilanteissa. Terveydenhuolto on yksi elintärkeistä toiminnoista. Terveystoimiala on kyberhyökkäysten top-5-listalla ensimmäisenä. Hyökkäysten keskeisin motivaatio on potilastietojen arvo pimeillä markkinoilla. Vuonna 2015 varastettiin yli satamiljoonaa potilastietoa, jotka sisältävät rikollisille arvokkaita tietoja, kuten luottokorttinumeroita, työnantajatietoja ja sairaushistoriatietoja. Tässä artikkelissa kuvataan terveydenhuoltoon liittyviä kyberuhkia, kyberhaavoittuvuuksia ja toteutuneita kyberhyökkäyksiä kybermaailman eri ulottuvuudet kattaen.

Tarkastelussa käytetään kybermaailman viisikerroksista verkostomallia, joka sisältää fyysisen, syntaktisen, semanttisen, palvelu- ja kognitiivisen kerroksen. Malli kattaa laajasti koko kybermaailman fyysisen kerroksen laitteista ja verkoista kognitiivisen kerroksen inhimillisiin ongelmanratkaisu- ja tulkintaympäristöihin. Haavoittuvuuksia ja toteutuneita hyökkäyksiä voidaan mallin mukaan jaotella laitekohtaisista haavoittuvuuksista aina koulutuksen puutteista johtuviin haavoittuvuuksiin ja pelottelu- ja kalasteluohjelmilla tapahtuneisiin hyökkäyksiin. Paljon julkisuutta ovat saaneet myös terveydenhuoltoon kohdistuneet kiristyshaittaohjelmahyökkäykset.

Kyberuhkia vastaan voidaan suojautua useilla eri tasoilla ja tavoilla. Lähtökohtana on se, että jokainen organisaatio huolehtii oman toimintansa kyberturvallisuudesta tehden yhteistyötä muiden toimijoiden kanssa uhkien tunnistamisessa ja torjumisessa. Terveydenhuollon kyberturvallisuuden rakentaminen on systeemin hallintaa, jossa tulee keskittyä järjestelmien kokonaisuuteen yksittäisten laitteiden sijaan. Yhteistoiminnan tavoitteena on, että kokonaisosaaminen tukee yksittäisen toimijan toimintaedellytyksiä yhteistä uhkaa vastaan. Terveydenhuollon kyberturvallisuuden jatkuva parantaminen ja tietoisuuden lisääminen ovat kaikkien kansalaisten etuja, jotka vaativat vahvaa ymmärrystä niin tietoturvasta kuin terveydenhuollon toimintatavoistakin. Tämän vuoksi tietoisuuden kohottamisen ja henkilökunnan kouluttamisen tuleekin olla keskeisellä sijalla organisaatioiden kyberturvallisuudessa.

Avainsanat: kyberturvallisuus, kyberuhka, terveydenhuolto, kriittinen infrastruktuuri

Abstract

Finland's cyber security strategy states that Finland has to be capable of protecting the vital functions of society, such as health care, against cyber threats. Currently, health care heads the TOP-5 list of cyber attacks because of the value of patient data in dark markets. In this article, we describe actual cyber threats, cyber vulnerabilities, and cyber attacks covering different dimensions of the cyber world.

In this study, we use a five-layer cyber world network-model including physical, syntactic, semantic, service, and cognitive layers. The model covers widely the devices and networks from the physical layer to the human problem solving and interpretation environments in the cognitive layer. Also, the vulnerabilities of e.g. device-specific or human factor-related and realised attacks like phishing can be classified with the help of the model. Ransomwares, affecting the semantic layer, have received a lot of publicity lately.

There are many ways to take safeguards against cyber threats in different layers. The starting point is that each organisation takes care of their cyber security in collaboration with other actors in recognising threats and in taking action against them. Creating cyber security is actually about managing the system. It is vital to focus on systems as a whole instead of individual devices. The target of the collaboration is that comprehensive know-how supports the facilities of each actor against a common threat. The continuous improvement of cyber security in health care, increasing awareness, and educating staff should be an essential part of the cyber strategy of any organisation.

Keywords: cyber security, cyber threat, health care, critical infrastructure

Johdanto

Suomen kyberturvallisuusstrategian [1] yhtenä visiona on, että ”Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan”. Terveydenhuolto ja siihen liittyvät tietojärjestelmät ja laitteet ovat osa yhteiskunnan turvallisuusstrategiaan [2] kuuluvia elintärkeitä toimintoja. Kokonaisturvallisuuden näkökulmasta onkin tärkeää kiinnittää huomioita terveydenhuollon kyberturvallisuuteen ja siihen liittyviin uhkiin. Terveystoimiala on kyberhyökkäysten top-5-listalla ensimmäisenä [3]. Kyberhyökkäyksiltä suojautuminen ja Euroopan kyberturvallisuusviraston perustaminen on nostettu myös Euroopan unionin (EU) tasolla yhdeksi viidestä vuoden 2018 painopisteestä [4].

Artikkelissa kuvataan terveydenhuoltoon liittyviä kyberuhkia osana kriittistä infrastruktuurin suojaamista. Artikkelin tarkoituksena on tarkastella terveydenhuoltoon liittyviä kyberuhkia ja -haavoittuvuuksia sekä toteutuneita kyberhyökkäyksiä kybermaailman viisikerroksisen hierarkkisen verkostomallin mukaisesti.

Kyberturvallisuus ja kriittinen infrastruktuuri

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” [2].

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. [2]

Osana yhteiskunnan turvallisuusstrategian ja kokonaisturvallisuuden mallin käytännön toteutusta on laadittu

Suomen kyberturvallisuusstrategia [1], johon on kuvattu kyberturvallisuuden visio ja strategiset linjaukset ja sen päivitetty toimeenpano-ohjelma. Toimeenpano-ohjelmassa yhtenä kohtana on maakunta- ja soteuudistuksen toiminnallisten prosessien jatkuvuuden hallinta sekä tieto- ja kyberturvallisuuden varmistaminen. Tähän liittyen tuotetaan valtakunnallinen sosiaali- ja terveydenhuollon varautumisen ja jatkuvuuden hallinnan ohjeistus. [5]

Kyberturvallisuudesta on kansainvälisesti useita määritelmiä. Suomen kyberturvallisuusstrategiassa [1] ja Kyberturvallisuuden sanastossa [6] kyberturvallisuudella tarkoitetaan ”tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Määritelmän mukaan kyberturvallisuuteen katsotaan kuuluvan ne ”toimenpiteet, joiden avulla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia”. Kriittiseen infrastruktuuriin kuuluvat ”perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi”. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että digitaalisia toimintoja ja palveluja. [6] Kyberturvallisuus perustuu ymmärrykseen haavoittuvuuksista tieto- ja tietoliikennejärjestelmissä sekä sulautetuissa informaatioteknologiaa sisältävissä järjestelmissä. Eri järjestelmät sisältävät organisaation kannalta kriittisiä tietoja ja toiminnallisuuksia. Kyberturvallisuuden rakentaminen perustuu uhka- ja riskianalyyseihin, tehokkaaseen tilanneymmärrykseen sekä resilienssikyvykkyyden rakentamiseen. [7] Tässä artikkelissa kyberturvallisuus ja kriittinen infrastruktuuri ymmärretään Suomen kyberturvallisuusstrategian ja kyberturvallisuuden sanaston määritelmien mukaisesti.

Kybermaailman viitekehyksessä (Kuvio 1) kyberturvallisuus ja kyberpuolustus, jolla tarkoitetaan kyberturvallisuuden maanpuolustuksellista osaa [6], ovat osa kansallista kokonaisturvallisuutta. Kybermaailma koostuu muun muassa kriittisestä infrastruktuurista, minkä vuoksi kyberpuolustus on välttämätön osa kybermaailmaa. [8] Kybermaailma sisältää tiedon, järjestelmien ja tietoverkkojen lisäksi myös ihmisen kokonaisvaltaisen olemassaolon tässä kokonaisuudessa. Melkein kaikki yhteiskunnan perustoiminnot, sekä kriittiset toiminnot että palvelut, on automatisoitu, ja ne ovat yhteydessä toisiinsa. Tämän vuoksi turvallisuusnäkökulma niin tietoturvaan kuin teknologisiin ratkaisuihinkin on noussut keskeiseksi asiaksi kansalaisille, elinkeinoelämälle ja julkiselle sektorille. [9]

Kuvio 1. Kybermaailman viitekehys [8].

Martin C. Libicki on luonut kybermaailman tarkasteluun nelikerroksisen rakenteen (physical, syntactic, semantic, pragmatic), jonka idea perustuu OSI-malliin (Open Systems Interconnection Reference Model). OSI-malli kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa. [10] Kukin kerroksista käyttää yhtä alemman kerroksen palveluja ja tarjoaa palveluja yhtä kerrosta ylemmäs. Tästä mallista on kehitetty viisikerroksinen malli, jota käytetään tässä tutkimuksessa. Sen kerrokset ovat fyysinen, syntaktinen, semanttinen, palvelut ja kognitiivinen (Kuvio 2). Fyysinen kerros sisältää tiedonsiirtoverkkoon kuuluvat erilaiset laitteet sekä kiinteät ja langattomat yhteydet. Syntaktisessa kerroksessa ovat muun muassa järjestelmien erilaiset ohjaus- ja hallintaohjelmat, liityntäteknologiat ja verkkoprotokollat. Semanttinen kerros sisältää käyttäjien hallitseman informaatio- ja tietosisällön sekä käyttäjän hallinnassa olevan järjestelmän toimintojen ohjauksen. Palvelukerroksessa ovat esimerkiksi erilaiset julkiset ja kaupalliset verkkopalvelut sekä kansalaisten palvelut. Kognitiivinen kerros sisältää inhimillisen ongelmanratkaisu- ja tulkintaympäristön sekä informaation merkityssisällön ymmärtämisen ja tulkinnan. [11]

Kyberturvallisuutta ylläpidetään monenlaisten teknisten keinojen, kuten palomuurien, virustorjuntaohjelmien ja salausten, avulla. Tunnettua on kuitenkin se, että heikoin lenkki tässä kokonaisuudessa on ihminen itse. Työntekijöiden huolimattomuus tietoturvaan liittyvissä asioissa sekä yleistynyt ihmisten profilointi (social engineering) ovat keskeisin myötävaikuttava tekijä kyberhyökkäyksissä [12].

Kuvio 2. Viisikerroksinen hierarkkinen verkostomalli [8].

Kyberturvallisuuden kokonaisuuteen kuuluvat sellaiset tekijät kuten kyberturvallisuuden strateginen johtaminen, tilannetietoisuuden muodostaminen sekä viranomaisten erilaiset kyberkeskukset. Tutkimuksen [13] mukaan kyberturvallisuuden strategisen johtamisen tärkeimmäksi tehtäväksi Suomessa on nähty vision ja kansallisen ajattelutavan luominen. Nämä tulisi tunnistaa kaikilla kyberturvallisuustyöhön osallistuvilla toimijatasoilla, ja niiden tulisi ohjata toimintaa niin normaalikuin häiriötilanteissakin. Keskeistä on myös kriittisen infrastruktuurin eri toimijoiden kyberturvallisuuden tilannetietoisuuden muodostaminen ja ylläpitäminen sekä jatkuvuuden hallintaan liittyvä päätöksenteko.

Kriittinen infrastruktuuri sisältää monitahoisia riippuvuussuhteita, joten Suomessa on oltava myös kansallisella tasolla kattava tilannetietoisuus kansallisesta kyberturvallisuustilanteesta ja siihen vaikuttavista tekijöistä. Suomessa tehdäänkin tiivistä viranomaisyhteistyötä Viestintäviraston Kybertuvallisuuskeskuksen, Keskusrikospoliisin kyberrikosten torjuntakeskuksen, Puolustusvoimien, Valtioneuvoston kanslian tilannekeskuksen ja Helsingissä toimivan Euroopan hybridiosaamiskeskuksen (The European Centre of Excellence for Countering Hybrid Threats) kanssa.

Kyberuhkia ja toteutuneita hyökkäyksiä terveydenhuollossa

Kyberuhkalla tarkoitetaan ”mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön ja [joka] toteutuessaan vaarantaa siitä riippuvaisen toiminnon”. Uhkat voivat siis aiheutua toteutuneista tietoturvauhkista, jotka vaarantavat tietojärjestelmän oikeanlaisen tai tarkoitetun toiminnan, tai digitaalisessa viestintäympäristössä toteutettavista yhteiskunnan turvallisuutta vaarantavista teoista. [6] Kyberuhkien katsotaan kohdistuvan suoraan tai välillisesti yhteiskunnan elintärkeisiin toimintoihin ja kansalaisia vastaan joko maan rajojen sisältä tai ulkopuolelta. Kyberuhkina pidetään kybervandalismia, kyberrikollisuutta, kybervakoilua, kyberterrorismia sekä kybersodankäynnin erilaisia kyberoperaatioita. Uhkien luonteeseen kuuluu se, että ne voivat esiintyä itsenäisinä, samanaikaisina tai toistensa jatkumoina. Ne voivat myös vaihdella ajallisesti. [11]

Kyberhyökkäysten top-5-listalla ovat terveystoimiala, valmistus ja tuotanto, pankki- ja rahoitustoimiala, julkishallinto sekä liikenne- ja kuljetustoimialat. Terveystoimiala on siis ensimmäisenä. Esimerkiksi vuonna 2015 varastettiin yli satamiljoonaa potilastietoa. Potilastiedot sisältävät rikollisille arvokkaita luottokorttinumeroita, sähköpostiosoitteita, sairausvakuutusnumeroita, työnantajatietoja ja sairaushistoriatietoja. Näitä tietoja myydään ja niitä käytetään erilaisissa kyberrikoksissa, kuten tietojen kalasteluhyökkäyksissä, petoksissa sekä identiteettivarkauksissa. [3]

Ennusteen mukaan kyberhyökkäyksiä lisääviä teknologioita ovat esineiden internet (IoT), pilvipalvelut, big data, mobiiliteknologia ja BYOD-toiminta (Bring Your Own Device). [3] Terveydenhuollon merkittävät uhkat liittyvät terveydenhuollon laitteisiin ohjelmistoihin, mobiililaitteisiin, etähallittaviin laitteisiin sekä käyttäjän toimiin muun muassa salasanojen ja järjestelmien käytössä [14].

Kyberriskit ovat lisääntyneet terveydenhuollossa. KPMG:n vuoden 2015 kyberturvallisuuskyselyssä kävi ilmi, että 81 prosenttia terveydenhuollon organisaatioista oli kahden viime vuoden aikana joutunut kyberhyökkäyksen kohteeksi ja vain puolet niistä oli ollut riittävästi varautuneita. Hyökkäysten tärkein motivaatio oli potilastietojen arvo pimeillä markkinoilla. Rikolliset käyttävät myös kiristyshaittaohjelmia salaamaan tietoja ja sitten vaativat maksua digitaalisen valuutan avulla tietojen palauttamiseksi (mukaan luettuna potilastiedot), mikä on vaikuttanut sairaaloihin useissa maissa, kuten Yhdysvalloissa, Isossa-Britanniassa ja Australiassa. [15]

Puutteellinen kyberturvallisuus voi vaikuttaa potilaan terveyteen ja vahingossa saattaa vaaranalaiseksi myös potilastietoja. Lääkinnällisten laitteiden yritykset ja terveydenhuollon organisaatiot kohtaavat joukon kyberhyökkäyksiä, joihin kuuluvat kohdistamattomat ja yhä kehittyneemmät kohdistetut hyökkäykset. [15]

Uhkia ovat

- hoidon ja/tai palvelun häiriöt (jotka voivat pahimmillaan johtaa potilaan kuolemaan)
- henkilöstön harhauttaminen huijaussähköpostilla tai väärennetyillä verkkosivustoilla kirjautumistunnusten hankkimiseksi tai haittaohjelmien levittämiseksi
- tahaton tai tarkoituksellinen ”sisäpiiriläisen uhka”, joka liittyy sisäpiiriläisen luottamukselliseen asemaan organisaatiossa
- potilastietojen – erityisesti elektronisesti turvattujen terveystietojen – menetys
- tietomurto, tietojen vuotaminen ja arvon menetys
- kiristys ja pakottaminen arkaluonteisia vuotaneita tietoja hyödyntämällä
- immateriaalioikeuksien varastaminen.

Tutkimus on osoittanut, että terveydenhuollon kyberturvallisuus painottuu edelleen potilaskertomustietojen suojaamiseen. Vielä ei kuitenkaan osata riittävästi puuttua ja suojautua varsinaisilta potilaiden terveyteen kohdistuvilta todellisilta uhkilta. [15]

Kyberhaavoittuvuuksia, uhkia ja toteutuneita hyökkäyksiä tarkastellaan tässä artikkelissa kybermaailman viisikerroksisen hierarkkisen verkostomallin mukaan (Taulukko 1) jakaen kybermaailma fyysiseen, syntaktiseen, semanttiseen, palvelu- ja kognitiiviseen kerrokseen. [8] Terveydenhuoltoon kohdistuneita kyberhyökkäyksiä käsitellään esimerkinomaisesti ja esille tuodaan eri kerroksiin kohdistuneita hyökkäystyyppejä.

Taulukko 1. Kybermaailman haavoittuvuuksia ja hyökkäyksiä viisikerroksisen hierarkkisen verkostomallin mukaisesti.

Kerros	Kuvaus/sisältö	Haavoittuvuuksia	Hyökkäyksiä
Fyysinen	Tiedonsiirtoverkko: kytketyt laitteet, kiinteät ja langattomat yhteydet	Laitteiden ja laitetilojen puutteellinen fyysinen suojaus, verkkosalauksen puutteet, suojaamattomat WLAN-verkot ja laitteet, vaillinaiset salasanat, USB-tikkujen ja muistikorttien käyttö, kattavat ohjekirjat	Kineettinen tuhoaminen, fyysinen varkaus/katoaminen Komponenttitason saastuttaminen
Syntaktinen	Järjestelmien ohjaus- ja hallintalaitteet, liityntäteknologiat, verkkoprotokollat	Tietoverkkoon kytketyt laitteet, heikosti suojatut etäyhteydet mm. huolto- ja vikatilanteissa, puutteellinen käyttäjän tunnistaminen, haasteet valvontaohjelmien päivittämisessä	Laitteiden haltuunotto, ja saastuttaminen haittaohjelmilla
Semanttinen	Käyttäjien hallitsema informaatio- ja tietosisältö sekä järjestelmän toimintojen ohjaus	Puutteellinen tietosuojaus, heikko varmuuskopiointi, puutteet ohjelmistosuunnittelussa ja -tuotannossa (ohjelmistovirheet)	Tiedon varastaminen, tuhoaminen, väärentäminen, saastuttaminen, tiedon luottamuksellisuuden, eheyden ja saatavuuden kiistäminen, lunnashaittaohjelmat
Palvelu	Julkiset ja kaupalliset verkkopalvelut, kansalaisten palvelut	Osaaminen hajallaan eri yksiköissä, liika optimismi suhteessa omaan suojautumiseen kyberhyökkäyksiltä, puutteellinen johtaminen	Palvelunestohyökkäykset, palvelusivustojen saastuttaminen
Kognitiivinen	Inhimillinen ongelmanratkaisu- ja tulkintaympäristö, informaation merkityssisällön ymmärtäminen ja tulkinta	Sähköposti, murretut verkkosivustot ja verkkomainokset, sosiaalinen media, vaillinainen koulutus, puutteet teknisessä valvonnassa	Tietojen kalastelu, pelotteluohjelmat, identiteettivarkaudet

Fyysinen kerros

Fyysiseen kerrokseen liittyviä haavoittuvuuksia ovat puutteellinen fyysinen suojaus, suojaamattomat WLAN-verkot, verkkosalauksen puutteet ja suojaamattomat laitteet [8]. Terveydenhuollossa on erityisesti viimeisen kymmenen vuoden aikana ollut vahva suuntaus paperittomuuteen ja potilaan suostumuksella tietojen liikkuvuuteen yli organisaatiorajojen, millä on myönteinen vaikutus potilaan hoitoon ja potilasturvallisuuteen. Tämän vuoksi terveydenhuollon laitteet ovat hyvin suurelta osin tietoverkkoon liitettyjä ja niillä on integraatiorajapintoja potilastietojärjestelmiin.

Lehto ja Lehto [16] raportoivat terveydenhuollon laitteiden turvallisuudesta, muun muassa lepo-EKG-laitteista, potilasvalvontamonitoreista, ruiskupumpputelakoista, kuvalevylukijoista ja ultraäänilaitteista. Useissa laitteissa oli puutteellinen WLAN-yhteys, jonka salauksista ei löytynyt tietoa kattavasti. Raportissa oli myös tunnistettu laitteita, jotka käyttivät salaamatonta liikennettä tai helposti murrettavissa olevaa WEP-salausta. Toisaalta löytyi myös laitteita, jotka tukivat WPA- ja WPA2-salauksia ja joissa oli kattava mahdollisuus autentikointiin. Muita laitteisiin liittyviä haavoittuvuuksia ovat vaillinaiset salasanat [17] sekä USB-tikkujen ja muistikorttien käyttö [16]. Williams ja Woodward [17] esittävät myös, että terveydenhuollon laitteiden ohjekirjat sisältävät paljon hyödyllistä tietoa kyberhaavoittuvuuksien löytämiseksi, mutta toisaalta terveydenhuollon laitteita koskeva lainsäädäntö ja turvallisuusvaatimukset edellyttävät kattavia ohjekirjoja. Heikosti suojatut laitteet voivat olla portti tunkeutua laajemminkin organisaation tietoverkkoon.

Fyysiseen kerrokseen liittyvät raportoidut hyökkäykset ovat kineettistä tuhoamista ja laitevarkauksia. Yhdysvalloissa on raportoitu myös ultraäänilaitteen varkaus, jolloin menetettiin henkilötietoja ja kuvantamisaineistoja. Hakkerointi on yleisin sairaalaan kohdistuva hyökkäys, ja viime vuosina on ollut lukuisia potilastietojen varkauksia. [16] Henkilökohtaisia tietoja, nimiä, osoitteita, henkilötunnuksia ja terveystietoja sekä luottokorttinumeroita voidaan käyttää hyväksi identiteettivarkauksissa luotettavien profiilien muodostamiseen, minkä vuoksi tietovarkauksia on kyberhyökkäyksinä paljon.

Syntaktinen kerros

Syntaktisen kerroksen haavoittuvuudet johtuvat puutteellisista valvontajärjestelmistä (SIEM/IDS/IPS), epätarkasta kybertilannekuvasta ja heikosta järjestelmien suojaustasosta [8]. Sairaalan tietoverkkoon on tyypillisesti liitetty työasemat, palvelimet ja terveydenhuollon laitteet [18]. Lisäksi sisäverkko ja julkinen verkko on erotettu palomuurilla ja erilaisilla tunkeilijantorjuntajärjestelmillä. Uhkan aiheuttavat erityisesti terveydenhuollon laitteet. Osaan laitteista voidaan huollon ja vikatilanteiden selvittelyn vuoksi tehdä etäyhteyksiä [14]. Ongelmien selvittely voi vaatia laajoja käyttöoikeuksia ja mahdollistaa salassa pidettävien ja potilasturvallisuuteen vaikuttavien tietojen käsittelyn. Heikosti suojatut etäyhteydet ja puutteellinen käyttäjän tunnistaminen voivat myös olla mahdollisuus tunkeutujalle [14]. Terveydenhuollon laitteiden laitekohtainen suojaus muun muassa virustorjuntaohjelmilla on jossain määrin haasteellista. Osassa laitteita voidaan käyttää vain valmistajien hyväksymiä tietoturvaohjelmia [18] ja osaan laitteita niitä ei voida ollenkaan asentaa [17]. Lisäksi osa laitteista toimii verkossa vain lyhytaikaisesti datan lähettämisen tai vastaanottamisen ajan, jolloin muun muassa niiden valvontaohjelmien päivittäminen verkon kautta on haasteellista [17].

Symantec julkaisi 23. huhtikuuta 2018 blogin [19], jossa esitettiin tilastoja Orangeworm-matohaittaohjelmasta terveydenhuollossa. Symantecin mukaan kyseessä ei ole satunnaisesti leviävä haittaohjelma, vaan hyökkäykset on kohdistettu erityisesti terveystekniikan teollisuuteen, ja haittaohjelmaa on löydetty muun muassa röntgen- ja magneettikuvauslaitteiden ohjaustietokoneista. Tämän haittaohjelman löydetyistä uhreista 2 prosenttia on Ruotsissa ja samoin 2 prosenttia Norjassa. Suomi ei ollut mukana Symantecin tilastossa.

Löytäessään sopivan kohteen haittaohjelma pystyy leviämään verkossa hyvin aktiivisesti. Sinänsä on kuitenkin epäselvää, mikä on tämän hyökkäyksen varsinainen motiivi ja päämäärä. Kuvantamislaitteiden ohjaus-

tietokoneet ovat sairaalan verkossa, mutta niiden päivitettävyys ja haittaohjelmilta suojaaminen voi olla rajattua. Ne eivät yleensä ole kattavasti valvontaohjelmien piirissä, ja ne ovat siten hyvä kohde hyökkäykselle ja haittaohjelmien levittämiselle.

Semanttinen kerros

Kolmas kerros on semanttinen kerros, jossa uhkat ja haavoittuvuudet liittyvät puutteelliseen tietosuojaukseen, heikkoon varmuuskopiointiin ja puutteisiin ohjelmistosuunnittelussa ja -tuotannossa [8]. Ohjelmistosuunnittelun ja -tuotannon haavoittuvuudet liittyvät usein ohjelmistovirheisiin [14]. Haavoittuvuudet voivat mahdollistaa mielivaltaisten komentojen suorittamisen, haittaohjelmien levittämisen, salassa pidettävien tietojen paljastamisen tai haittaohjelmien levittämisen. Aktivoitunut haittaohjelma voi myös käyttää ohjelmistohaavoittuvuutta saadakseen korkeamman tason käyttäjäoikeuksia [16]. Tyypilliset uhkat ovat muun muassa sähköpostin kautta leviävät haittaohjelmat, jotka pystyvät aktivoitumaan ilman liitetiedoston avaamistakin. Onnistuneissa hyökkäyksissä on usein ollut kyse vaillinaisesti testatusta ohjelmistosta [17]. Kyberuhkien näkökulmasta myös varmuuskopiointi on olennaista, sillä tyypillisiä uhkia ovat tietojen tuhoaminen, tietojen vääristäminen ja kiristyshaittaohjelmat.

Semanttiseen kerrokseen kohdistuneet kyberhyökkäykset, erityisesti kiristyshaittaohjelmat, ovat saaneet runsaasti näkyvyyttä mediassa. Toukokuussa 2017 Iso-Britannian kansallisen terveyspalvelun (National Health Service, NHS) työasemille levisi ”WannaCry”-kiristyshaittaohjelma, joka lukitsi tiedostoja ja kirjasi käyttäjiä ulos [20]. Toiminnan ollessa suurelta osin paperitonta ongelma aiheutti potilaiden vastaanotto- ja toimenpideaikojen ja leikkausten peruutuksia, sekä jopa terveydenhuollon yksiköiden sulkemisia. Kriittiset potilaat saatiin kuitenkin hoidettua. Hyökkäys perustui Windows-järjestelmän haavoittuvuuteen, mutta NHS:n vanhentuneeseen työasemankantaan ei ollut voitu asentaa julkaistua tietoturvapäivitystä. Suomessakin on ainakin Varsinais-Suomen sairaanhoitopiiriin ja Helsingin ja Uudenmaan sairaanhoitopiiriin kohdistunut kiristyshaittaohjelmahyökkäyksiä, mutta ne ovat olleet vaikutuksiltaan paljon vähäisempiä ja käsittäneet yksittäisiä työasemia.

Kokonaisuutena viime vuosina sairaaloihin kohdistuneiden kiristyshaittaohjelmien vaikutus on kuitenkin mittava. [16] Sairaalat ovat kohteina otollisia, sillä niiden toiminta häiriintyy merkittävästi ilman sähköisiä potilastietoja, ja toisaalta sairaaloiden työasemien ja laitteiden rajallinen päivitettävyys tarjoaa haavoittuvuuden hyökkääjän käyttöön.

Palvelukerros

Palvelukerros kattaa kyberturvallisuuden johtamisen, ohjelmistotuotannon ja turvallisuusprosessit, ja uhkat liittyvät niissä esiintyviin puutteisiin [8]. Palvelukerros kattaa erilaisia kansalaisen palveluita ja julkisia verkkopalveluita. Suomessa terveydenhuollon näkökulmasta merkittävimpiä ovat jo nyt Kanta-palvelut, joissa kaikkien terveydenhuollon toimijoiden potilaskertomustiedot kerätään tulevaisuudessa saman palvelun alle ja myös OmaKannasta kansalaisen itse käytettäviksi. Johtamisen näkökulmasta yhdeksi uhkaksi on tunnistettu, että osaaminen on hajallaan terveydenhuollon eri yksiköissä [21], ja toimenpiteenä sille on esitetty asiantuntijoista koottuja poikkihallinnollisia ryhmiä. Terveydenhuollon organisaatiot saattavat muiden organisaatioiden tapaan usein olla liian optimistisia suhteessa omaan suojautumiseensa kyberhyökkäyksiltä [22].

Palvelukerrokseen kohdistuneet hyökkäykset ovat tyypillisesti palvelunestohyökkäyksiä. Niissä jonkin palvelun verkkoliikennettä kuormitetaan niin, että palvelut lakkaavat toimimasta tai ainakin ne hidastuvat estäen käyttäjien pääsyn palveluihin [16]. Palvelunestohyökkäyksissä potilastiedot eivät varsinaisesti ole vaarassa, mutta potilasturvallisuus voi vaarantua, kun palveluihin ja tietoihin ei päästä käsiksi.

Kelan Kanta-palveluihin kohdistui vuonna 2017 palvelunestohyökkäyksiä, jotka häiritsivät muutamien tuntien ajan Kanta.fi-, OmaKanta- ja Kelain-palvelun käyttöä [23, 24]. Palvelunestohyökkäys vaikutti siihen, että tietoja ei päässyt katsomaan, mutta esimerkiksi merkittävää vaikutusta apteekkitoimintaan ei ollut, vaikka

sähköinen resepti toimii saman Kanta-palvelun kautta. Ainoastaan pienimmissä apteekeissa, joissa ei ollut kiinteää tietoliikenneyhteyttä, saattoi olla häiriöitä.

Kognitiivinen kerros

Viimeinen kerroksista, kognitiivinen kerros, sisältää tiedon, osaamisen ja kompetenssin puutteet sekä puutteellisen kybertilannetietoisuuden [8]. Sähköposti, murretut verkkosivustot ja verkkomainokset sekä sosiaalinen media ovat mahdollisia reittejä haittaohjelmien levitykselle [14]. Yhden työaseman saastuttua haittaohjelma voi edelleen levitä organisaation tietoverkossa muihin työasemiin. Mikäli henkilökunnalla ei ole tietoa sähköpostin, verkkosivujen tai sosiaalisen median haittaohjelmavaaroista, voi jokaisen yksilön toiminta aiheuttaa uhkaa organisaatiolle. Siten vaillinainen henkilöstön koulutus on uhka organisaatiolle [17].

Terveydenhuollon työntekijöihin kohdistuu jatkuvasti, samoin kuin laajasti muuhunkin väestöön, erilaisia urkinta- ja kalasteluviestejä. Kuopion yliopistollisessa sairaalassa on ollut muun muassa sähköpostiviestejä, joissa ehdotetaan tilaamaan sähköpostin lisätilaa [25]. Mikäli käyttäjä ryhtyy tilaamaan lisätilaa, hän joutuu syöttämään näennäiseen nettikaavakkeeseen käyttäjätunnuksensa ja salasanansa. Postilaatikko on tällöin otettu haltuun nopeimmillaan 11 minuutin kuluttua viestin saapumisesta.

Yhdysvalloissa KPMG:n terveydenhuollon toimijoille tekemän kyselytutkimuksen [26] mukaan neljä viidestä vastanneesta arveli IT-infrastruktuurinsa vaarantuneen kyberhyökkäyksien vuoksi. Vastaajia oli 223, joten tutkimuksen antamaa kuvaa voi pitää edustavana. Suurimpana uhkana pidettiin ulkopuolisia hyökkäyksiä (65 %) ja datan jakamista kolmannen osapuolen kanssa (48 %). Työntekijöiden tietomurrot ja -varkaudet, langattomat verkot ja palomuurien puutteet seurasivat näitä kahta (noin 30 %:n osuudella kukin). Vastaavasti tietoturvahuolista suurin olivat haittaohjelmia levittävät systeemit (67 %), tietosuojan ja potilaan yksityisyyden vaarantuminen (57 %) sekä työntekijöistä johtuvat tietosuojaongelmat (40 %). Vajaa kolmannes vastaajista (30 %) piti terveydenhuollon laitteiden turvallisuutta tai ikääntyvää tietotekniikkaa suurimpana huolena.

Terveydenhuollon kyberuhkiin varautuminen ja resilienssi

Kyberuhkia vastaan voidaan suojautua useilla eri tasoilla ja tavoilla. Lähtökohtana on se, että jokainen organisaatio huolehtii oman toimintansa kyberturvallisuudesta. Toimialakohtaisesti, kuten terveydenhuollossa, on järkevää tehdä yhteistyötä uhkien tunnistamisessa ja torjumisessa. Yhteistoiminnan tavoitteena on, että kokonaisosaaminen tukee yksittäisen toimijan toimintaedellytyksiä yhteistä uhkaa vastaan.

Valtakunnallisesti tehdään toimialat ylittävää yhteistyötä, ja tässä keskeisessä roolissa on Viestintäviraston kyberturvallisuuskeskus. Se kerää tietoa tietoturvauhkista ja jakaa tietoa sekä ohjeita yhteistyötahoilleen. Yhteistoiminta tarvitsee myös tukitoimintoja. Näitä ovat esimerkiksi akateeminen maailma, tietoturvapalveluja tarjoavat organisaatiot ja Huoltovarmuuskeskus, jotka tukevat omalla erikoisosaamisellaan muita toimijoita. Yksi suojautumisen keino on erilaiset tietoturvastandardit, suositukset ja lainsäädäntö. Kybertoimintaympäristössä kansainvälinen yhteistyö on keskeistä, koska erilaisissa kyberhyökkäyksissä on yleensä kansainvälinen elementti mukana. [27] Kyberuhkat voivat varautumisesta huolimatta myös toteutua, minkä vuoksi organisaatioiden tulee kehittää sietokykyään (resilienssi).

Toteutuneiden hyökkäysten, strategioiden edellyttämien toimenpiteiden ja valtionhallinnon tietoturvaohjeistusten myötä terveydenhuollossa on ryhdytty viime vuosina varautumistoimenpiteisiin. Kuopion yliopistollisessa sairaalassa on varautumisprojekti, jossa merkittävänä keinona on kriittisten järjestelmien kahdentaminen [28]. Kahdentaminen koskee konesalia ja tietoliikenneyhteyksiä. Aiemmin on jo kahdennettu muun muassa potilastietojärjestelmiä ja tehohoidon järjestelmä. Kahdentamisen lisäksi parannetaan tietoturvaa ja lisätään henkilöstöä IT-palvelutuotantoon. Varautumisen kustannusarvio on 15 miljoonaa euroa kolmen vuoden aikaperiodilla. Poikkeustilanteiden

lisäksi kahdentamisen hyötynä on se, että IT-huoltotöitä voidaan tehdä aiheuttamatta toimintaan keskeytyksiä [29].

NHS:ä kohtaan vuonna 2017 kohdistuneen hyökkäyksen perusteella on myös ryhdytty varautumistoimenpiteisiin [30]. Varautumistoimenpiteistä on tehty selvitys ja sen perusteella on hyväksytty mittava kustannuslisä sekä muita toimia, jotka liittyvät pääasiassa tietoturvallisuuteen ja kybertilannetietoisuuteen.

Molemmissa edellä mainituissa tapauksissa kyse on mittavista toimenpiteistä. Käytännön toimet voivat ja niiden tulee alkaa myös aivan ruohonjuuritasolta. Yksittäisten laitteiden kyberhaavoittuvuutta voidaan vähentää niin kutsutulla laitteiston tai ohjelmiston koventamisella [18]. Tällä tarkoitetaan ominaisuuksien ja asetusten tiukentamista normaalista. Laitepohjaisessa koventamisessa voidaan kytkeä USB-liitäntä pois käytöstä, deaktivoida tarpeettomat verkkoliitynnät ja määrittää BIOS-salasana, jolloin asetuksia ei päästä vapaasti muuttamaan. Ohjelmistopohjaisessa koventamisessa vastaavasti laitteeseen asennetaan vain käytön kannalta välttämättömät ohjelmistot ja sammutetaan kaikki tarpeettomat palvelut, estetään internetin ja sähköpostin käyttö sekä aktivoidaan ohjelmistopalomuuri sallimaan vain tarvittava liikennöinti ja estämään julkisesta osoiteavaruudesta tuleva liikennöinti. Myös salasanasuojaukset aktivoidaan [18] ja huolehditaan siitä, että paikallinen järjestelmävalvojatunnus ei ole oletuksen mukainen (administrator). Yhteiskäyttöisistä käyttäjätunnuksista tulee luopua, koska niiden salasanat ovat helposti tarpeettoman useiden tiedossa niiden ollessa nk. julkisia salaisuuksia [14].

Ohjelmistojen päivitysten tulee aina olla ajan tasalla [18, 31] ja varmuuskopioinnin kunnossa. On myös tärkeää suojata varmuuskopiot päällekirjoitukselta, jotta vältetään niiden vahingoittuminen hyökkäystilanteessa. Virustorjuntaohjelmien ja muiden tietoturvaohjelmien on oltava pakollisia kaikille niille työasemille ja laitteille, joihin ne voidaan toiminnan vaarantumatta asentaa [18]. Myös jokaisissa uusissa järjestelmähankinnoissa tulee huomioida kyberturvallisuusnäkökulma [31]. Terveydenhuollon kyberturvallisuuden rakentaminen on systeeminhallintaa, jossa tulee enemmän keskittyä kokonaisuuteen kuin yksittäisiin laitteisiin – jotta vältetään osaoptimoinnin vaara.

Terveydenhuollon tietoverkot kannattaa jakaa niin, että terveydenhuollon laitteet ovat omassa verkko-osiossaan erillään talotekniikan laitteista ja yleisistä työasemista [32]. Tämä mahdollistaa laitteiden paremman suojaamisen, vaikka niissä olisikin jouduttu tinkimään virustorjunnasta ja valvontaohjelmista. Etäyhteyden käytöstä on myös tehtävä asianmukaiset sopimukset tietojen suojaamisen ja vastuukysymysten vuoksi [14]. Tämä käsittää muun muassa palomuurin käytön, osapuolten vahvan tunnistamisen, yhteyden salaamisen ja henkilökohtaiset tunnukset etäyhteyden käyttöön. On myös hyödyllistä asettaa etäyhteyksiä tarvitsevat laitteet omaan verkkosegmenttiinsä, jolloin sisäverkon toiminta ei vaarannu etäyhteyksien mahdollisista haavoittuvuuksista.

Tärkeää on myös terveydenhuollon henkilökunnan toiminta, erityisesti kun haittaohjelmien tärkeä leviyskanava on sähköposti. Jokaisen tulee tunnistaa huijausyritykset [14]. Tällöin on tärkeää olla riittävän epäluuloinen ja tarkistaa viestin lähettäjä ja asia, arvioida muutoin viestin aitoutta (onko esim. jokin liian hyvää ollakseen totta) ja olla avaamatta liitetiedostoja ilman harkintaa.

Tietoturvaloukkauksia tapahtuu kuitenkin väistämättä, minkä vuoksi myös niiden sietokykyä pitää kehittää ja ylläpitää [31]. Sietokykyään kehittäneet organisaatiot eivät ole niin alttiita turvallisuusloukkauksille, ja toteutuneet hyökkäykset aiheuttavat yleensä vähemmän harmia. Organisaatioilla tulee olla toimintasuunnitelma kyberhyökkäyksien varalta [14]. Tähän sisältyy muun muassa ajantasainen laitelista järjestelmien ja ohjelmistojen ennakkoon arvioituine riippuvuuksineen, kybertilannetietoisuuden jatkuva ylläpito tietoturvatiedotteita seuraamalla ja haavoittuvuuksia havainnoimalla sekä havaittuihin haavoittuvuuksiin reagoimalla.

Kyberuhkatilanteita on tärkeää harjoitella niin organisaation sisällä kuin yhteiskunnan kokonaisturvallisuuden näkökulmasta sekä valtakunnallisissa että paikallisissa harjoituksissa. Kansallisia kyberharjoituksia on järjestetty vuodesta 2012 alkaen [33], ja tänä vuonna

Puolustusvoimat osallistui Naton kyberosaamiskeskuksen järjestämään maailman suurimpaan kyberpuolustusharjoitukseen [34]. Alueellisella tasolla järjestetään myös säännöllisesti erilaisia valmius- ja paikallispuolustusharjoituksia, joissa tavoitteena on viranomaisyhteistyön kehittäminen. Näissä harjoituksissa ovat tyypillisesti mukana myös sairaanhoitopiirit ja alueiden sosiaali- ja terveydenhuollon kuntayhtymät. Viime vuosina näissä harjoituksissa on harjoiteltu varautumista hybridiuhkiin, mikä sisältää myös kyberuhkat. [35–37]

Pohdinta

Terveydenhuolto on osa yhteiskunnan kriittistä infrastruktuuria, ja sen toimivuuden takaamiseksi kaikissa tilanteissa kyberturvallisuudesta huolehtiminen on keskeistä. Terveydenhuolto on kyberhyökkäyksien ykköskohde [3], ja hyökkäyksiä on raportoitu tapahtuneen kaikissa kybermaailman rakenteen viidessä kerroksessa. Jokaisessa kerroksessa on myös useita tunnistettuja haavoittuvuuksia [8]. Yhteiskunnan turvallisuusstrategian [2] mukaisesti varautumista tulee tehostaa organisaatioissa kaikilla tasoilla.

Tietoisuus kyberuhkista on lisääntynyt, mutta organisaatiot eivät välttämättä halua antaa kattavia tietoja toteutuneista hyökkäyksistä [21]. Tämä voi olla organisaatiolle jo imagokysymyskin. Tietojärjestelmät tyypillisesti tunnistetaan helpommin haavoittuviksi kuin yksittäiset laitteet, joiden tietoturva saattaa olla huomattavasti tietojärjestelmiä heikompaa [18]. Yksittäinen laite voi toimia porttina terveydenhuollon organisaation verkkoon, ja se voi olla väylä monenlaisille kyberhyökkäyksille, jotka pahimmillaan lamauttavat sairaalan toimintaa tai aiheuttavat potilasturvallisuusriskin [14, 18].

Varautumisen yksityiskohtien kertominen tavalliselle työntekijälle voi myös aiheuttaa organisaatiolle uhkan. Tiedon rajallisen saatavuuden vuoksi työntekijät helposti unohtavat arjen työssään kyberturvallisuusnäkökulman. Tutkimusten mukaan työntekijän toiminta (human factor) on organisaation kybervarautumisen heikoin lenkki [12]. Tämän vuoksi tietoisuuden kohottamisen ja henkilökunnan kouluttamisen tulee olla keskeisellä sijalla organisaation kyberturvallisuudessa.

Terveydenhuolto on toimialana kiinnostava kyberhyökkäyksiä tekeville yksittäisille ihmisille tai organisaatioille muun muassa sensitiivisen tietosisällön vuoksi. Terveydenhuollon kyberturvallisuuden jatkuva parantaminen ja tietoisuuden lisääminen ovat meidän kaikkien kansalaisten etuja. Kyberturvallisuuden parantaminen vaatii vahvaa ymmärrystä tietoturvasta ja myös terveydenhuollon toimintatavoista.

Terveydenhuollon kyberturvallisuustyöryhmä (Health Care Industry Cybersecurity Task Force, HCIC) on määritellyt kuusi ylätason kyberturvallisuussuositusta. Ne auttavat lisäämään tietoisuutta, hallitsemaan uhkia, vähentämään riskejä ja haavoittuvuuksia sekä toteuttamaan suojauksia, joita tällä hetkellä ei ole suurimmassa osassa terveydenhuollon sektoria. Vaatimukset ovat seuraavat:

1. Määritä ja tehosta terveydenhuollon kyberturvallisuuden johtajuutta, hallintotapaa ja tavoitteita.
2. Lisää lääkinnällisten laitteiden ja terveydenhuollon tietoturvaa ja resilienssiä.
3. Kehitä terveydenhuollon henkilöstön kyvykkyyttä kyberturvallisuustietoisuuden ja teknisten valmiuksien priorisoimiseksi ja varmistamiseksi.
4. Kasvata terveydenhuollon valmiutta parantamalla kyberturvallisuustietoisuutta ja -koulutusta.
5. Tunnista tarvittavat menettelytavat t&k-toiminnan ja tieto-omaisuuden (IPR) suojelemiseksi hyökkäyksiltä tai paljastumiselta.
6. Paranna tiedonvaihtoa uhkista, riskeistä ja toimenpiteistä. [38]

Jatkotutkimusten kenttä terveydenhuollon kyberturvallisuudessa on laaja. Laitehaavoittuvuuksien selvittelyn lisäksi tärkeä tutkimuskohde on terveydenhuollon henkilökunnan tietoisuus kyberturvallisuudesta. Mielenkiintoinen näkökulma on myös henkilökunnan tietoisuuden kohottaminen esimerkiksi verkko-opetusmateriaalilla ja kybertietouden mittaaminen ennen ja jälkeen koulutuksen.

Lähteet

[1] Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös / 22.1.2013. Turvallisuuskomitea; 2013. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

[2] Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös / 2.11.2017. Turvallisuuskomitea; 2017. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/YTS_2017_suomi.pdf

[3] Lehto M, Limnéll J, Innola E, Pöyhönen J, Rusi T, Salminen M. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Valtioneuvoston kanslia; 2017. Saatavilla: http://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

[4] European Commission – Speech, President Jean-Claude Juncker's State of the Union, Brussels, 13 September 2017. [Viitattu 22.4.2018]. Saatavilla: http://europa.eu/rapid/press-release_SPEECH-17-3165_en.htm

[5] Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020. Turvallisuuskomitea; 2017. Saatavilla: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

[6] Kyberturvallisuuden sanasto (TSK 52). Sanastokeskus TSK ry, Huoltovarmuuskeskus ja Turvallisuuskomitea; 2018. [Viitattu 19.6.2018]. Saatavilla: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

[7] Remenyi D, Wilson R. Glossary of Cyber Warfare, Cyber Crime, Cyber security. ACPI, UK; 2018.

[8] Lehto M. Kybermaailman ilmiöitä ja määrittelyjä. v 8.0. 1.9.2017. Informaatioteknologian tiedekunta, Jyväskylän yliopisto; 2017.

[9] Kuusisto T, Kuusisto R. Cyber World as a Social System. Teoksessa: Lehto M, Neittaanmäki P. (toim.) Cyber Security: Analytics, Technology and Automation, Intelligent Systems, Control and Automation: Science and Engineering 78, Springer International Publishing Switzerland; 2015. https://doi.org/10.1007/978-3-319-18302-2_2

[10] Libicki MC. Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York; 2007. https://doi.org/10.7249/CB407

[11] Lehto M. Phenomena in the Cyber World. In Lehto M, Neittaanmäki P (Edit.) Cyber Security: Analytics, Technology and Automation. Berlin: Springer; 2015. p. 3-29, https://doi.org/10.1007/978-3-319-18302-2_1

[12] The Human Factor in IT Security: How Employees are Making Businesses Vulnerable form Within. [Viitattu 22.4.2018]. Saatavilla: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

[13] Lehto M, Limnéll J, Kokkomäki T, Pöyhönen J, Salminen M. Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. Valtioneuvoston kanslia. Saatavilla: http://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf/efea3c33-3c74-4cf6-b237-d49b4f10ab83?version=1.0

[14] Terveydenhuoltoalan kyberuhkia. Viestintävirasto, Kyberturvallisuuskeskus; 2016. [Viitattu 29.4.2018]. Saatavilla: https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf

[15] Piggin R. Cybersecurity of medical devices: Addressing patient safety and the security of patient health information. BSI; 2017.

[16] Lehto M, Lehto M. Kyberturvallisuus sairaalajärjestelmissä: Osa 1. 14.8.2017. Informaatioteknologian tiedekunta, Jyväskylän yliopisto; 2017.

[17] Williams PAH, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical devices: Evidence and Research. 2015;(8):305-316. https://doi.org/10.2147/MDER.S50048

[18] Vartiainen J. Lääkintälaitteen turvallinen liittäminen sairaalan tietoverkkoon. Opinnäytetyö. Lahden ammattikorkeakoulu, tekniikan ala. Lahti; 2017. Saatavilla: http://urn.fi/URN:NBN:fi:amk-2017060212042

[19] New orangeworm attack group targets the health care sector in the US, Europe and Asia. Symantec Blogs 23.4.2018. [Viitattu 29.4.2018]. Saatavilla: https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

[20] Clarke R, Youngstein T. Cyberattack on Britain's National Health Service – A wakeup call for modern medicine. NEJM 2017;377(5):409-411. https://doi.org/10.1056/NEJMp1706754

[21] Kyberhyökkäykset lisääntyvät terveydenhuollossa. Potilaan lääkärilehti 5.6.2016. [Viitattu 29.4.2018]. Saatavilla: http://www.potilaanlaakarilehti.fi/uutiset/kyberhyokkaykset-lisaantyvat-terveyden-huollossa/

[22] Verkkohyökkääjät uhka sairaaloille, kyberhyökkäys voi asettaa potilaat hengenvaaraan. Verkkouutiset 27.10.2016. [Viitattu 29.4.2018]. Saatavilla: https://www.verkkouutiset.fi/verkkohyokkaajat-uhka-sairaaloille-kyberhyokkays-voi-asettaa-potilaat-hengenvaaraan-56934/

[23] Kelan Kanta-palvelut vaikeuksissa – syynä jälleen palvelunestohyökkäys. Yle Uutiset 3.6.2017. [Viitattu 29.4.2018]. Saatavilla: https://yle.fi/uutiset/3-9647957

[24] Palvelunestohyökkäys haittaa Kanta-palveluiden toimintaa. Yle uutiset 27.9.2017. [Viitattu 29.4.2018]. Saatavilla: https://yle.fi/uutiset/3-9854962

[25] Pekkarinen T. Kyberturvallisuus sairaalan eri toimialoilla. Sairaanhoitopiirien kyberturvallisuusseminaari 19.10.2016. [Viitattu 29.4.2018]. Saatavilla: http://ssty.fi/download/valmiusseminaari19102016/Pekkarinen_kybertuvallisuus_sairaalan_eri_toimialoilla.pdf

[26] Health care and cybersecurity: Increasing threats require increased capabilities. KPMG. [Viitattu 29.4.2018]. Saatavilla: https://assets.kpmg.com/content/dam/kpmg/pdf/2015/09/cyber-health-care-survey-kpmg-2015.pdf

[27] Kuusisto T. Kybertaistelu 2020. Taktiikan laitos. Julkaisusarja 2, No. 1/2014. Maanpuolustuskorkeakoulu. Saatavilla: http://urn.fi/URN:ISBN:978-951-25-2618-5

[28] Savossa otetaan kyberhärkää sarvista – tietoturvaan uppoaa 15 miljoonaa. TIVI 24.5.2016. [Viitattu 29.4.2018]. Saatavilla: https://www.tivi.fi/Kaikki_uutiset/savossa-otetaan-kyberharkaa-sarvista-tietoturvaan-uppoaa-15-miljoonaa-6553444

[29] Suomalaissairaala kahdentaa IT:tä ja parantaa palvelutasoaan 15 miljoonalla. TIVI 26.5.2016 [Viitattu 29.4.2018]. Saatavilla: https://www.tivi.fi/Kaikki_uutiset/suomalaissairaala-kahdentaa-it-ta-ja-parantaa-palvelutasoa-15-miljoonalla-6554183

[30] O'Dowd A. NHS patient data security is to be tightened after cyberattack. BMJ 2017;358;j3412. https://doi.org/10.1136/bmj.j3412

[31] Martin G, Martin P, Hankin C. Cybersecurity and healthcare: how safe we are? BMJ 2017;358;j3179. https://doi.org/10.1136/bmj.j3179

[32] Hemming T. Lääkinnällisten ja taloteknisten tietoverkkojen eriyttäminen. Sairaalatekniikan päivät 8.–9.2.2017, Hämeenlinna. [Viitattu 29.4.2018]. Saatavilla: http://ssty.fi/download/luentomateriaalit_sairaalatekniikan_paivat_2017/019_Tero_Hemming.pdf

[33] Kyberharjoitus alkaa Jyväskylässä. Helsingin Sanomat 18.5.2015 [Viitattu 4.5.2018]. Saatavilla: https://www.hs.fi/kotimaa/art-2000002824814.html

[34] Puolustusvoimat osallistuu jättikokoiseen kyberharjoitukseen. Yle uutiset 20.4.2018 [Viitattu 29.5.2018]. Saatavilla: https://yle.fi/uutiset/3-10169440

[35] POSA 2015 -valmiusharjoituksen teemana kyberuhat, tietojärjestelmien ja voimahuollon vakavat häiriöt Pohjois-Savossa. Itä-Suomen aluehallintovirasto 18.11.2015. [Viitattu 29.4.2018]. Saatavilla: https://www.avi.fi/web/avi/-/posa-2015-valmiusharjoituksen-teemana-kyberuhat-tietojarjestelmien-ja-voimahuollon-vakavat-hairiot-pohjois-savossa-ita-suomi-

[36] Yhteiskunnan häiriötilanne ei katso maakuntarajoja – Pirkka17 -harjoitus alkaa viikon kuluttua. AVI tiedote

2017. [Viitattu 29.4.2018]. Saatavilla: https://www.avi.fi/web/avi/-/yhteiskunnan-hairiotilanne-ei-katso-maakuntarajoja-pirkka17-harjoitus-alkaa-viikon-kuluttua-lansi-ja-sisa-suomi-

[37] Kuopio 18 -harjoitus kehittää viranomaisyhteistyötä Pohjois-Savossa. Maavoimat 19.2.2018. [Viitattu 29.4.2018]. Saatavilla: http://maavoimat.fi/artikkeli/-/asset_publisher/kuopio-18-harjoitus-kehittaa-viranomaisyhteistyota-pohjois-savossa

[38] Health Care Industry Cybersecurity Task Force, Report on Improving Cybersecurity in the Health Care Industry, June 2, 2017.