Elina Oksanen

Kyberresilienssin rooli sosiaalihuollon organisaatioiden toiminnassa

Tietotekniikan kandidaatintutkielma

13. joulukuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Elina Oksanen

Yhteystiedot: elina.p.oksanen@student.jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Kyberresilienssin rooli sosiaalihuollon organisaatioiden toiminnassa

Title in English: The Role of Cyber Resilience for the Organizations implementing Social Welfare Services

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 32+0

Tiivistelmä: Sosiaalihuollon toiminta on osa yhteiskunnan kriittisiä toimintoja ja toiminnan jatkuvuus tulee taata myös erilaisissa häiriötilanteissa. Kyberresilienssillä viitataan kykyyn kohdata digitaalisen maailman häiriötilanteita sekä palautua niistä takaisin normaaliin toimintaan häiriötilanteista oppien. Kyberresilienssiä ei ole aiemmin tutkittu sosiaalihuollon viitekehyksessä. Tässä tutkielmassa pyritään selvittämään sitä, millainen rooli kyberresilienssillä on sosiaalihuollon organisaatioiden toiminnassa. Terveydenhuollon toimintakentän on havaittu hyötyneen kybertoimintaympäristön sekä kyberresilienssin vahvistamisen toimenpiteistä. Myös sosiaalihuollon toimintakenttä voisi hyötyä samoista toimenpiteistä, mutta aihe kaipaa lisää tutkimusta.

Avainsanat: kyberturvallisuus, kyberresilienssi, sosiaalihuolto, jatkuvuudenhallinta

Abstract: The sector of Social Welfare is essential for ideally functioning society and it's services' continuity should be quaranteed in unexpected situations. Social Welfare Services must be offered on daily basis and also during exceptional conditions. Cyber resilience refers to an ability to cope with various disruptions in the digital world and to recover from them. Cyber resilience has not been studied within the sector of Social Welfare. This thesis aims to clarify the role of cyber resilience within the sector of Social Welfare. It has been observed that cyber resilience is important for the sector of Health Care. According to this, the sector of

Social Welfare might benefit from the same actions to improve it's cyber resilience. However, more research is needed to prove the importance of cyber resilience for the sector of Social Welfare.

Keywords: Cyber Security, Cyber Resilience, Social Services, Continuity Management

Sisällys

1 Johdanto

Kyber on läsnä kaikkialla. Se läpäisee yhteiskunnan, työelämän sekä vapaa-ajan tehden meidät kaikki yhä enenevissä määrin riippuvaisiksi itsestään. Elämämme jokaisella osa-alueella vaikuttava digitalisaatio sekä riippuvuutemme niin tietoverkoista kuin erilaisista teknologioista on nostanut riskiä erilaisten häiriötilanteiden kehittymiselle ja kyberhyökkäysten kohteeksi joutumiselle. Digitaalisen maailman aikaansaamia ja siellä ilmeneviä häiriötilanteita on mahdotonta välttää nykyisessä tietoyhteiskunnassa, minkä johdosta niihin tulee varautua etukäteen yhteiskunnan jokaisella tasolla ja joka sektorilla.

Sosiaalihuollon toimintasektori palveluineen on kiinteä osa hyvinvointiyhteiskuntaa ja sen digitaalista kehitystä, joten myös sosiaalihuollon tulee kehittyä vastaamaan yhä paremmin digitaalisuuden asettamiin vaatimuksiin. Sosiaalihuollon normaaliolojen toimintavalmiuden lisäksi toiminnan jatkuvuus on välttämätöntä myös erilaisissa häiriötilanteissa, ja esimerkiksi laajempien yhteiskunnallisten häiriötilanteiden aikana paine myös sosiaalihuollon palvelujen toteuttamiselle kasvaa. Lisäksi sosiaalihuollon toiminnassa käsitellään sensitiivisiä asiakastietoja, joiden johdosta toimintasektori on paitsi altis mahdollisille häiriötilanteille, myös houkutteleva kohde kyberhyökkäyksille. Näiden tekijöiden johdosta alan varautumiseen ja jatkuvuudenhallintaan tulee kiinnittää erityistä huomiota, ja näin vahvistaa alan kyberresilienssiä häiriötilanteiden varalle ja niistä toipumiseksi.

Tähän mennessä sosiaali- ja terveydenhuollon toimintasektorin varautumista, jatkuvuudenhallintaa ja resilienssiä on kirjallisuudessa ja tutkimuksissa käsitelty pääosin terveydenhuollon näkökulmasta, sillä terveydenhuollon palvelujen ja toimintojen digitalisoitumisella on pidemmät perinteet. Sosiaalihuollon osalta asiaan ei tehdyn tutkimuksen valossa ole juurikaan perehdytty, mistä johtuen aineistoa sosiaalihuollon varautumisesta on niukasti. Tämän tutkielman tavoitteena on kuvata kybertoimintaympäristöä sekä hahmottaa kyberresilienssin merkitystä varautumiselle ja jatkuvuudenhallinnalle. Tutkielmassa tarkastellaan sosiaalihuollon toimintasektorin toimintaa ja toiminnan linkittymistä kybertoimintaympäristöön, sekä kartoitetaan sitä, millaisia uhkia ja riskejä kybertoimintaympäristö sosiaalihuollolle asettaa. Lisäksi tutkielmassa perehdytään varautumisen ja jatkuvuudenhallinnan merkitykseen sekä siihen, millainen rooli kyberresilienssillä on sosiaalihuollon toimintasektorilla.

2 Resilienssi

Resilienssillä tarkoitetaan kykyä kohdata vastoinkäymisiä sekä erilaisia häiriö- ja muutostilanteita. Resilienssi on selviytymiskykyä ja paineensietokykyä, sekä kykyä hyödyntää käytettävissä olevia voimavaroja ja henkisiä resursseja tavoite- ja tulevaisuussuuntautuneesti. Resilienssin termi on omaksuttu monilla eri tieteenaloilla. Psykologian alueella resilienssillä viitataan yksilölliseen kykyyn selviytyä suurtakin stressiä aiheuttavista muutoksista ja kriisitilanteista (Lipponen (2020), 21-22). Politiikan kentällä termiä käytetään maailmanlaajuisesti kuvaamaan yhteiskuntien sopeutumista haasteisiin niin fyysisessä kuin digitaalisessa maailmassa, sekä esimerkiksi erilaisten maailmanlaajuisten ilmiöiden, kuten esimerkiksi ilmastonmuutoksen, kohtaamisessa (Kaufmann (2017), 4). Teknologian alan toimintaympäristössä resilienssillä viitataan riskinhallinnan ja turvallisuuden ulottuvuuteen osana monimuotoisia teknologisia ympäristöjä ja prosesseja. Tällöin resilienssi käsitetään organisaation kykynä ylläpitää toimintojaan äkillisissä häiriötilanteissa, palautua stabiiliin tilaan mahdollisimman nopeasti ja jatkaa tämän jälkeen normaalia toimintaansa (Wreathall (2006), 275). Tieto- ja viestintäteknologian viitekehyksessä resilienssin käsitettä voidaan tarkastella järjestelmien näkökulmasta, jolloin keskiössä ovat erilaiset tietojärjestelmät sekä niiden kyky kohdata häiriöitä ja palautua niistä (Kaufmann (2017), 21).

Digitaalinen yhteiskunta, jonka toiminnot ovat linkittyneitä niin tietoverkkoihin kuin toisiinsa, on altis häiriöille, sillä erilaiset häiriötilanteet vaikuttavat monella tasolla ja monissa järjestelmissä yhtä aikaa. Näiden monimutkaisten järjestelmien ja keskinäisten riippuvuussuhteiden määrittelemissä kompleksisissa kokonaisuuksissa resilienssillä on suuri merkitys, sillä linkittyneessä digitaalisessa maailmassa ilmenevillä häiriötilanteilla saattaa olla kauaskantoisia vaikutuksia myös fyysisessä maailmassa. (Kaufmann (2017), 101, 187.) Tämän kompleksisen kokonaisuuden häiriösietoisuutta kuvataan kyberresilienssin termillä. Kyberresilienssi määritellään kyvyksi kohdata ennakoitavissa olevia sekä ennakoimattomia digitaalisen maailman häiriötilanteita ja toipua niistä mahdollisimman tehokkaasti (Karjaluoto ym. (2019), 27).

2.1 Resilienssi yksilön näkökulmasta

Resilienssi on kiinteä osa ihmisen kokemaa turvallisuuden tunnetta, joka järkkyy, kun normaali turvallisuuden tila on uhattuna häiriö- tai kriisitilanteiden vallitessa (Limnéll, Majewski ja Salminen (2015), 35). Yksilön näkökulmasta resilienssissä on kyse paineensietokyvystä, muutosjoustavuudesta sekä henkisestä kyvystä sietää vaikeuksia ja selvitä vastoinkäymisistä. Resilienssi sisältää ajatuksen tavoitesuuntautuneisuudesta, jolloin sopeutuminen muuttuneeseen tilanteeseen auttaa pääsemään kohti tavoitetta. Erilaiset häiriö- ja kriisitilanteet voivat näin ollen tarjota mahdollisuuden oppimiseen, sillä ne ajavat väistämättä muutokseen ja aiempien ajattelu- ja toimintatapojen kehittämiseen. Kyse onkin yksittäisen hetken sijasta vaiheittaisesta prosessista, jossa tilanteen tunnistamisesta, tunnustamisesta sekä rutiinien ylläpidosta on mahdollista edetä kohti asteittaista edistymistä ja tilanteesta toipumista. (Lipponen (2020), 119, 144, 146, 150.)

Resilienssin termi voidaan jakaa sisäiseen ja ulkoiseen resilienssiin, jolloin sisäisellä resilienssillä viitataan yksilön psyykkiseen hyvinvointiin, kun taas ulkoisella resilienssillä tarkoitetaan yksilön kykyä selviytyä osana ympäröivää todellisuutta (Lipponen (2020), 26-27). Resilienssistä voidaankin vain harvoin puhua täysin yksilökeskeisesti, sillä kyse on lopulta yksilön sekä häntä ympäröivän yhteisön ja yhteiskunnan vuorovaikutuksesta ja yhteistoiminnasta. Resilienssi ei synny eikä kehity tyhjiössä, vaan se vaatii aktiivista vuorovaikutusta ympäristön kanssa (Kaufmann (2017), 28). Tästä näkökulmasta käsin tarkasteltuna resilienssi on enemmänkin kykyä muodostaa yhteys selviytymistä edistäviin ja ylläpitäviin psykologisiin, sosiaalisiin, kulttuurisiin sekä fyysisiin resursseihin (Lipponen (2020), 79-80).

2.2 Resilienssi ryhmien näkökulmasta

Resilienssillä on merkittävä rooli organisaatioiden toiminnassa. Organisaatiot muodostuvat ryhmistä ja ryhmät yksilöistä, jolloin jokaisen yksilön resilienssin tasolla on vaikutusta ryhmän toimintaan ja ryhmän toiminnalla puolestaan organisaation toimintaan. Organisaation näkökulmasta juuri ryhmätason resilienssillä on suurin vaikutus, sillä ryhmien kyky kriisi- ja muutostilanteiden kohtaamiseen sekä selviämiseen ja tilanteista oppimiseen on merkittävää organisaation selviytymisen kannalta.

Siinä missä psykologinen lähestymistapa tarkastelee resilienssiä etenkin yksilön näkökulmasta, sosiaalis-ekologiset lähestymistavat tarkastelevat sitä ryhmien ja yhteisöjen näkökulmasta (Kaufmann (2017), 20). Lipponen (2020) jaottelee ryhmissä esiintyvän resilienssin kolmeen sosiaalisen resilienssin ulottuvuuteen, joita ovat toimintakyvyn säilyttäminen muutostilanteissa, muutoksiin sopeutuminen sekä muuttuminen muutostilanteen seurauksena. On selvää, että jokaisen yksilön henkilökohtaisen resilienssin taso siirtyy suoraan organisaatioissa toimivien ryhmien toimintaan, mutta organisaatiolla itsellään on vaikutusta siihen, kuinka resilienssi yksilöiden ja ryhmien toiminnassa näyttäytyy. Näin ollen organisaation toimintakäytänteet joko mahdollistavat tai estävät resilienssin ilmenemisen, sillä organisaation toimintakulttuurilla on suora vaikutus siihen, kuinka kyvykäs se on kohtaamaan muutostilanteita. Työntekijöiden kasvua ja osallisuutta korostava johtamistyyli sekä työn tekemisen kulttuuri luovat pohjaa resilientin organisaation syntymiselle sekä epävarmoissa olosuhteissa menestymiselle. (Lipponen (2020) 271.) Resilienssi voidaankin nähdä paitsi yksilön ominaisuutena ja kyvykkyytenä, myös organisaation halukkuutena toimia resilienssiä kehittävällä tavalla sekä kykynä sitoutua tavoitteisiin ja toimia tavoitesuuntautuneesti myös haastavissa tilanteissa (Kaufmann (2017), 28).

2.3 Kyberresilienssi organisaatioiden toiminnan näkökulmasta

Limnéll, Majewski ja Salminen (2015) määrittelevät kyberresilienssin olevan yksi neljästä organisaation kyberturvallisuuden tasoa parantavasta tekijästä. Conklin ja Shoemaker (2017) kuvaavat kyberresilienssin kulkevan rinnakkain kyberturvallisuuden kanssa, jolloin kyberturvallisuuden toimenpiteet pyrkivät suojaamaan organisaatiota varsinaisilta häiriö- ja hyökkäystilanteilta, mutta kyberresilienssi vahvistaa organisaation toiminnan jatkuvuutta. Myös Stallings (2019), IBM (2020) sekä *The Cyber Resilience Index* (2022) korostavat kyberresilienssin merkitystä organisaatioiden toiminnan jatkuvuudelle, sillä sen avulla organisaatiot voivat lieventää taloudellisten tappioiden mahdollisuutta, vahvistaa asiakkaiden luottamusta sekä parantaa organisaation kilpailukykyä. Kyberresilienssin huomioiminen liiketoiminnan koko elinkaaren aikana niin strategisella kuin operatiivisella tasolla voi parantaa organisaation kyberresilienssin tasoa merkittävästi. (IBM (2020).

Kyberresilienssi syntyy eri tahojen ja toimijoiden yhteistoimintana ja vuorovaikutuksellisena

prosessina, jolloin prosessissa ovat osallisina niin yksilöt kuin erilaiset yhteisöt ja organisaatiot. Tällöin eri tahojen ja toimijoiden ennalta määrittelemät ja omaksumat turvallisuustoimet, sopimukset, prosessit, vastuunjaot, turvalliset käytänteet sekä lainsäädännön määrittämät reunaehdot muodostavat kokonaisuuden, joka selviää myös erilaisista häiriötilanteista. (Hausken (2020)) Lisäksi erilaiset viranomaisten ja muiden kyberturvallisia toimintaympäristöjä määrittelevien tahojen ohjeistukset tukevat organisaatioita kyberresilienssin parantamisessa ja toiminnan jatkuvuuden varmistamisessa. Kybertoimintaympäristön monimuotoisten uhkakuvien johdosta esimerkiksi Euroopan Unionin kyberturvallisuusvirasto on julkaissut yhteistyössä CERT-EU:n kanssa monivaiheisen ohjeistuksen suosituksineen, joiden avulla Euroopan Unionin alueella toimivat organisaatiot voivat parantaa kyberesilienssiään osana muuttuvaa kybertoimintaympäristöä (*Boosting your Organisations's Cyber Resilience* (2022)). Niin ikään Maailman talousfoorumi (WEF) on julkaissut yhdessä Accenturen kanssa oman viitekehyksensä organisaatioiden kyberresilienssin kehittämisen tukemiseksi. Sen suosittamien ohjeiden ja konkreettisten toimenpide-ehdotusten luvataan vastaavan sekä julkisen, että yksityisen sektorin tarpeisiin. (*The Cyber Resilience Index* (2022), 5-6.) Huomionarvoista on, että osalla toimijoista on suurempi vaikutus kyberresilienssin synnyssä ja ylläpidossa kuin toisilla eri toimijoiden rooleista ja vastuista johtuen, mutta tästä huolimatta prosessi on vuorovaikutteinen ja näin ollen myös häiriötilanteista voidaan toipua yhteistyöllä (Hausken (2020)).

Kyberresilienssin määritteleminen ja resilienssin tason mittaaminen organisaatiotasolla ei kuitenkaan ole ongelmatonta, sillä se koetaan terminä ja sisällöllisesti vieraaksi, eikä se ole hankalan mitattavuutensa vuoksi sisällytettävissä suoraan osaksi organisaatioiden toimintaa. Lisäksi, vaikka resilienssi ja turvallisuus liittyvätkin organisaatioiden kontekstissa saumattomasti toisiinsa, saattavat näistä olla kuitenkin vastuussa eri tahot, eikä myöskään sen vuoksi resilienssin mittaaminen ole aina järkevää, saati mahdollista sillä hetkellä käytössä olevilla menetelmillä. Euroopan Unionin kyberturvallisuusviraston (ENISA) julkaisema tutkimusraportti kuitenkin korostaa resilienssin merkitystä kybertoimintaympäristössä ja organisaatioiden toiminnassa, ja nostaa esiin tarpeen paitsi resilienssin mitattavuuden kehittämiseksi erilaisin investoinnein ja toimenpitein, myös tietoisuuden lisäämiseksi ja ohjeistusten kehittämiseksi. (Trimintzios (2011), 11-12, 15, 34.)

3 Kybertoimintaympäristön toiminta ja tavoitteet

Kybertoimintaympäristöllä tarkoitetaan tietokoneiden ja muiden teknisten laitteiden muodostamaa kokonaisuutta, jonka toiminta on täysin riippuvaista tietoverkoista sekä erilaisista tieto- ja viestintäteknologisista ratkaisuista. Kokonaisuuden toiminta perustuu laitteiden väliseen vuorovaikutukseen, sekä siihen informaatioon, jota laitteet käyttävät, varastoivat, käsittelevät ja prosessoivat toimintansa takaamiseksi. Tämän linkittyneen ja monimutkaisen ekosysteemin turvaaminen on kyberturvallisuuden sekä sen sisältämien prosessien ja toimenpiteiden päämäärä. (Stallings (2019), 3.) Täydellisen turvallisuuden saavuttaminen jokaisella osa-alueella ei kuitenkaan ole mahdollista, vaan kyberturvallisuuden rakentaminen vaatii priorisointia ja kerroksellisuutta. Lisäksi toimintaympäristöön liittyvien uhkien kuvasto on jatkuvassa muutoksessa, joten myös turvallisuusympäristön tarkastelun tulisi olla jatkuvaa. Kohteiden ja toimijoiden tunnistaminen, mahdollisten uhkien tunnistaminen ja keinot uhkilta suojautumiseen toimivat pohjana turvallisuuden rakentamiselle. (Limnéll, Majewski ja Salminen (2015), 29-30, 37.)

3.1 Kybertoimintaympäristö ja sen elementit

Kyberturvallisuus on kompleksinen kokonaisuus, jonka tarkoituksena on turvata siihen liittyvän toimintaympäristön, teknologioiden sekä toimintojen turvallisuus, toimintavalmius ja toiminnan jatkuvuus. Kybertoimintaympäristön sisältämän tiedon turvaamiseen sekä toiminnan mahdollistavien tietoverkkojen turvaamiseen tähdätään erilaisin teknologioin, toimenpitein, ohjeistuksin, standardein, työkaluin ja koulutuksin, sekä huolehtimalla riskiarviointien ja toiminta- sekä turvallisuuspolitiikkojen ajantasaisuudesta. Lisäksi jatkuva ja systemaattinen monitorointi, testaaminen, arviointi, palautteen kerääminen sekä toiminnan kehittäminen ovat osa alati muuttuvan kybertoimintaympäristön turvallisuuden varmistamista. (Stallings (2019), 34-37.)

Turvallisen kybertoimintaympäristön luomisen ja ylläpidon tueksi on julkaistu lukuisia kansainvälisiä standardeja. Kansainvälinen standardisoimisjärjestö International Organization for Standardization (ISO) on julkaissut tietoturvastandardien tuoteperheen, jonka käytetyim-

piä standardeja ovat ISO/IEC 27001, ISO/IEC 27002 ja ISO/IEC 27005. Lisäksi tuoteperheeseen kuuluu lukuisia muita standardeja turvallisen kybertoimintaympäristön luomisen ja ylläpidon tueksi. ("ISO/IEC 27001 and related standards" (2022)) National Institute of Standards and Technology (NIST) on julkaissut merkittäviä ja paljon käytettyjä standardeja, ohjeistuksia ja kyberturvallisuuden viitekehyksiä niin valtiollisten toimijoiden kuin muidenkin organisaatioiden toiminnan tueksi ("Cybersecurity" (2022)). Lisäksi voittoa tavoittelemattomien järjestöjen ja yksityishenkilöiden muodostama The Center for Internet Security (CIS) on julkaissut kansainvälisesti käytettyjä ohjeita ja toimintaperiaatteita organisaatioiden kybertoimintaympäristön turvaamiseksi ("Center for Internet Security" (2022)).

3.1.1 Teknologiat

Teknologiset ratkaisut ovat kybertoimintaympäristön ydintekijä. Teknologisiin ratkaisuihin luetaan esimerkiksi käytettävät laitteet, järjestelmät ja sovellukset, tietoverkot, tekniset toimintaympäristöt, lokitusjärjestelmät, fyysisten laitteiden suojaamiseksi käytettävät tekniset menetelmät sekä erilaiset identiteetin ja pääsynhallinnan teknologiat.

Teknisten laitteiden osalta keskiössä on paitsi käytettävien laitteiden riittävä turvallisuustaso, myös laitteen koko elinkaaren hallinta. Tietoverkkojen osalta huomio kiinnittyy etenkin konfigurointiin sekä käytettävien protokollien turvallisuuteen. Lokitusjärjestelmien avulla lokitiedon kerääminen eri järjestelmien käytöstä sekä mahdollisista tietoturvapoikkeamista on mahdollista. (Stallings (2019), 211, 217, 556-557.) Palomuurien avulla voidaan kontrolloida organisaation verkkoon kohdistuvaa tietoliikennettä (Stallings (2019), 290-291). Erillisten tunkeilijan havaitsemisjärjestelmien avulla voidaan puolestaan havaita mahdollisia organisaatioon kohdistuvia hyökkäyksiä. Niin ikään organisaation käyttämät järjestelmät ja sovellukset muodostavat omat riskinsä toiminnalle, joten niissä esiintyvien haavoittuvuuksien paikkaaminen ja järjestelmien jatkuva päivittäminen on olennaista. (Campbell (2016), 26, 148.) Myös identiteetin ja pääsynhallinnan kontrolloinnissa teknologiset ratkaisut ovat ensisijainen keino järjestelmien valtuudettoman käytön estämiseksi. Jotta käyttäjä voi päästä järjestelmiin, tulee tällä olla käytössään käyttöoikeudet määrittelevä identiteetti. Identiteetin luomisen jälkeen käyttäjän autentikaatio ja autorisaatio tähtäävät käyttäjän tunnistamiseen ja tunnistetun käyttäjän käyttövaltuuksien aktivoitumiseen. (Stallings (2019), 304-305.)

3.1.2 Prosessit

Organisaatioiden kybertoimintaympäristön suojaamisen toisena elementtinä toimivat erilaiset toimintaprosessit, joiden avulla pyritään varmistamaan riittävä turvallisuuden taso sekä minimoimaan riskejä, joita organisaation eri toimintoihin liittyy. Prosessit voivat liittyä esimerkiksi henkilöstöhallinnan, tiedonhallinnan tai liiketoiminnan prosesseihin.

Henkilöstöön liittyvät prosessit kattavat henkilöstöhallinnon käytänteisiin liittyvät prosessit, koulutuksiin liittyvät prosessit sekä henkilöstön toiminnan monitorointiin liittyvät prosessit työsuhteen aikana ja sen päättyessä. Tiedonhallinnan prosessihin kuuluvat esimerkiksi käytänteet organisaatiossa käsiteltävän tiedon suojaamisesta ja kategorisoinnista, tiedon käsittelystä sekä tietoturvaan ja tietosuojaan liittyvistä toimintaprosesseista. Liiketoiminnan prosesseihin voidaan puolestaan lukea esimerkiksi prosessit liittyen toiminnan jatkuvuuden suunnitteluun, riskiarviointien tekemiseen sekä häiriötilanteiden hallintaan. (Stallings (2019), 162-166, 176, 179, 205, 630, 642, 655.)

3.1.3 Ihmiset

Ihmiset ovat merkittävä kybertoimintaympäristön elementti, sillä parhaimmatkaan teknologiset ratkaisut organisaation kybertoimintaympäristön suojaamiseksi eivät ole riittäviä, mikäli henkilöstö ei noudata varovaisuutta tai turvallisuusmääräyksiä. Henkilöstöön saatetaan kohdistaa esimerkiksi erilaisia tietojenkalastelun toimenpiteitä, joiden kautta pyritään hankkimaan tietoja tai saamaan pääsy organisaation järjestelmiin. Ihmiset ovatkin usein organisaatioiden toimintaympäristön heikoin lenkki. (Campbell (2016), 113-117.) Organisaation henkilöstöllä on vastuu toimia työssään organisaation turvallisuusmääräyksiä sekä hyviä toimintakäytänteitä noudattaen. Tämä vaatii organisaatiolta aktiivista ja avointa toimintakulttuuria henkilöstön tietoisuuden ja osaamisen lisäämiseksi turvallista kybertoimintaympäristöä silmällä pitäen. Säännölliset koulutusrutiinit aihealueesta rooleineen ja vastuineen ovat henkilöstön osaamisen kehittämisen kannalta olennaisia tekijöitä, ja niiden kautta voidaan paitsi lisätä tietoisuutta turvallisen digitaalisen ympäristön ylläpitämisestä ja organisaation suojaamisesta, myös sitouttaa henkilöstöä vahvemmin osaksi organisaatiota. Huomionarvoista on, että organisaation turvallisuuskulttuurista on vastuussa koko organisaatiossa työs-

kentelevä henkilöstö. Näin ollen organisaation toteuttama turvallisuuskulttuuri, määräykset ja ohjeistukset koskevat kaikkia organisaation työntekijöitä, ja näistä tulee myös viestiä sen mukaisesti. (Stallings (2019), 168-170.)

Tietoturvallisuuden lisäksi henkilöstön osalta korostuu myös tietosuojaosaamisen merkitys. Henkilöstön tietosuojaosaaminen on paitsi ammatillista osaamista, myös oikeusturvaa parantava tekijä, ja lisäksi sen kautta voidaan vaikuttaa positiivisesti myös organisaation asiakasprosessien tehokkuuteen. Virheellinen asiakastietojen käsittely on organisaation toiminnan riskitekijä, joka voi pahimmillaan johtaa valvontaviranomaisten selvitysprosesseihin sekä tuomioistuinten langettamiin rangaistuksiin. Henkilötietojen puutteellinen ja lainsäädännön vastainen käsittely saattaakin pahimmillaan vaarantaa niin henkilöstön kuin asiakkaiden turvallisuuden kun esimerkiksi turvakiellon alaiset tiedot paljastuvat tai henkilöstön ja asiakkaiden tietoihin pääseminen mahdollistuu organisaation ulkopuolisille tahoille. (Andreasson, Koivisto ja Ylipartanen (2016), 27.)

3.2 Tietoturvan ja tietosuojan määrittelyä

Kybertoimintaympäristöön ja kyberturvallisuuteen kiinteästi liittyvä kokonaisuus on tietoturvallisuus. Tietoturvaan liittyvät tavoiteet voidaan jaotella lähteestä riippuen hieman eri tavoin. Stallings (2019) jakaa tavoitteet viiteen eri osa alueeseen, joita ovat luotettavuus, eheys, saatavuus, vastuu sekä autenttisuus. Campbell (2016), Andreasson, Koivisto ja Ylipartanen (2016) sekä Kyberturvallisuuskeskus (2020) puolestaan jakavat tavoitteet tiedon luotettavuuden, saatavuuden ja eheyden takaamiseen.

Järvinen ja Rousku (2017) niputtavat tietoturvallisuuteen liittyvät ja sitä määrittävät tekijät kolmen keskeisen tietoturvavaatimuksen alle, joista jokainen osa-alue tulee huomioida minkä tahansa alan organisaatiossa. Ensimmäinen näistä on lainsäädäntö, jonka avulla säädellään niin viranomaistoimijoiden kuin muidenkin organisaatioiden tietoturvaan liittyviä tekijöitä siten, että toiminta täyttää lakien ja asetusten määrittämät vaatimukset. Toisen vaatimuksen tietoturvalle asettavat asiakasvaatimukset sekä erilaiset sopimukset liittyen esimerkiksi tiettyyn palveluun ja sen toteuttamiseen, jolloin nämä vaatimukset ja sopimukset määrittävät vaadittavan tietoturvan tason. Kolmas tietoturvaan liittyvä näkökulma on liiketoiminnan

jatkuvuus, jolloin tietoturvaa tarkastellaan jatkuvuudenhallinnan ja riskinhallinnan näkökulmasta. Tietoturvaan liittyvien politiikkojen ja ratkaisujen päämääränä on puolestaan organisaation toiminnan turvaaminen, tiedon eheyden, luotettavuuden ja saatavuuden varmistaminen, sekä organisaation järjestelmien, verkkojen ja sovellusten valtuudettoman käytön estäminen. (Andreasson, Koivisto ja Ylipartanen (2016), 18.)

Tietoturvaan liittyy keskeisesti tietosuojan käsite. Tietosuojan avulla turvataan rekisteröidyn oikeudet häntä koskevien henkilötietojen käsittelyssä. Henkilötietojen käsittelyyn liittyvät toimenpiteet koostuvat tietojen keräämisestä, tallentamisesta, käytöstä, luovuttamisesta, säilyttämisestä, arkistoimisesta, hävittämisestä sekä siirrosta ulkomaille. Käsittelyyn saattaa näiden lisäksi liittyä myös muita henkilötietoihin kohdistuvia toimenpiteitä. Tietosuojan tarkoituksena onkin varmistaa, että rekisterinpitäjät noudattavat hyviä henkilötietojen käsittelykäytänteitä, jolloin tietojen käsittelyn edellytykset määrittyvät lainsäädännön perusteella. (Andreasson, Koivisto ja Ylipartanen (2016), 18, 27.)

3.3 Organisaation kyberresilienssin vahvistaminen

Stallings (2019) jakaa resilienssin termin järjestelmien resilienssiin (Information System Resilience) sekä liiketoiminnan resilienssiin (Business Resilience). Järjestelmien resilienssillä viitataan käytössä olevien järjestelmien toimintavalmiuteen myös häiriötilanteiden vallitessa sekä kykyyn palautua normaaliin tilaan häiriötilanteen jälkeen. Liiketoiminnan resilienssillä puolestaan tarkoitetaan organisaatioiden kykyä adaptoitua häiriötilanteisiin ja turvata liiketoiminnan jatkuvuus myös häiriötilanteen vallitessa. Liiketoiminnan resilienssin parantaminen koostuu sekä defensiivisistä että offensiivisista toimista prosessien vahvistamiseksi, häiriötilanteen aikaisen toiminnan varmistamiseksi ja häiriötilanteista palautumiseksi. (Stallings (2019), 639-640.) Kyberresilienssin vahvistaminen on organisaation toiminnan kannalta merkityksellistä ja prosessia voidaan tarkastella neljän vaiheen kautta sekä järjestelmät ja liiketoiminta, että toiminnan jatkuvuus huomioiden.

3.3.1 Varautuminen

Varautumisessa uhkien, riskien ja haavoittuvuuksien havaitseminen ja arviointi on tärkeää, sillä vasta tämän jälkeen on mahdollista varautua riittävällä tasolla. Uhkat voivat olla luonteeltaan joko konkreettisia tai abstrakteja, mutta vahingollisuutensa vuoksi niiden toteutuminen tulee pyrkiä estämään riittävin toimenpitein. Uhkat voivat muodostua paitsi organisaatioiden ulkopuolella, myös sisäisten toimijoiden ja toimintojen johdosta. (Limnéll, Majewski ja Salminen (2015), 103-104.) Kun uhkat, riskit ja haavoittuvuudet on organisaatiossa tunnistettu, voidaan laatia tavoitteet organisaatioiden kyberturvallisuudelle ja tarvittaville suojaustoimenpiteille (*The Cyber Resilience Index* (2022), 8). Monikerroksinen tietoturvaarkkitehtuuri auttaa organisaatiota varautumaan mahdollisiin häiriö- ja kyberhyökkäystilanteisiin ja tarvittaessa estää sen, ettei kyberhyökkäys epääse etenemään organisaatiossa yhdeltä kerrokselta seuraavalle. Varautumisessa tulee huomioida myös sisäisiltä uhkilta suojautuminen niin käyttäjien valtuuksia hallinnoimalla, kuin verkon segmentoinnilla. (*Kyberturvallisuus ja yrityksen hallituksen vastuu* (2020), 28–29.)

Riskienhallinta on osa varautumista sekä organisaatioiden johtamista ja toiminnan tukemista. Riskienhallinta on tavoitteellista toimintaa, joka käsittää sellaiset toimenpiteet, joiden avulla organisaatiot voivat käsitellä niihin kohdistuvia riskejä sekä pienentää realisoituvien riskien vaikutusta organisaation toimintaan. Riskienhallinnan ytimessä on ajantasainen kuva varteenotettavista ja realisoituvissa olevista riskeistä, joita organisaation toimintaan sisältyy. Organisaation toimintaan liittyy väistämättä riskejä, mutta niiden tunnistamisella sekä niihin varautumisella on merkittävä vaikutus organisaation toimintaan ja toiminnan jatkuvuuteen. (Rousku (2017), 11-13.) Organisaatioiden riskienhallinnassa tulee olla määriteltynä ja dokumentoituna tarkat toimintaohjeet sekä vastuujaot riskien realisoitumisen varalle. Riskienhallintaprosessi auttaa organisaatiota hahmottamaan riskienhallinnan kokonaisuutta vaiheineen ja vastuujakoineen. Riskienhallinnassa voidaan hyödyntää esimerkiksi SFS-ISO 31000 -riskienhallintastandardia, jonka avulla organisaatio voi arvioida ja käsitellä sen toimintaan kohdistuvia riskejä sekä määritellä mahdollisesti toteutuviin riskeihin vastaamisen periaatteet. (Rousku (2017), 19-27; Andreasson, Koivisto ja Ylipartanen (2016), 118-119.)

Harjoittelu on olennainen osa varautumista, sillä harjoittelun kautta voidaan tehdä näkyväksi organisaation todellinen valmiustila häiriötilanteiden varalle, arvioida reagointikykyä mah-

dollisten häiriötilanteiden tapahtuessa sekä tarkastella nykyisten prosessien ja säännösten toimivuutta. (Limnéll, Majewski ja Salminen (2015), 209.) Säännöllinen testaus ja tehtyjen toimenpiteiden arviointi sekä uhka-arviointien ja suojaustoimenpiteiden arviointi vahvistavat organisaation turvallisuuteen tähtäävien toimenpiteiden tehokkuutta. Lisäksi pääsyhallinnan politiikkoihin tulee kiinnittää huomiota riittävällä tasolla. (*Kyberturvallisuus ja yrityksen hallituksen vastuu* (2020), 30-31.)

3.3.2 Tilannetietoisuus

Tilannetietoisuudella tarkoitetaan realistisen ja ajantasaisen tilannekuvan muodostamista, joka on välttämättömyys oikea-aikaisten toimenpiteiden toteuttamiseksi. Ajantasaisen tilannekuvan muodostaminen muodostaa pohjan päätösten tekemiselle, jolloin hahmottuu myös kuva päätöksen vaikutuksista sekä mahdollisista riskeistä. Olennaista ajantasaisen tilannekuvan muodostamiselle on, että jollain on vastuu tilannekuvan hallinnoinnista, analysoinnista ja mahdollisten päätösten tekemisestä. Tilannekuvaan liittyvän tiedon tuleekin olla analysoitua ja ymmärrettävää, sekä terminologialtaan ja luokituksiltaan yhdenmukaista toiminta-alasta riippumatta. (Lehto ym. (2018), 39–40.)

Riittävän tilannekuvan muodostamiseksi organisaation tulee olla tietoinen kaikista sen käytössä olevista järjestelmistä, niiden keskinäisistä suhteista, sekä suhteesta organisaation ulkopuolisiin tahoihin ja järjestelmiin. Tämä tulisi tehdä paitsi teknisestä näkökulmasta, myös organisaation liiketoimintamalliin liittyvät tekijät huomioiden. Organisaation kaikilla toimintatasoilla tulisi olla riittävä ja ajantasainen tilannetietoisuus tarvittavien päätösten tekemiseksi. (Limnéll, Majewski ja Salminen (2015), 153-154, 215.)

3.3.3 Torjunta

Häiriötilanteiden tapahtuessa organisaatioiden tulee päättää välittömät toimenpiteet häiriötilanteeseen vastaamiseksi. Toimenpiteisiin vaikuttavat häiriön vakavuus ja välittömät uhat, organisaation järjestelmien suojaustaso, palveluiden kriittisyyden taso sekä mahdollinen leviämisuhka muihin järjestelmiin. Lisäksi toimenpiteistä päätettäessä on huomioitava käytössä olevat sekä ajalliset resurssit, jotka vaikuttavat häiriöstä toipumiseen. (Ilkka ym. (2017),

40–41.) Vastatoimenpiteet voidaan jaotella passiivisiin ja aktiivisiin vastatoimenpiteisiin. Passiivisiin toimenpiteisiin kuuluvat esimerkiksi säännöt ja asetukset sekä erilaiset organisatoriset turvallisuusratkaisut. Pääosin käytössä ovat passiiviset vastatoimenpiteet, sillä aktiiviset vastatoimenpiteet rikkovat lakia useissa maissa ja ne rajoittuvat pääosin asevoimien tai rikollisten tekemiin operaatioihin. (Limnéll, Majewski ja Salminen (2015), 190–191.)

Torjuntavaiheessa korostuu ajantasaisen tiedottamisen merkitys, sillä näin voidaan ylläpitää tietoisuutta jo tehdyistä toimenpiteistä sekä suunnitelluista jatkotoimenpiteistä. Samalla vältytään virheellisen tai puutteellisen tiedon leviämiseltä epävirallisten väylien kautta. Huomionarvoista on kuitenkin se, että mikäli häiriötilannetta tutkitaan rikoksena, ovat tällöin viestintävastuussa poliisin erikseen nimeämät edustajat. (Ilkka ym. (2017), 49.)

3.3.4 Palautuminen

Häiriötilanteesta palautuminen tapahtuu torjuntavaiheen jälkeen, kun on varmistuttu siitä, että tehdyt toimenpiteet ovat auttaneet ja paluu normaalitilaan on mahdollista. Palautuminen normaaliin tapahtuu sen jälkeen, kun tästä vastaava taho tekee asiasta päätöksen. Häiriötilanteeseen johtaneiden syiden analysointi, korjaavien toimenpiteiden toteuttaminen selkeine toipumismenettelyineen, jatkuvuussuunnitelmat sekä riittävät henkilöstöresurssit ovat vaatimuksia onnistuneelle palautumiselle. Häiriötilanne voi johtaa paitsi teknisiin korjaustoimenpiteisiin, myös tarpeeseen muuttaa totuttuja toimintatapoja ja tiukentaa aiempia tietoturvapolitiikkoja. Dokumentointi on ensiarvoisen tärkeää häiriötilanteesta toipumiseksi, sillä se mahdollistaa ennaltaehkäisevien toimenpiteiden toteuttamisen ja ohjeiden riittävän päivittämisen, sekä paljastaa mahdolliset koulutustarpeet. (Ilkka ym. (2017), 51–53.)

4 Sosiaalihuollon toimintasektori

Sosiaalihuollolla tarkoitetaan niitä yksilön, tämän lähipiirin sekä erilaisten yhteisöjen psyykkistä, fyysistä ja sosiaalista toimintakykyä edistäviä sosiaalipalveluita ja erilaisia tukipalveluita, joita toteutetaan sosiaalihuollon lainsäädännön pohjalta ja sosiaalihuollon palvelunantajien toimesta (Lehmuskoski, Suhonen, Palm ym. (2022), 97). Sosiaalihuolto jaetaan palvelutehtäviin, jotka määritellään Terveyden ja hyvinvoinnin laitoksen vuonna 2016 julkaistussa määräyksessä 1/2016. Määräyksen mukaiset palvelut voidaan jakaa palvelutehtävittäin peruspalveluihin (lapsiperheiden palvelut, työikäisten palvelut ja iäkkäiden palvelut), sekä erityispalveluihin (lastensuojelu, vammaispalvelut ja päihdehuolto). (*Määräys 1/2016* (2016)) Näiden lisäksi perheoikeudelliset palvelut muodostavat oman palvelutehtävänsä. Jokaisen palvelutehtävän alla järjestettävässä sosiaalipalvelussa on oma palveluprosessinsa, joka koostuu asian vireilletulokäsittelystä, palvelutarpeen arvioinnista, asiakkuuden suunnittelusta, palvelun järjestämisestä sekä palvelun toteuttamisesta. (Lehmuskoski, Suhonen, Palm ym. (2022), 99, 117-118.)

Julkisen sosiaalihuollon palveluiden järjestämisvastuu on kunnilla sekä kuntayhtymillä, jotka tuottavat palvelut joko itse tai ostopalveluna muilta kunnilta, yksityisiltä palveluntuottajilta tai järjestökentän eri toimijoilta. Kunnilla ja kuntayhtymillä oleva sosiaalipalveluiden järjestämisvastuu kuitenkin päättyy 31.12.2022, jolloin hyvinvointialueet aloittavat toimintansa. Täten sosiaalipalveluiden järjestämisvastuu siirtyy 1.1.2023 alkaen kunnilta ja kuntayhtymiltä hyvinvointialueille. (Lehmuskoski, Suhonen, Palm ym. (2022), 97-98.)

4.1 Sosiaalihuollon toiminta ja ohjaava lainsäädäntö

Sosiaalihuollon toimintaa ohjaa lainsäädäntö, joka määrittelee tarkasti sosiaalihuollon järjestämisvastuut, järjestettävät palvelut sekä jokaiseen palveluun liittyvän viranomaisprosessin. Sosiaalihuollon pohjana toimivat Suomen perustuslaki (731/1999), Laki sosiaali- ja terveydenhuollon järjestämisestä (612/2021), Laki sosiaali- ja terveydenhuollon suunnittelusta ja valtionavustuksesta (733/1992), Sosiaalihuoltolaki (1301/2014) sekä Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000). Näiden lisäksi on olemassa lukuisia erityisla-

keja, jotka määrittelevät tarkemmin eri sosiaalipalveluiden sisältöjä ja palveluiden toteuttamista. (“Lainsäädäntö” (2022))

Laki sosiaalihuollon asiakasasiakirjoista (254/2015) määrittelee sosiaalihuollon asiakkaiksi ne henkilöt, jotka hakevat ja käyttävät sosiaalihuollon palveluita. Sosiaalihuollon asiakkaita ovat myös henkilöt, jotka ovat sosiaalihuollon palveluiden kohteena tahdostaan riippumatta. Sosiaalihuoltoa koskee velvoite asiakasprosessin dokumentointiin ja dokumentoinnin tallentamiseen ja käsittelyyn lainsäädännössä määritetyllä tavalla (“Laki sosiaalihuollon asiakasasiakirjoista” (2015)). Sosiaalihuollon asiakirjojen sisältöä ja rakennetta koskevat määräykset laatii Terveyden ja hyvinvoinnin laitos sen mukaan, mitä reunaehtoja Laki sosiaalihuollon asiakasasiakirjoista (254/2015) kullekin kyseessä olevalle sosiaalipalvelulle asettaa. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021) puolestaan määrittelee reunaehdot sosiaali- ja terveydenhuollon asiakastietojen turvalliselle käsittelylle. Lisäksi laissa linjataan velvoite sosiaalihuollon palvelunantajien liittymisestä Kanta-palvelun ja tämän myötä Sosiaalihuollon asiakastiedon arkiston käyttäjäksi. Siirtyminen osaksi Kanta-palveluja tapahtuu asteittain palvelutehtävittäin määriteltyjen siirtymäaikojen puitteissa. (Lehmuskoski ym. (2022), 14, 138, 167.)

Muita keskeisiä sosiaalihuollon tiedonhallintaa määritteleviä lakeja ovat Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019), Tietosuojalaki (1050/2018), Laki viranomaisten toiminnan julkisuudesta (621/1999), Laki sähköisestä asioinnista (13/2003), Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista (617/2009), Laki digitaalisten palvelujen tarjoamisesta (306/2019), Laki väestötietojärjestelmästä ja Digi- ja väestötietoviraston varmennepalveluista (661/2009), Arkistolaki (831/1994) sekä EU:n yleinen tietosuoja-asetus (GDPR).

4.2 Sosiaalihuollon tietojärjestelmäarkkitehtuuri

Sosiaalihuollon tietojärjestelmäkokonaisuuteen kuuluu käyttöliittymän tarjoavia järjestelmiä, Kanta-kokonaisuuteen kuuluvia järjestelmiä sekä pääosin valtakunnallisia taustajärjestelmiä, jotka mahdollistavat tiettyjen toiminnallisuuksien toteutumisen, kuten ammattilaisen ammattioikeuksien tarkastamisen tai asiakkaan henkilötietojen hakemisen väestötietorekiste-

ristä. Käyttöliittymän tarjoavilla järjestelmillä tarkoitetaan sosiaalihuollon palvelunantajien omia asiakastietojärjestelmiä, jotka toimivat Kanta-viestinvälitysrajapinnan kautta Kanta-kokonaisuuteen kuuluvien järjestelmien kanssa. Kanta-palveluiden ympäristöön toteutettavia tietojärjestelmäpalveluita ovat puolestaan Sosiaalihuollon asiakastiedon arkisto, Omakanta sekä arkistonhoitajan käyttöliittymä. (Lehmuskoski ym. (2022), 23-24.)

Sosiaalihuollon asiakastietojärjestelmille on määritelty tietyt minimivaatimukset liittyen järjestelmien toiminnallisuuksiin ja tietosisältöihin, yhteentoimivuuteen Kanta-palveluiden kanssa sekä järjestelmien tietoturvaan ja tietosuoja-asioihin liittyen. Kuten terveydenhuollon potilastietojärjestelmät, myös sosiaalihuollon asiakastietojärjestelmät jaetaan Terveyden ja hyvinvoinnin laitoksen määräyksen 4/2021 mukaan luokkiin A ja B, sekä luokka A edelleen luokkiin A1, A2 ja A3. Kanta-palveluihin suoraan tai viestinvälitysrajapinnan kautta liittyvät asiakastietojärjestelmät kuuluvat luokkaan A. Alaluokkiin A1, A2 tai A3 kuuluminen määräytyy järjestelmän sisältämien asiakastietojen luonteen ja tietojen laajuuden, sekä käyttötarkoituksen ja kriittisyystason perusteella. Luokkaan B kuuluvat ne asiakastietojärjestelmät, joissä käsitellään asiakastietoa, mutta jotka eivät liity Kanta-palveluihin. Näiden lisäksi käytössä voi olla luokittelemattomia järjestelmiä, joissa ei käsitellä sosiaalihuollon asiakastietoa. Vastuu järjestelmien luokittelusta on järjestelmäpalvelun tuottajalla, joka vastaa myös asiakastietojen käsittelyyn liittyvien riskien arvioinnista ja mitoittaa järjestelmän tietoturvallisuuteen liittyvät tekijät tämän mukaisesti. (*Määräys 4/2021* (2021), 6-7.) Luokkaan A kuuluvia järjestelmiä sekä Kanta-palveluita koskee sertifioinnin vaatimus, johon kuuluu sekä tietoturva-auditointi, että Kelan järjestämä yhteistestaus. Lisäksi kaikki sosiaalihuollon asiakastietoa käsittelevät ja tuotantokäyttöön otettavat järjestelmät tulee ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirasto Valviran ylläpitämään rekisteriin. (Lehmuskoski, Suhonen, Palm ym. (2022), 69.)

4.3 Näkökulmia sosiaalihuollon varautumiseen ja kyberresilienssiin

Sosiaalihuollon toimintasektorille kohdistuvia uhkia ja toimintasektorilla esiintyviä riskejä ei ole juuri tutkittu, vaan tutkimus on painottunut terveydenhuollon toimintasektorin uhkiin, riskeihin ja realisoituneisiin häiriö- ja kyberhyökkäystilanteisiin. Tämän johdosta tässä kappaleessa tarkastellaan varautumista, riskienhallintaa sekä kybertoimintaympäristön turval-

lisuuden kehittämisen toimenpiteitä terveydenhuollon näkökulmasta käsin. Vaikka sosiaalihuolto ja terveydenhuolto poikkeavat sisällöiltään ja toiminnoiltaan merkittävästi, uhkakuvat lienevät molempien osalta kuitenkin saman suuntaisia. Kirjallisuuden mukaan sosiaalihuollon toimintakentältä ei ole vielä raportoitu samanlaisia laajoja ja vakavia kyberhyökkäystilanteita, joita terveydenhuollon toimintasektorille on maailmanlaajuisesti kohdistunut.

Terveydenhuollon toimintasektori on ollut kiihtyvään tahtiin kohteena niin pienemmille kuin massiivisemmillekin kyberhyökkäyksille. Pääasiallisia keinoja ovat olleet haittaohjelmat, palvelunestohyökkäykset sekä erilaiset ja eri asteiset tietomurrot. (Lehto, Pöyhönen ja Lehto (2019), 33; Ghayoomi ym. (2021); Iacono, Wojcieszek ja Glass (2022)) Terveydenhuolto nähdään houkuttelevana hyökkäyskohteena sensitiivisen tietosisältönsä vuoksi ja riski erilaisille hyökkäyksille kasvaa jatkuvasti, mikä nousee esiin myös eri tietoturvayhtiöiden raporteissa (*Threats Unmasked - Cyber Threat Intelligence Report* (2021); Iacono, Wojcieszek ja Glass (2022)). Tämän johdosta toimintatapojen jatkuva parantaminen on ensiarvoisen tärkeää (Lehto, Pöyhönen ja Lehto (2019), 32). Terveydenhuollossa ei kuitenkaan ole panostettu tietoturvaan samalla tavoin kuin muilla kriittisillä aloilla ja myös henkilöstön osaamisessa on raportoitu olevan puutteita (Garcia-Perez ym. (2022)). Kyberhyökkäyksen vaikutukset terveydenhuollossa ulottuvat potilaiden ja työntekijöiden yksityisyyteen ja turvallisuuteen, käytettävien tietojärjestelmien toimintaan, sekä toimintayksikön toimintakykyyn, talouteen ja maineeseen (Lehto, Pöyhönen ja Lehto (2019), 31-32).

Vaikka sosiaalihuollon toiminta poikkeaa sisällöiltään merkittävästi terveydenhuollosta, olisivat kyberhyökkäysten vaikutukset asiakasturvallisuuteen ja yksityisyyteen, henkilöstön turvallisuuteen, tietojärjestelmien toimivuuteen sekä toimintayksikön toimintaan, maineeseen ja talouteen terveydenhuollon tavoin merkittäviä. Näin ollen alan varautumiseen ja tämän kautta resilienssin parantamiseen tulee kiinnittää erityistä huomiota.

4.3.1 Varautuminen ja jatkuvuudenhallinta

Terveydenhuollon toimintasektorilla riskien on tutkittu ja havaittu kohdistuvan niin tietojärjestelmiin, ohjelmistoihin, pilvipalveluihin, langattomaan lähiverkkoon, lääkinnällisiin laitteisiin, henkilöstöön, fyysiseen toimintaympäristöön kuin etätyöhönkin (Vertainen ym. (2021),

12-13). Lehto, Pöyhönen ja Lehto (2019) listaavat lisäksi terveydenhuollon riskeiksi sairaalaympäristössä muunmuassa vialliset laitteet ja ohjelmistot, virheelliset tietoverkkojen määrittelyt, huonot turvallisuuskäytännöt, tietoturvapäivitysten asentamisen laiminlyömisen, heikot salasanapolitiikat, potilastietojen muuttamisen tai tuhoamisen, potilastietojen valtuudettoman käytön, luvattoman laitteen asetusten muuttamisen sekä mahdolliset palvelunestohyökkäykset ja haittaohjelmat. (Lehto, Pöyhönen ja Lehto (2019), 26-27, 32.)

Sosiaalihuollon tuottamat palvelut poikkeavat terveydenhuollon tuottamista palveluista. Kuitenkin toiminnan toteuttamisen kannalta uhkat lienevät hyvin samankaltaisia kohdistuen niin tietojärjestelmiin, ohjelmistoihin ja laitteisiin, fyysiseen toimintaympäristöön ja henkilöstöön, kuin etätyön mukanaan tuomiin uhkiin. *Valmius- ja jatkuvuudenhallintasuunnitelma - Ohje sosiaali- ja terveydenhuollon toimijoille* (2019) määrittelee sosiaalihuollon varautumisen tavoitteeksi yhteiskunnan keskeisten sosiaalipalveluiden saatavuuden ja toiminnan jatkuvuuden takaamisen, joten organisaation tulee määritellä kriittiset palvelut ja toiminnot, jotka sen tulee voida toteuttaa myös mahdollisessa häiriötilanteissa. Sosiaalihuollon osalta kriittisiksi toiminnoiksi lasketaan sosiaalipäivystys, lastensuojelu, laitos- ja asumispalvelut, kotiin vietävät palvelut sekä toimeentulotuki ja palvelutarpeen arviointi. Lisäksi koko yhteiskuntaa kohtaavissa poikkeustilanteissa sosiaalihuollon vastuulle tulee evakuointikeskusten toiminnan aloittaminen, hätämajoituksen järjestäminen sekä vaate- ja ruokahuollon tehtäviä. Myös viestintä ja ICT-palvelut ovat osa-alueita, joiden toimivuus korostuu häiriö- ja poikkeustilanteissa. (*Valmius- ja jatkuvuudenhallintasuunnitelma - Ohje sosiaali- ja terveydenhuollon toimijoille* (2019), 17,19,21, 27, 29.)

Riskeihin varautuminen ja jatkuvuudenhallinta vaativat selkeät prosessit vastuun jakoineen ja resursseineen. Tämä vaatii säännönmukaista riskien määrittelyä sekä paikallisesti että kansallisella tasolla, että tarkat toimenpidesuunnitelmat riskeihin vastaamiseksi ja niiden vaikutusten vähentämiseksi. Terveydenhuollon toimintasektorilla järjestelmien tulee taata toiminnan jatkuvuus, adaptoitua mahdollisiin muutoksiin sekä mukautua muuttuneeseen toimintaympäristöön niin, että toiminnan jatkuvuus mahdollistuu myös häiriötilanteissa. (Rogers ym. (2021)) Sosiaalialan toimintaan liittyy lisäksi eri palveluntuottajia sekä materiaalien toimittajia, jolloin varautumiseen liittyvät yksityiskohdat tulee kirjata myös sopimuksiin (*Valmius- ja jatkuvuudenhallintasuunnitelma - Ohje sosiaali- ja terveydenhuollon toimijoil-*

le (2019), 25, 27-29). Jatkuvuudenhallinnan prosesseihin kuuluu myös toimintaympäristön seuranta sekä poikkeamien ja väärinkäytösten systemaattinen havainnointi. Toteutuakseen kaikki edellä mainitut vaativat paitsi systemaattista suunnittelua ja häiriötilanteisiin varautumista asianmukaisin tietoturva- ja varautumissuunnitelmin, myös säännöllistä omavalvontaa sekä viranomaisvalvontaa. (Vuokko ym. (2022), 27-28, 31-32.)

4.3.2 Kybertoimintaympäristön vahvistaminen

Lehto, Pöyhönen ja Lehto (2019) jaottelevat terveydenhuollon toimintasektorin kyberturvallisuuden kehittämisen toimenpiteet strategisesta, operatiivisesta ja taktis-teknisestä näkökulmasta. Terveydenhuolto lasketaan mukaan yhteiskunnan kriittiseen infrastuktuuriin, jonka johdon tulee tehdä strategisia päätöksiä sekä seurata niiden toimeenpanoa tietoturvan näkökulma huomioiden läpi koko organisaation. Operatiivisten toimien kautta tähdätään strategisten tavoitteiden saavuttamiseen, jolloin huomio kiinnittyy tietoturvaratkaisujen toteuttamiseen sekä jatkuvuudenhallintaan. Taktis-tekninen näkökulma puolestaan liittyy kiinteästi laitteisiin ja järjestelmiin sekä niiden riittäviin suojaustoimenpiteisiin. (Lehto, Pöyhönen ja Lehto (2019), 64-65.) Sosiaalihuollon toiminnot luetaan kuuluvaksi kriittiseen infrastruktuuriin, joten samat kyberturvallisuuden edistämisen toimenpiteet tulevat kyseeseen myös sosiaalihuollon palveluita toteutettaessa.

Sosiaalihuollon tiedonhallinnan ratkaisuissa ja toimintamalleissa pätee terveydenhuollon tavoin vaatimus tietojen saatavuuteen, luotettavuuteen ja eheyteen, ja etenkin kriittiseksi luokitellun tiedon saatavuus sekä tietojoukkojen muuttumattomuus tulee pyrkiä turvaamaan. Huomionarvoista on, että vaikka sosiaalihuollon tietojärjestelmiin pätevät vaatimukset saatavuuden, käytettävyyden ja eheyden varmistamiseen ja ylläpitämiseen, on käytettävissä järjestelmissä havaittu myös puutteita. Salovaara ym. (2022) ovat tutkineet sosiaalihuollossa käytettäviä asiakastietojärjestelmiä ammattilasten ja työn toteutumisen näkökulmasta. Tutkimuksessa kartoitettiin sosiaalihuollossa työskentelevien korkeakoulutettujen työntekijöiden kokemia järjestelmien hyötyjä, toimivuutta, käytettävyyttä, tapauskohtaisen työn tukea, työn hallinnan tukea sekä tukea yhteistyölle ja tiedonkululle. Mikään mainituista osa-alueista ei kuitenkaan toteutunut toivotulla tavalla. (Salovaara ym. (2022), 198.)

Järjestelmien käytön osalta käyttövaltuuksien, käyttäjien roolien hallinnoinnin ja tietoturvan toimintakäytänteiden toteuttamisen tulee olla asianmukaisin keinoin säädeltyä (Vuokko ym. (2022), 32). Sosiaali- ja terveydenhuollon palvelunantajien on lakiin perustuen laadittava omavalvontasuunnitelma tietoturvaan, tietosuojaan sekä asiakastietoja sisältävien tietojärjestelmien käyttöön liittyen. Omavalvontasuunnitelma on osa tietosuojatyötä ja sen tarkoituksena on varmistaa henkilöstön osaaminen tietosuojaan liittyvistä periaatteista sekä toimialaan liittyvista tietoturvavaatimuksista rooleineen, vastuunjakoineen sekä sanktioineen. Lisäksi Kanta-palveluihin liittyvien asiakastietojärjestelmien osalta omavalvontasuunnitelmaan tulee kirjata, kuinka varmistetaan tietoturvavaatimukset valtakunnallisten palveluiden käytön osalta. (Andreasson, Koivisto ja Ylipartanen (2016), 83-84.)

5 Yhteenveto

Kirjallisuus ja kansainvälinen alan tutkimus on määritellyt tarkasti kybertoimintaympäristön sekä siihen liittyvät turvallisuuskäytänteet. Näitä tukevat erilaiset kansainvälisten organisaatioiden tuottamat tietoturvaan ja hyviin toimintakäytänteisiin liittyvät standardit sekä eri maiden lainsäädännön määrittelemät reunaehdot ja viranomaistahojen julkaisemat ohjeet. Kybertoimintaympäristön määritteleminen sosiaalihuollon viitekehykseen peilaten on kuitenkin kirjallisuuden ja tehdyn tutkimuksen valossa ollut hyvin minimaalista. Tämän johdosta tämän tutkielman puitteissa sosiaalihuoltoa koskeva taustamateriaali on ollut pääosin kansallista, sillä kansainvälistä tutkimusta aihealueesta ei juurikaan löytynyt. Terveydenhuollon osalta tilanne on kirjallisuuskatsauksen mukaan valoisampi, sillä aiheeseen on kiinnitetty vahvasti huomiota niin kansallisella kuin kansainvälisellä tasolla paitsi tietoturva, myös resilienssi huomioiden. Valitettavasti sosiaalihuollon osalta tilanne ei kuitenkaan vielä vaikuta olevan samanlainen.

Suomessa sosiaalihuollon osalta kaiken toiminnan pohjana toimii lainsäädäntö, joka paitsi määrittelee toteutettavan toiminnan reunaehtoineen, myös tavat sen toteuttamiseen sekä tietoturvallisten järjestelmien ja käytänteiden luomiseen. Kirjallisuuteen, tutkimuksiin, ohjeisiin ja oppaisiin sekä lainsäädäntöön peilaten sosiaalihuollossa on paitsi vahvuuksia kyberresilienssin näkökulmasta, myös varmasti tarvetta sen vahvistamiselle. Lainsäädännön määrittämät reunaehdot ja vaatimukset toiminnalle, käytettäville asiakastietojärjestelmille, tietosuojaperiaatteille sekä pääosin järjestäytynyt toimintakenttä näyttäytyvät vahvuuksina sosiaalihuollon kyberresilienssin muodostumiselle. Sosiaalihuolto on tarkasti säädeltyä viranomaistoimintaa, jonka suojaustaso sekä varautumiskäytänteet lienevät sen mukaisia. Poikkeuksen tälle luonee viranomaistoiminnasta erillään toimiva sosiaalialan järjestökenttä, jonka osuutta ei tämän tutkielman puitteissa kuitenkaan kartoitettu.

Tutkielmaa tehdessä esiin nousi kuitenkin myös mahdollisia kehitystarpeita, joihin tulisi kiinnittää huomiota sosiaalihuollon toimintakentällä. Koska kansainvälistä tutkimusta sosiaalihuollon kyberresilienssistä ei ole löydettävissä, on tässä tutkielmassa kyberresilienssiä peilattu terveydenhuollon viitekehykseen. Kyberturvallisuuden ja tämän myötä kyberresilienssin parantamiseksi myös sosiaalihuolto voisi hyötyä samoista toimenpiteistä, joita

terveydenhuollon toimintakentälle on tutkimusten mukaan suositeltu. Strategisen tason päätöksenteko tietoturvanäkökulmat ja mahdolliset riskit aidosti huomioiden, selkeät ja tarkasti dokumentoidut jatkuvuudenhallinnan periaatteet ja tietoturvaratkaisut, sekä päivitetyt, oikein konfiguroidut ja käyttövaltuuksiltaan ajantasaiset järjestelmät ja laitteet ovat tutkimusten mukaan välttämättömyys terveydenhuollon turvallisen kybertoimintaympäristön rakentumisessa ja tämän myötä kyberresilienssin vahvistamisessa. Samoista suosituksista ja toimenpiteistä voisi hyötyä myös sosiaalihuollon toimintakenttä. Lisäksi huomiota tulee kirjallisuuden perusteella kiinnittää henkilöstön osaamiseen ja säännölliseen lisäkoulutukseen tietoturvakysymyksissä niin toiminnan, käyttöoikeuksien kuin salasanapolitiikkojenkin kannalta.

Tämän tutkielman puitteissa tehdyn kirjallisuuskatsauksen perusteella johtamisella ja organisaation toimintakulttuurilla vaikuttaa olevan merkitystä resilienssin kehittymiseen yksilö-, ryhmä- ja organisaatiotasoilla. Sosiaalihuollon osalta herää kuitenkin ajatus siitä, millaisia vaikutuksia mahdolliset puutteet työn ja toiminnan resurssoinneissa, johtamisessa, toimintatavoissa ja ohjeistuksissa saattavat aiheuttaa toiminnan jatkuvuudelle muutoinkin raskaalla toimialalla. Työkenttä itsessään on haastava, joten mikäli toiminnan resurssoinnissa on puutteita ja henkilöstön työkuorma on suuri, organisaatioiden toimintakäytänteet ja ohjeistukset ovat puutteellisia, tai mikäli riittävät ohjeistukset esimerkiksi tietoturvallisiin käytänteisiin puuttuvat kokonaan, on organisaatio tällöin melko altis häiriöille ja sen aikaansaamille vaikutuksille. Lisäksi mikäli teknologisten ratkaisujen käyttö on vierasta tai käytön opettelulle ei päivittäisten toimintojen lomassa ole aikaa, riskit kasvavat entisestään. Nämä näkökulmat korostavat entisestään organisaation johdon vastuuta ja sitoutumista turvallisen kybertoimintaympäristön luomiseen, säännölliseen riskienhallintaan, tarkkojen toimenpiteiden määrittämiseen, tulosten seuraamiseen sekä ympäristön monitorointiin ja henkilöstön sitouttamiseen ja kouluttamiseen.

Varmojen johtopäätösten tekeminen sosiaalihuollon toimintaympäristön kyberresilienssistä vaatisi kuitenkin lisätutkimusta. Aiemman tutkimuksen puuttuessa soveltaminen terveydenhuollon puolelta viitoittanee tietä jossain määrin, mutta suora vertaaminen terveydenhuollon viitekehykseen ei kuitenkaan ole mahdollista alojen sisällöllisten ja toiminnallisten eroavaisuuksien vuoksi. Tämä kirjallisuuskatsaus antoi kuitenkin viitteitä siitä, että sosiaalihuolto voisi mahdollisesti hyötyä samanlaisesta kybertoimintaympäristön kartoituksesta ja jatku-

vuudenhallinnan prosessien tutkimisesta, mitä terveydenhuollon toimintakentällä on jo toteutettu kyberresilienssin näkökulma huomioiden. Näin voitaisiin myös varmistua siitä, että sosiaalihuollon jatkuvuudenhallinta, riskienhallinnan prosessit sekä kyberresilienssi tulisivat huomioiduksi terveydenhuollon kyberresilienssin tavoin.

Lähteet

Andreasson, A., J. Koivisto ja A. Ylipartanen. 2016. *Tietosuojakäsikirja johdolle.* 3. painos. Tallinna: Printon: Helsinki: Tietosanoma Oy.

Boosting your Organisations's Cyber Resilience: Joint Publication 22-01. 2022, 14. helmikuuta 2022. Viitattu 23. marraskuuta 2022. https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience.

Campbell, Tony. 2016. *Practical Information Security Management: A Complete Guide to Planning and Implementation.* New York, NY: Apress.

"Center for Internet Security". 2022. Viitattu 20. marraskuuta 2022. https://www.cisecurity.org/.

Conklin, W. A., ja D. Shoemaker. 2017. "Cyber-Resilience: Seven Steps for Institutional Survival". *EDPACS* 55:14–22.

"Cybersecurity". 2022. Viitattu 20. marraskuuta 2022. https://www.nist.gov/cybersecurity.

Garcia-Perez, A., J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro ja A. Chinnaswamy. 2022. "Resilience in healthcare systems: Cyber security and digital transformation". *Technovation.*

Ghayoomi, H., K. Laskey, E. Miller-Hooks, C. Hooks ja M. Tariverdi. 2021. "Assessing resilience of hospitals to cyberattack". *Digital health,* p.20552076211059366–20552076211059366.

Hausken, K. 2020. "Cyber resilience in firms, organizations and societies". *Internet of Things* 11. https://doi.org/10.1016/j.iot.2020.100204.

Iacono, L., K. Wojcieszek ja G. Glass. 2022. "Q2 2022 Threat Landscape: Ransomware Returns, Healthcare Hit", 10. elokuuta 2022. Viitattu 11. joulukuuta 2022. https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q2-2022-threat-landscape-ransomware-healthcare-hit.

IBM. 2020. "What is cyber resilience?" Viitattu 26. marraskuuta 2022. https://www.ibm.com/topics/cyber-resilience.

Ilkka, J., A. Sahlman, H. Mäntylä, J. Hartikainen, K. Janhunen, K. Grönroos, M. Raappana ym. 2017. *Tietoturvapoikkeamatilanteiden hallinta: Valtiovarainministeriön julkaisuja 8/2017,* helmikuu. Viitattu 26. marraskuuta 2022. https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf.

"ISO/IEC 27001 and related standards: Information security management". 2022. Viitattu 20. marraskuuta 2022. https://www.iso.org/isoiec-27001-information-security.html.

Järvinen, P., ja K. Rousku. 2017. *Työpaikan tietoturvaopas: tunnista uhat, hallitse riskit.* Helsinki: Alma Talent.

Karjaluoto, A., Ü. Parts, R. Lehtinen ja T. Frantti. 2019. *Kasvua digitaalisesta turvallisuudesta: Tiekartta 2019–2030.* Helsinki: Työ- ja elinkeinoministeriö. Viitattu 10. marraskuuta 2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161428/TEM_17_19_Digitaalisen_turv_tiekartta_WEB.pdf?sequence=1&isAllowed=y.

Kaufmann, M. 2017. *Resilience, Emergencies and the Internet: Security In-Formation.* Toimittanut David Chandler. Routledge Studies in Resilience. Abingdon, Oxon : Routledge.

Kyberturvallisuus ja yrityksen hallituksen vastuu. 2020. Versio Traficomin julkaisuja 2/2020, helmikuu. Viitattu 26. marraskuuta 2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf.

Kyberturvallisuuskeskus. 2020. "Tietoturva". Viitattu 26. marraskuuta 2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

"Lainsäädäntö". 2022. Viitattu 9. marraskuuta 2022. https://stm.fi/sotepalvelut/lainsaadanto.

"Laki sosiaalihuollon asiakasasiakirjoista". 2015, 20. maaliskuuta 2015. Viitattu 10. marraskuuta 2022. https://www.finlex.fi/fi/laki/alkup/2015/20150254#Pidm45949345597024.

Lehmuskoski, A., ym. 2022. *Kanta-käsikirja sosiaalihuollon toimijoille.* Syyskuu. https://yhteistyotilat.fi/wiki08/pages/viewpage.action?pageId=61058878&preview=/61058878/91106493/Kanta-palvelujen%20k%C3%A4sikirja%20sosiaalihuollon%20toimijoille%20v3-2.pdf.

Lehmuskoski, A., M. Suhonen, N. Palm ym. 2022. *Kanta-palvelujen käsikirja sosiaalihuollon toimijoille.* Syyskuu. Viitattu 9. marraskuuta 2022. https://yhteistyotilat.fi/wiki08/pages/viewpage.action?pageId=61058878&preview=/61058878/91106493/Kanta-palvelujen%20k%C3%A4sikirja%20sosiaalihuollon%20toimijoille%20v3-2.pdf.

Lehto, M., J. Limnéll, T. Kokkomäki, J. Pöyhönen ja M. Salminen. 2018. *Kyberturvallisuuden strateginen johtaminen Suomessa.* Versio Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018, 29. maaliskuuta 2018. Viitattu 26. marraskuuta 2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf.

Lehto, M., J. Pöyhönen ja M. Lehto. 2019. *Kyberturvallisuus sosiaali- ja terveydenhuollossa: Loppuraportti Vol 2.* Viitattu 6. lokakuuta 2022. https://jyx.jyu.fi/bitstream/handle/123456789/63325/Kyberturvallisuus_Vol2FINAL.pdf.

Limnéll, J., K. Majewski ja M. Salminen. 2015. *Cyber Security for Desicion Makers.* Toimittanut Raj Samani. Docendo.

Lipponen, K. 2020. *Resilienssi arjessa.* Helsinki: Duodecim.

Määräys 1/2016: Määräys sosiaalihuollon palvelutehtävien luokituksesta. 2016. Versio THL 1419/4.00.00/2015, 16. helmikuuta 2016. Viitattu 9. marraskuuta 2022. https://www.thl.fi/attachments/tiedonhallinta/Maarays_1_2016_sosiaalihuolto.pdf.

Määräys 4/2021: Määräys sosiaali- ja terveydenhuollon tietojarjestelmien luokittelusta ja sertifioinnista. 2021. Versio THL/4310/4.09.00/2021, 9. joulukuuta 2021. Viitattu 25. marraskuuta 2022. https://thl.fi/documents/920442/2816495/THL-Maarays_4-2021_Sote-tietojarj_Luokittelu-Sertifiointi.pdf.

Rogers, H. L., Barros P. P., J. De Maeseneer, L. Lehtonen, C. Lionis, M. McKee, L. Siciliani, D. Stahl, J. Zalatel ja D. Kringos. 2021. “Resilience Testing of Health Systems: How Can It Be Done?” *International journal of environmental research and public health,* p.4742.

Rousku, K. 2017. *Ohje riskienhallintaan: Valtiovarainministeriön julkaisuja 22/2017.* Valtiovarainministeriö, Julkisen hallinnon ICT, 2. kesäkuuta 2017. Viitattu 15. marraskuuta 2022. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf.

Salovaara, S., K. Ylönen, M. Silén, J. Viitanen, T. Lääveri ja S. Hautala. 2022. “Sosiaalialan korkeakoulutettujen ammattilaisten arviot asiakastietojärjestelmistä 2020”. *Finnish Journal of eHealth and eWelfare.*

Stallings, W. 2019. *Effective Cybersecyurity - A Guide to Using Best Practices and Standards.* Upper Saddle River, NJ: Addison-Wesley.

The Cyber Resilience Index: Advancing Organizational Cyber Resilience. 2022, heinäkuu. Viitattu 11. marraskuuta 2022. https://www3.weforum.org/docs/WEF_Cyber_Resilience_Index_2022.pdf.

Threats Unmasked - Cyber Threat Intelligence Report. 2021. Viitattu 11. joulukuuta 2022. https://www.accenture.com/_acnmedia/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report.pdf.

Trimintzios, P. 2011. *Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations.* European Network / Information Security Agency (ENISA), 1. helmikuuta 2011. Viitattu 23. marraskuuta 2022. https://www.enisa.europa.eu/publications/metrics-survey.

Valmius- ja jatkuvuudenhallintasuunnitelma - Ohje sosiaali- ja terveydenhuollon toimijoille: Sosiaali- ja terveysministeriön julkaisuja 2019:10. 2019. https://julkaisut.valtioneuvosto.fi/handle/10024/161627.

Vertainen, V., E. Suni, M. Vatanen, J. Hautamäki, T. Laava ja J. Piispanen. 2021. *Kyberhäiriöiden hallinta: Käsikirja terveydenhuollon toimijoille.* https://jyvsectec.fi/wp-content/uploads/2020/12/kyberhairioiden-hallinta-kasikirja-terveydenhuollon-toimijoille.pdf.

Woods, D., D., E. Hollnagel ja N. Leveson, toimittaneet. 2006. *Resilience Engineering: Concepts and Precepts: Properties of Resilient Organizations: An Initial View.* Aldershot, England; Burlington, VT: Ash gate.

Vuokko, R., M. Huovila, M. Pentikäinen, J. Mykkänen, T. Siira ja M. Jalonen. 2022. *Sosiaali- ja terveydenhuollon kokonaisarkkitehtuuri: tiedonhallinnan yhteiset periaatteet ja kuvaukset.* Toukokuu. Viitattu 10. marraskuuta 2022. https://yhteistyotilat.fi/wiki08/display/SYPLJULK?preview=/85934658/86868907/Sosiaali-%20ja%20terveydenhuollon%20kokonaisarkkitehtuuri_%20tiedonhallinnan%20yhteiset%20periaatteet%20ja%20kuvaukset_2022_05_20.pdf.