Täydennyskoulutukseen osallistuneiden näkökulmia kyberturvallisuuteen sosiaali- ja terveysalalla

Tiia Haaranen

Opinnäytetyö, ylempi AMK
Joulukuu 2024
Projektijohtamisen tutkinto-ohjelma (YAMK), sosiaali- ja terveysala

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Haaranen, Tiia

Täydennyskoulutukseen osallistuneiden näkökulmia kyberturvallisuuteen sosiaali- ja terveysalalla

Jyväskylä: Jyväskylän ammattikorkeakoulu. Joulukuu 2024, 66 sivua.

Projektijohtamisen tutkinto-ohjelma (YAMK), sosiaali- ja terveysala. Opinnäytetyö ylempi AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Kyberturvallisuus on noussut yhä keskeisemmäksi aiheeksi nykypäivän digitalisoituneessa maailmassa. Kyberhyökkäykset ovat muuttuneet aiempaa vakavimmiksi ja kohdennetuimmiksi. Sosiaali- ja terveysala on yksi eniten verkkohyökkäysten kohteena olevista aloista maailmanlaajuisesti. Kyberhyökkäykset voivat vaikuttaa negatiivisesti niin yksilöön kuin organisaatioon. Kyberturvallisuuden hallinnassa suurin riskitekijä on ihminen itse. Tarkoituksenmukainen ja ajantasainen koulutus on keskeistä, jotta inhimillisen tekijän aiheuttama riski saadaan minimoitua. Tietämättömyydestä tai ajattelemattomuudesta johtuvia kyberturvallisuutta heikentäviä toimia voidaan vähentää laadukkaalla koulutuksella.

Täydennyskoulutukseen osallistuvien sosiaali- ja terveysalan ammattilaisten näkökulmasta selvitettiin niitä kyberturvallisuuden seikkoja, jotka vaikuttavat kyberturvallisuutta lisäävästi. Lisäksi tarkasteltiin sitä, miten täydennyskoulutus vaikutti osallistujien kyberturvallisuusosaamiseen. Aineisto kerättiin täydennyskoulutuksen viimeisen opintojaksotehtävän reflektio-osuuden avoimista kysymyksistä. Niissä pohdittiin muun muassa opintojakson sisältöä suhteessa kyberturvallisuuteen, sosiaali- ja terveysalan ammattilaisen osaamisen tarpeita sekä oppimista. Opinnäytetyö toteutettiin laadullisin eli kvalitatiivisin menetelmin. Opinnäytetyön lähestymistavassa mukailtiin fenomenologiaa ja aineiston analyysissa hyödynnettiin induktiivista sisällönanalyysia.

Opinnäytetyössä tunnistettiin viisi kokonaisuutta kuvaamaan kyberturvallisuutta edistäviä tekijöitä: (1) osaaminen ja ymmärrys, (2) yksilön vastuullinen toiminta, (3) organisaation panostus kyberturvallisuuteen, (4) organisaation kyberturvallisuuskäytänteet sekä (5) järjestelmien ja laitteiden turvallisuus. Nämä kyberturvallisuutta lisäävät tekijät korostavat osaamisen, organisaation käytänteiden sekä työntekijöiden roolin merkitystä kyberturvallisuutta lisäävinä teemoina. Lisäksi havaittiin kolme kokonaisuutta, jotka kuvaavat täydennyskoulutuksen vaikutuksia osaamisen kehittymiseen: (1) kyberturvallisuuden perusasioiden oppiminen, kertaaminen sekä tietojen soveltaminen käytäntöön, (2) ymmärrys kyberturvallisuuden dynaamisuudesta ja (3) organisaation ja yksilön roolien ymmärrys kyberturvallisuuden toteuttajina.

Tuloksia voidaan hyödyntää suunniteltaessa sosiaali- ja terveysalalle kohdennettuja kyberturvallisuuteen liittyviä kokonaisuuksia. Näitä ovat esimerkiksi organisaation perehdytysohjelmat, osaamisen kehittäminen, täydennyskoulutukset sekä koulutusohjelmien kehittäminen.

Avainsanat (asiasanat)

kyberturvallisuus, kyberuhka, kyberresilienssi, sosiaali- ja terveysala, osaaminen, täydennyskoulutus

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Haaranen, Tiia

Perspectives on Cybersecurity in the Social and Health care: Insights from Continuing Education Participants

Jyväskylä: JAMK University of Applied Sciences, December 2024, 66 pages.

Master's Degree Programme in Professional Project Management, Social and Health Care. Master's thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

Cybersecurity has become an increasingly important in today's digital world. Cyber attacks have become more serious and targeted. The social and health care sector is one of the sectors most affected by cyber attacks worldwide. Cyber attacks can have a negative impact on both the individual and the organisation. The biggest risk factor in managing cybersecurity is the human factor. Appropriate and up-to-date training is essential to minimise the risk posed by the human factor. Quality training can reduce cybersecurity breaches caused by ignorance or carelessness.

From the perspective of social and health professionals participating in the continuing education programme, the cybersecurity issues that contribute to cybersecurity were identified. In addition, the impact of the education on the cybersecurity skills of the participants was examined. The material for the study was collected from the open-ended questions of the reflection part of the final module. These questions included a discussion of the course content in relation to cybersecurity, the competency needs of social and health care professionals, and learning. The thesis was conducted using qualitative methods. The research approach was based on phenomenology and the data analysis was based on inductive content analysis.

The study identified five entities to describe the drivers of cybersecurity: (1) knowledge and understanding, (2) individual responsibility, (3) organisational commitment to cybersecurity, (4) organisational cybersecurity practices and (5) system and equipment security. These cybersecurity drivers highlight the importance of skills, organisational practices and the role of employees as cybersecurity issues. In addition, three themes were identified that describe the impact of continuing education on skills development: (1) learning, refreshing and applying the basics of cybersecurity, (2) understanding the dynamics of cybersecurity, and (3) understanding the roles of the organization and the individual as implementers of cybersecurity.

The results can be used in designing targeted cybersecurity entities for the social and health sector. These include organisational orientation programmes, skills development, continuing education and the development of training programmes.

Keywords/tags (subjects)

cybersecurity, cyber threat, cyber resilience, social and health care, competence, continuing education

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

1 Johdanto

Kyberturvallisuus on läsnä kaikkialla ja kaikkien elämässä. Kyberturvallisuusosaaminen on noussut yhä keskeisemmäksi aiheeksi nykypäivän digitalisoituneessa maailmassa. Aihe koskettaa jokaista niin organisaatio- kuin yksilötasolla. Kyberhyökkäykset ovat muuttuneet aiempaa vakavimmiksi ja kohdennetuimmiksi. Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen Tietoturvan vuosi 2023-katsaus paljastaa Suomen kyberturvallisuuden uhkatason pysyneen kohonneena ja arvioi tilanteen jatkuvan myös tulevaisuudessa. (Tietoturvan vuosi 2023 2024.) Kyberturvallisuus ei kosketa pelkästään tiettyjä yhteiskunnan osa-alueita vaan se linkittyy ihan kaikkialle. Siksi onkin tärkeää, että kyberturvallisuuteen panostetaan yhteiskunnan kaikilla sektoreilla, myös sosiaali- ja terveysalalla. Nyt jos koskaan on aihetta kohdentaa toimia kyberturvallisuuden parantamiseksi.

Sosiaali- ja terveysalan lisääntyvä teknologinen kehitys vaatii yhä tarkempaa huomiota kyberturvallisuuteen. Terveydenhuollon tietomurtojen määrä on kasvanut ja ala on yksi eniten verkkohyökkäysten kohteena olevista aloista maailmanlaajuisesti. Sosiaali- ja terveysalan tietoihin pääsy kiinnostaa rikollisia erityisesti, sillä niiden sisältämä tieto on muuttumatonta ja rikollisten käsiin vuotaneita tietoja ei voida palauttaa. Kyberhyökkäykset voivat aiheuttaa paitsi potilaiden identiteetin ja talouden vaarantumisen, myös haitata sairaalan toimintaa ja potilaiden terveyttä. Organisaatiotasolla ne saattavat aiheuttaa niin toiminnallisia viivästyksiä ja taloudellisia menetyksiä kuin vaikkapa mainehaittaa. (Cartwright 2023; Argaw, Troncoso-Pastoriza, Lacey, Florin, Calcavecchia, Anderson, Burleson, Vogel, O'Leary, Eshaya-Chauvin & Flahault 2020; Coventry & Branley 2018.) Sosiaali- ja terveysalan lisääntyneet kyberriskit eivät kuitenkaan korreloidu organisaatioiden panostukseen kyberturvaa kohtaan. Cartwright (2023) toteaa, että riittämätön investoiminen kyberturvallisuuteen lisää entisestään kyberhyökkäysten mahdollisuutta. Kyberturvallisuuden investoinnin ja panostuksen puutteellisuudella viitataan vanhentuneeseen teknologiaan (esim. laitteet ja järjestelmät), ammattitaitoisten tietotekniikka- ja kyberturvallisuushenkilöstön vähyyteen ja henkilöstön riittämättömään koulutukseen. (Cartwright 2023.)

Ammattitaitoisten kyberturvallisuusosaajien tarve yleisesti on valtava ja tulevaisuudessa osaavien ammattilaisten määrä ei tule riittämään yhteiskunnan tarpeisiin (Lehto 2023; Kyberturvallisuuden kehittämisohjelma 2021). Kyberturvallisuuskoulutusta pidetään ensisijaisen tärkeänä väylänä saada lisää eri tasoisia osaajia (AlDaajeh, Saleous, Alrabaee, Barka, Breitinger & Choo 2022). Kyberturvallisuuden hallinnassa suurin riskitekijä on ihminen ja hänen toimintansa (mm. Cartwright

2023; Blek & Solankallio-Vahteri 2022; Jalali, Bruckers, Westmattelmann & Schewe 2020; Kruse ym. 2017). Tarkoituksenmukainen ja ajantasainen koulutus on keskeistä, jotta inhimillisen tekijän aiheuttama riski saadaan minimoitua (Argaw ym. 2020). Organisaation turvallisuuden lisäämiseksi tulisi kouluttaa kaikki työntekijät työtehtävistä riippumatta. Koulutuksen tulisi olla säännöllistä ja kohdennettua, jotta se olisi helposti integroitavissa omaan työhön. (Cartwright 2023.) Lokakuussa 2024 Suomessa alettiin soveltaa käytäntöön EU:n NIS2-direktiiviä (Network and Information Security Directive 2), jonka tavoitteena on vahvistaa kriittisten toimialojen, kuten sosiaali- ja terveysalan, kyberturvallisuutta EU:ssa sekä kansallisesti jäsenvaltioissa. Myös siinä korostetaan koulutuksen merkitystä ja velvoitetaan organisaatioita investoimaan osaamisen lisäämiseksi. (NIS2 - Euroopan unionin kyberturvallisuusdirektiivi 2024; Direktiivi 2022/2555/EU.)

Kyberturvallisuus on olennainen osa myös jokaisen sosiaali- ja terveysalan ammattilaisen työtä. Teknisten ratkaisujen ja huolellisesti suunniteltujen prosessien tehokas toiminta edellyttää ammattitaitoista henkilöstöä, joka on keskeinen tekijä kyberturvallisuuden varmistamisessa. Tämän pitäisi läpileikata koko organisaation kaikkia työtehtäviä, koska henkilöstön osaamattomuus tai tietämättömyys kyberturvallisuudesta voi johtaa kybertoimintaympäristön haavoittuvuuteen. (Lehto 2023.) Sosiaali- ja terveysalan henkilöstön tulee olla tietoisia kyberturvallisesta toiminnasta ja ymmärtää, että heidän käyttäytymisensä voi vaikuttaa negatiivisesti huolimatta organisaation asianmukaisista kyberturvallisuusjärjestelmistä. Kyberturvallisen toimintakulttuurin tulisi edistää riittävää kyberturvallisuustietoisuutta sekä kykyä tunnistaa mahdollisia uhkia. (Cartwright 2023.)

Sosiaali- ja terveysalan ammattilaisen työssä kyberturvallisuus ei tarkoita monimutkaista teknologista osaamista. Sen sijaan keskeistä ovat ne toistuvat päivittäisessä työssä tehtävät päätökset, jotka osaltaan vaikuttavat kyberturvallisuutta lisäävästi tai vähentävästi. Sosiaali- ja terveysalan ammattilaiset toimivat laajasti siinä rajapinnassa, jossa tehdään näitä valintoja, onko toiminta kyberturvallista vai ei. Huomioitavaa on, että ihmisen toiminta riskin lisääjänä voi olla tahallista tai tahatonta (Argaw ym. 2020). Äärimmäisen tärkeää on, että jokainen tiedostaisi kyberturvallisuusosaamisen merkittävyyden niin yhteiskunnassa, organisaatiotasolla kuin omassa toiminnassa.

Tässä opinnäytetyössä selvitettiin Jyväskylän ammattikorkeakoulun (JAMK) järjestämän sosiaali- ja terveysalan ammattilaisille suunnatun kyberturvallisuutta käsittelevän täydennyskoulutuksen osallistujien arvioita siitä, mitkä seikat lisäävät kyberturvallisuutta sosiaali- ja terveysalan kontekstissa.

Lisäksi selvitettiin, miten täydennyskoulutus on vaikuttanut osallistujien kyberturvallisuusosaamiseen. Opinnäytetyön lopputuloksena saatiin selvitys siitä, mitkä tekijät lisäävät kyberturvallisuutta sekä miten täydennyskoulutus vaikuttaa kyberturvallisuusosaamiseen ammattilaisten itsensä arvioimina. Tavoitteena oli vahvistaa olemassa olevaa tietoa ja tuoda uutta näkökulmaa aiheeseen. Aiheen tarkastelu on tärkeää siksi, että sen tuloksia voidaan hyödyntää tulevaisuudessa niin sosiaali- ja terveysalan organisaation kyberturvallisuuden edistämisen näkökulmasta kuin kyberturvallisuusosaamisen kehittämisen kannalta.

2 Katsaus kyberturvallisuuden käsitteisiin

Kyberturvallisuuteen liittyviä käsitteitä ja ilmiöitä voidaan selventää monella tapaa; toisaalta hyvin laajasti ja toisaalta hyvinkin spesifisti. Joitain käsitteitä saatetaan käyttää toistensa synonyymeina ja toisaalla niillä viitataan erilaisiin sisältöihin. Käsitteiden määritelmät muuttuvat ja niitä on syytä tarkastella myös suhteessa kansainväliseen toimintaympäristöön (Suomen kyberturvallisuusstrategia 2024–2035 2024). Seuraavissa alaluvuissa määritellään ja täsmennetään kyberturvallisuuteen liittyviä käsitteitä tämän opinnäytetyön näkökulmasta. Tarkoituksena on saada yhtenäinen lähtökohta aiheeseen tässä opinnäytetyössä.

2.1 Kyberturvallisuus

Kyberturvallisuus terminä on Suomessa suhteellisen uusi. Se alkoi yleistyä Suomessa 2010-luvun alussa. Ensimmäinen kyberturvallisuusstrategia valmistui tammikuussa 2013, mikä keskittyi perusperiaatteisiin, kuten yhteiskunnan elintärkeiden toimintojen turvaamiseen ja kansallisen valmiuden lisäämiseen kyberuhkia vastaan (Suomen kyberturvallisuusstrategia 2013). Tähän strategiaan nojautuu myös Suomen kyberturvallisuusstrategia 2019, jonka pohjalta käynnistettiin kansallinen kyberturvallisuuden kehittämisohjelma. Kehittämisohjelman tavoitteet liittyivät kansallisen tilannekuvan parantamiseen ja koordinaation tehostamiseen sekä kansainvälisen yhteistyön syventämiseen. Kyberuhkien ulottuessa yli valtion rajojen, kansainvälinen yhteistyö on ensisijaista. Kyberturvallisuus tunnistettiin osaksi yhteiskunnan turvallisuusstrategiaa. Huomioitavaa on myös se, että kyberturvallisuus ja kybertoimintaympäristö ovat merkittävät teemat Suomen ulko- ja turvallisuuspolitiikassa. (Kyberturvallisuuden kehittämisohjelma 2021; Suomen kyberturvallisuusstrategia 2019.)

Uusin kyberturvallisuusstrategia julkaistiin lokakuussa 2024. Ensimmäiseen kyberturvallisuusstrategiaan verrattuna se laajentaa näkökulmaa painottamalla kyberresilienssiä ja kokonaisvaltaista lähestymistapaa, joka kattaa niin kansallisen kuin kansainvälisen yhteistyön. Lisäksi siinä on huomioitu nykyaikaiset, kehittyneet kyberuhkat, mukaan lukien valtiolliset toimijat ja poliittisen paineen välineenä käytettävät kyberhyökkäykset. Strategia keskittyy neljään pääalueeseen: kyberosaamisen ja tutkimuksen kehittäminen, yhteiskunnan kyberresilienssin parantaminen, kansallisen ja kansainvälisen yhteistyön vahvistaminen sekä oikea-aikainen reagointi ja vastatoimet. Näillä pyritään varmistamaan kyberturvallisuuden kokonaisvaltainen parantaminen ja kriittisten toimien suojaaminen Suomessa. (Suomen kyberturvallisuusstrategia 2024–2035 2024.)

Kyberturvallisuus on käsitteenä monivivahteinen ja sitä on haastavaa määritellä yksiselitteisesti. Se on saanut vaikutteita ulkomaisista digi-, kyber- ja tietoturvallisuus käsitteiden käännöksistä; varsinkin eri maiden käyttäessä englannin kieltä yleiskielenä. Sana kyber voi siis tarkoittaa eri asiaa eri maissa tai eri yhteyksissä. Ajoittain kyberturvallisuus voi tarkoittaa jotain hyvin spesifistä kokonaisuutta ja toisinaan taas laajaa digiturvallisuuden käsitettä. (VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään 2022.)

Sanan kyber alkuperä liittyy kreikan kielen sanaan kybereo, joka tarkoittaa ohjaamista, opastamista tai hallitsemista (Tepa-termipankki n.d). Sana saattaa kuulostaa tekniseltä tai jopa dramaattiselta, vaikka se nykyään tarkoittaa hyvin arkipäiväistä erilaisten järjestelmien suojaamista tai turvaamista (Järvinen 2018). Kyberturvallisuuden käsite pitää sisällään digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuuden sekä niiden toimintoihin kohdistuvat vaikutukset. Kyberturvallisuus on sitä, että kybertoimintaympäristöön kohdistuvat uhkat ovat hallinnassa ja kaikki toimii oikein ja virheettömästi. Kyberturvallisuuteen liittyy erilaisia toimenpiteitä, joiden avulla pyritään ennakoivasti hallitsemaan ja tarvittaessa sietämään erilaisia kyberuhkia ja niiden vaikutuksia. (Kyberturvallisuuden sanasto 2018.)

Kyberturvallisuus on tullut yhä tärkeämmäksi osaksi myös sosiaali- ja terveysalan toimintaa. Digitalisaation ja teknologian nopea kehitys on muuttanut alan prosesseja, jolloin potilastietojen suojaaminen, järjestelmien toimintavarmuuden turvaaminen ja erilaisten kyberuhkien ennaltaehkäisy ovat nousseet keskeisiksi turvallisuuskysymyksiksi. (Kruse, Frederick, Jacobson & Monticone 2017.)

Terveydenhuollossa käsitellään suuria määriä luottamuksellista tietoa ja jatkuvasti verkottuneemmat järjestelmät ovat alttiita erilaisille kyberuhkille. Tämä tekee kyberturvallisuudesta kriittisen osan alan toimivuutta ja potilasturvallisuutta. Kyberturvallisuus toimii tärkeänä linkkinä teknologian, tietosuojan ja terveydenhuollon laadunhallinnan välillä. (McLeod & Dolezel 2018.)

Yksinkertaistettuna kyberturvallisuus tarkoittaa verkottuneiden järjestelmien häiriöihin ja niiden vaikutuksiin varautumista, niiden tunnistamista, torjumista ja kestämistä (Kyberturvallisuuden sanasto 2018). Kyberturvallisuus on kokonaisvaltainen käsite, joka yhdistää tekniset, organisatoriset ja inhimilliset elementit suojatakseen verkottuneita järjestelmiä. Se edellyttää jatkuvaa kehitystä ja yhteistyötä eri toimijoiden kesken, jotta pystytään ennakoimaan ja reagoimaan uusiin uhkiin tehokkaasti. (Suomen kyberturvallisuusstrategia 2024–2035 2024.)

Puhuttaessa kyberturvallisuudesta on lisäksi selventävää tuoda esiin termi tietoturvallisuus. Näitä saatetaan käyttää jossain yhteyksissä synonyymeina, koska molempien perimmäisenä tavoitteena on informaation suojaaminen sekä tietojärjestelmien toiminnan varmistaminen. Termien välinen ero voidaan ajatella olevan laajuudessa. Tietoturva keskittyy varmistamaan tietojen, tiedostojen ja yksittäisten laitteiden turvallisuuden. Kyberturvallisuus puolestaan ulottuu koskemaan koko yhteiskuntaa, sen peruspalveluita (esim. kriittinen infrastruktuuri) tai vaikkapa valtion sotilaallista puolustusta. Kyberturvallisuus sisältää kuitenkin myös tietoturvan. Tietoturvallinen toiminta verkossa on avainasemassa, kun halutaan ehkäistä mahdollisia uhkia ja ylläpitää tietoturvaa kokonaisvaltaisesti niin yksilön, organisaation kuin koko valtion näkökulmasta. (Järvinen 2018.) Tietoturvallisuus keskittyy tietojen suojaamiseen niiden luottamuksellisuuden, eheyden ja käytettävyyden varmistamiseksi. Se kattaa tiedon, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaamisen. Kyberturvallisuus on taas laajempi käsite, joka sisältää tietoturvallisuuden lisäksi kybertoimintaympäristön suojaamisen haitallisilta ilmiöiltä. (Lönnqvist & Moilanen 2017.) Tietosuojalla taas tarkoitetaan erilaisia toimia ja sääntöjä, joilla pyritään suojaamaan ihmisen yksityisyyttä väärinkäytöksiä ja vahinkoja vastaan. Se kattaa henkilötietojen (tiedot, joiden avulla yksilö voidaan tunnistaa) käsittelyn lainmukaisesti ja turvallisesti. Tietosuojaa pyritään toteuttamaan tietoturvan avulla. (Tepa-termipankki n.d; Suomen kyberturvallisuusstrategia 2013.) Yksinkertaistettuna kyberturvallisuus kattaa tietoturvan ja tietoturvaan sisältyy tietosuojan varmistaminen (Järvinen 2018; Lönnqvist & Moilanen 2017; Tepa-termipankki n.d; Suomen kyberturvallisuusstrategia 2013.).

2.2 Kyberresilienssi

Yleisesti resilienssillä viitataan valmiuteen kohdata häiriöitä ja kriisejä sekä palautua niistä. (Kyberturvallisuuden sanasto 2018.) Kyberresilienssillä tarkoitetaan kyberuhkien sietokykyä (Tepa-termipankki n.d). Se merkitsee siis kykyä pysyä toimintakykyisenä muuttuvissa kybertoimintaympäristöissä uhkia tai häiriöitä kohdatessa ja ennen kaikkea kykyä palautua niistä ja reagoida niihin (Suomen kyberturvallisuusstrategia 2024–2035 2024).

2.3 Kybertoimintaympäristö

Kybertoimintaympäristö muodostuu yhdestä tai useammasta digitaalisesta tietojärjestelmästä, datan tai informaation käsittelyyn liittyvistä rakenteista sekä eri toimijoista (Suomen kyberturvallisuusstrategia 2024–2035 2024; Kyberturvallisuuden sanasto 2018; Tepa-termipankki n.d). Kybertoimintaympäristö kattaa myös yhteiskunnan kriittiset toiminnot, kuten infrastruktuurin, tietovarannot, julkiset palvelut ja huoltovarmuuden. Näiden toimintojen häiriönsietokyky ja toimivuus on turvattava, jotta yhteiskunta voi säilyttää toimintakykynsä ja vastata tehokkaasti kybertoimintaympäristön uhkiin ja häiriöihin. Kybertoimintaympäristössä esiintyy siis haitallisia ilmiöitä, mutta sen painopisteenä on sen hyödyntäminen tavoitteellisen toiminnan edistämiseksi. (Suomen kyberturvallisuusstrategia 2024–2035 2024.)

Kybertoimintaympäristöstä puhuttaessa on myös hyvä tuoda esiin termi digitaalinen toimintaympäristö. Termejä saatetaan käyttää synonyymeina, mutta on tärkeää määritellä ne sen mukaan, missä yhteydessä niitä käytetään. Molemmat termit liittyvät digitaalisuuteen ja verkkojen käyttöön, mutta ne eroavat hieman painotukseltaan ja laajuudeltaan. Digitaalinen toimintaympäristö kattaa laajemmin kaiken digitaalisten järjestelmien ja teknologioiden hyödyntämisen, kun taas kybertoimintaympäristö korostaa turvallisuutta ja uhkien hallintaa. (VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään 2022.)

Digitaalisella toimintaympäristöllä tarkoitetaan kaikkia digitaalisia järjestelmiä, verkkoja, laitteita ja alustoja, joissa käsitellään tietoa jollain tavoin. Tietoa voidaan tallentaa, välittää ja jakaa eri tarkoituksiin. Digitaalinen toimintaympäristö kattaa niin teknologian kuin ihmisen toiminnan. Käytän-

nössä digitaalinen toimintaympäristö muodostuu siis erilaisista järjestelmistä ja niiden keskinäisistä yhteyksistä. (VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään 2022.)

Kybertoimintaympäristö on osa digitaalista toimintaympäristöä ja se keskittyy tietoverkkojen ja -järjestelmien suojaamiseen, tietoturvaan ja kyberuhkien hallintaan. Kybertoimintaympäristössä keskitytään tarkastelemaan digitaalista ympäristöä turvallisuuden näkökulmasta, erityisesti siihen liittyviä riskejä, haavoittuvuuksia ja uhkia. Tähän liittyy merkittävänä osatekijänä myös se, että toimijat voivat toimia niin laillisesti kuin laittomastikin, kukin oman intressinsä mukaan. (VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään 2022.)

2.4 Kyberuhka

Kyberuhka on mahdollisesti toteutuva tapahtuma, tilanne tai toiminta, joka voi aiheuttaa haittaa tai häiriötä viestintäverkoille, tietojärjestelmille, niiden käyttäjille tai muille tahoille (Suomen kyberturvallisuusstrategia 2024–2035 2024). Kyberuhkien kirjo on laaja ja monimuotoinen. Niitä ovat muun muassa kybervandalismi, kyberrikollisuus, kybervakoilu, kyberterrorismi ja kybersodankäynti. Uhkat voivat esiintyä yksinään tai yhdessä, ja niiden luonne voi muuttua ajan myötä. (Norri-Sederholm, Laitinen, Lehto & Kari 2019.) Uhka vaikuttaa kybertoimintaympäristöön ja sitä kautta aiheuttaisi vahinkoa siihen kuuluville toiminnoille. Uhka voi kohdistua niin yhteiskunnallisiin toimintoihin (mm. kriittinen infrastruktuuri) kuin kansalaisia vastaan (verkottunut yhteiskunta). Toteutuessaan kyberuhka etenee kyberhäiriötilanteeksi, jolloin organisaation tai järjestelmän toiminta on häiriintynyt kybertoimintaympäristössä. (Kyberturvallisuuden sanasto 2018.)

3 Kyberturvallisuus sosiaali- ja terveysalalla

3.1 Kyberturvallisuuden nykytila

Kyberturvallisuus Euroopassa ja Suomessa on muuttunut viime vuosina digitalisaation sekä merkittävien kansainvälisten kriisien (esim. COVID-19 pandemia, Venäjän hyökkäyssota) sekä muiden suurten muutosten (esim. Suomen Nato-jäsenyys) takia. Suomen kyberturvallisuus on kuitenkin kansainvälisesti arvioiden hyvällä tasolla. Tekninen osaaminen, kyberturvallisuuden ymmärrys ja

toimiva yhteistyö julkisen ja yksityisen sektorin välillä ovat Suomen vahvuuksia. Suomessa on koettu tietomurtoja, jotka ovat vaikuttaneet ihmisten arkeen, mutta yhteiskunta on toistaiseksi välttynyt pitkäaikaisesti vaikuttavilta kyberhyökkäyksiltä. Vihamielinen valtiollinen toiminta, kyberrikollisuus, palvelunestohyökkäykset ja haittaohjelmat ovat kuitenkin yleistyneet ja tekoäly mahdollistaa uusia uhkia kybertoimintaympäristöissä. Kyberhäiriöiden seuraukset, kuten pysyvä tietojen menetys ja luottamuksen heikkeneminen, korostavat riittävien resurssien, yhteistyön ja yhteisten toimintatapojen merkitystä. (Suomen kyberturvallisuusstrategia 2024–2035 2024.)

Euroopan unionin NIS2-direktiivin valmistelu Suomen kansalliseksi lainsäädännöksi, kyberturvallisuuslaiksi, on vielä kesken, mutta toteutunee myöhemmin. NIS2:n tarkoituksena on yhtenäistää ja vahvistaa kyberturvallisuuden tasoa kriittisillä aloilla EU:ssa sekä kansallisesti jäsenvaltioissa. Se velvoittaa, sanktioiden uhalla, määriteltyjen kriittisten toimialojen toteuttamaan riskienhallintaan perustuvia kyberturvallisuustoimenpiteitä. Sosiaali- ja terveysalan ollessa lisääntyvien kyberuhkien kohteena, myös heidän tulee panostaa huomattavan paljon tulevan lain velvoitteiden toteutumiseksi. NIS2:n sosiaali- ja terveysalaa velvoittavat toimenpiteet sisältävät muun muassa kyberturvallisuusriskeihin varautumisen ja niiden hallinnan, merkittävien tietoturvapoikkeamien nopean raportoinnin viranomaisille sekä henkilöstön kyberturvallisuuskoulutuksen järjestämisen turvallisuuden takaamiseksi kaikilla toiminnan tasoilla. NIS2 nostaa sosiaali- ja terveysalan kyberturvallisuusvaatimukset uudelle tasolle, mikä voi parantaa sekä potilaiden tietoturvaa että organisaatioiden kykyä vastata kyberuhkiin. Samalla se edellyttää investointeja teknologiaan, osaamiseen ja prosesseihin, mikä voi aiheuttaa taloudellisia ja organisatorisia haasteita. (NIS2 - Euroopan unionin kyberturvallisuusdirektiivi 2024; Direktiivi 2022/2555/EU.)

Sosiaali- ja terveysalan kyberturvallisuus on suhteellisen uutta ja sen tärkeyteen on herätty vasta lähivuosien aikana. Aiemmin ei ole ymmärretty, miksi joku taho haluaisi hyökätä terveydenhuoltojärjestelmiin eikä kyberturvallisuuteen liittyviä varotoimia ole pidetty tarpeellisina (Coventry & Branley 2018). Kiihtyvällä tahdilla lisääntynyt teknologinen kehitys on tuonut uusia haasteita sosiaali- ja terveysalan kyberturvallisuustarpeisiin (Argaw ym. 2020). Viime vuosina sosiaali- ja terveysala on myös tunnistettu olevan verkkorikollisten näkökulmasta haluttu kohde (mm. Al-Qarni 2023; Argaw ym. 2020; Coventry & Branley 2018).

Vuoden 2023 alussa toteutunut hyvinvointialueuudistus toi merkittäviä muutoksia kriittiseen infrastruktuuriin ja julkisiin palveluihin. Hyvinvointialueet vastaavat myös palveluidensa kyberturvallisuudesta. Tämän lisäksi on huomioitavaa, että kuntien kyberturvallisuuden taso on usein heikompi verrattuna valtion- ja aluehallintoon. Sekä hyvinvointialueet että kunnat tarvitsevat siis lisää tukea varmistaakseen toimintansa ja kyberturvallisuutensa. (Suomen kyberturvallisuusstrategia 2024–2035 2024.) Organisaatiotasolla joudutaan myös puntaroimaan sitä, missä laajuudessa erilaisista varautumisstrategioista kyberuhkia vastaan kerrotaan avoimesti ja mitkä seikat ovat salassa pidettäviä. Rajallisen tiedon takia kyberturvallisuusnäkökulma ei välttämättä ole mukana työntekijöiden tavallisessa arjessa, mikä voi johtaa siihen, että työntekijän toiminta realisoituu keskeiseksi kyberuhkaa lisääväksi tekijäksi. (Norri-Sederholm ym. 2019.)

Sosiaali- ja terveysalan ammattilaisten kyberturvallisuusosaaminen on tärkeä osa ammattitaitoa. Se ei kuitenkaan ole välttämättä itsestäänselvyys kaikille, jolloin työntekijän toiminta saattaa heikentää merkittävästi kyberturvallisuutta. (Norri-Sederholm ym. 2019.) Kyberturvallisuuden edistämiseksi on pyritty muuttamaan ajattelutapaa ennaltaehkäisevämpään ja ennakoivampaan suuntaan. Täydellinen ja virheetön kyberturvallisuus ei ole mahdollista, joten sitä lähestytään riskienhallinnan ja kyberresilienssin näkökulmasta. Tässä lähestymistavassa pyritään tunnistamaan, lieventämään, välttämään ja hyväksymään riskejä. (Argaw ym. 2020.)

3.2 Kyberturvallisuuden uhkatekijöitä sosiaali- ja terveysalalla

Sosiaali- ja terveysalan lisääntyvä teknologinen kehitys vaatii tarkempaa huomiota kyberturvallisuuteen, sillä terveydenhuollon tietomurtojen määrä on kasvanut ja ala on yksi eniten verkkohyökkäysten kohteena olevista aloista maailmanlaajuisesti (mm. Al-Qarni 2023; Argaw ym. 2020; Coventry & Branley 2018; Kruse ym. 2017). Sosiaali- ja terveydenhuollon tietoihin pääsy kiinnostaa rikollisia erityisesti, sillä niiden sisältämä tieto on muuttumatonta ja rikollisten käsiin vuotaneita tietoja ei voida palauttaa. Tällöin yksityisyyden suoja vaarantuu pysyvästi. Tiedot sisältävät henkilökohtaista dataa, kuten nimi, syntymäaika, terveydenhuollon tarjoajan tiedot sekä terveys- ja geneettiset tiedot. (Argaw ym. 2020; Coventry & Branley 2018.) Varastettuja tietoja voidaan käyttää moniin rikollisiin tarkoituksiin, mutta hyökkäysten taustalla on usein taloudellinen hyöty (Coventry & Branley 2018). Varastetun terveystiedon hinta pimeässä verkossa (dark web) voi olla jopa 1000 dollaria (n. 950 €), kun taas esimerkiksi varastetun luottokortin tietojen hinta on vain noin 5 dollaria (Jerry-Egemba 2023). Terveystietojen kohdalla puhutaan siten miljardeista petollisin keinoin

saaduista rahoista (Coventry & Branley 2018). Verkkohyökkäykset voivat aiheuttaa paitsi potilaiden identiteetin ja talouden vaarantumisen, myös haitata sairaalan toimintaa ja potilaiden terveyttä. Organisaatiotasolla hyökkäykset voivat aiheuttaa toiminnallisia viivästyksiä, taloudellisia menetyksiä ja mainehaittaa (Argaw ym. 2020; Coventry & Branley 2018.)

Sosiaali- ja terveysalan organisaatioihin kohdistuvat kyberuhkat liittyvät yleisimmin tietotekniikan infrastruktuurin haavoittuvuuksiin, kuten virheellisten palomuurien tai ohjelmistovirheiden hyödyntämiseen. Tämän lisäksi uhkia voivat aiheuttaa kiristyshaittaohjelmat, joiden tarkoitus on aiheuttaa palvelunestoa, sekä ihmisten toiminnasta johtuvat haavoittuvuudet, joita rikolliset hyödyntävät päästäkseen infrastruktuuriin. (Nifakos, Chandramouli, Nikolaou, Papachristou, Koch, Panaousis & Bonacina 2021; Coventry & Branley 2018.) Terveydenhuollon järjestelmiin kohdistuvista uhkista yleisimpiä ovat tietoturvaloukkaukset (data breach), tietojenkalastelu (phishing, vhishing, spoofing), kiristyshaittaohjelmat (ransomware) ja palvelunestohyökkäykset (denial of service, DoS). Tietoturvaloukkaukset liittyvät usein käyttäjätunnusten ja salasanojen väärinkäyttöön, tietomurtoihin ja tietojen varastamiseen. Tietojenkalastelun tavoitteena on huijata henkilöitä tai organisaatioita paljastamaan luottamuksellisia tietoja tai lataamaan haittaohjelmia. Kiristyshaittaohjelmat puolestaan salaavat tai manipuloivat laitteen tiedot ja vaativat lunnaita niiden palauttamiseksi. Palvelunestohyökkäyksessä tietoverkkoa kuormitetaan ja häiritään niin, ettei palvelu tai järjestelmä toimi normaalisti. (Blek & Solankallio-Vahteri 2022.)

Kyberturvallisuuden hallinnassa suurin riskitekijä on kuitenkin ihminen itse ja hänen toimintansa (mm. Cartwright 2023; Blek & Solankallio-Vahteri 2022; Jalali ym. 2020; Kruse ym. 2017). Ihmisen toiminta riskin lisääjänä voi olla tahallista tai tahatonta. Erityisesti tietämättömyyttä tai ajattelemattomuutta tapahtuneet tahattomat kyberturvallisuutta vähentävät toimet tulisi saada kitkettyä pois laadukkaan koulutuksen avulla. Tahaton toiminta voi liittyä tietoturvaan, tietojen tallentamiseen, ulkoisiin laitteisiin tai vaikkapa tunnistamattoman sähköpostiliitteen avaamiseen. (Argaw ym. 2020.)

Sosiaali- ja terveysalan kyberhyökkäykset ovat lisääntyneet ja ne ovat vaikutuksiltaan laajempia. Kyberuhkia ovat lisänneet muun muassa digitaalisten terveystietojen määrän kasvu ja terveydenhuollon IoMT-laitteiden (Internet of Medical Things, internetiin yhdistettävä laite datan siirtä-

miseksi) lisääntynyt käyttöönotto. IoMT-laitteet voivat muodostaa suojaamattoman ja houkuttelevan kohteen kyberrikollisille, jos yleisesti sovittuja turvallisuusstandardeja ei ole käytössä. Nopeaa reagointia ja lisää sääntelyä tarvitaan, jotta IoMT-laitteiden turvallisuus paranisi. (Cartwright 2023.)

Sosiaali- ja terveysalalla on siis monenlaisia turvallisuuteen liittyviä haasteita. Ne liittyvät järjestelmien haavoittuvuuksiin, ali-investointiin ja hoidossa käytettäviin päivittämättömiin tai vanhentuneisiin laitteisiin. Näiden lisäksi turvallisuuspuutteet voivat johtua myös riittämättömästä koulutuksesta ja henkilöstön kyberturvallisuustietoisuuden puutteista. Lisäksi potilastietoja käsitellään useissa järjestelmissä ja sovelluksissa, joiden keskinäisen käytettävyyden haasteet lisäävät kyberturvallisuusriskiä. (Cartwright 2023; Argaw ym. 2020; Coventry & Branley 2018.) Teknologioiden kehittyessä on todennäköistä, että myös uhkatekijät muuttuvat entistä kehittyneemmiksi. (Norri-Sederholm ym. 2019.)

3.3 Osaamisen kehittäminen

Tieto- ja viestintätekniikan kasvava rooli yhteiskunnassa, erityisesti COVID-19 pandemian aikana, on lisännyt tarvetta kehittää kyberturvallisuusosaamista ja koulutusta. Kyberhyökkäysten määrä on kasvanut koko ajan ja odotetaan edelleen kasvavan. COVID-19 pandemian aikana lisääntyneet kyberhyökkäykset korostivat kiireellistä tarvetta lisätä kyberturvallisuuden ammattilaisia ja tehokkaita kyberturvallisuutta lisääviä toimia. (AlDaajeh ym. 2022.)

Yksi tärkeimmistä asioista puhuttaessa kyberturvallisuudesta on ammattitaitoinen henkilöstö. Toteutuakseen se vaatii henkilöstön asianmukaisen koulutuksen, joka on kirjallisuuden mukaan tehokkain tapa lisätä kyberturvallisuutta. (Kruse ym. 2017.) Tekniset ratkaisut ja huolellisesti suunnitellut prosessit vaativat toimiakseen ammattitaitoisen henkilöstön. Tämän pitäisi läpileikata koko organisaation kaikkia työtehtäviä, koska henkilöstön osaamattomuus tai tietämättömyys kyberturvallisuudesta voi johtaa kybertoimintaympäristön haavoittuvuuteen. (Lehto 2023.)

Ammattitaitoisten kyberturvallisuusosaajien tarve on valtava ja tulevaisuudessa osaavien ammattilaisten määrä ei tule riittämään yhteiskunnan tarpeisiin (Lehto 2023; Kyberturvallisuuden kehittämisohjelma 2021). Kyberturvallisuuskoulutusta pidetään ensisijaisen tärkeänä väylänä saada lisää

osaajia (AlDaajeh ym. 2022). Suomessa kyberturvallisuutta voidaan opiskella ammattikorkeakoulutasolla (AMK ja YAMK) sekä kyberturvallisuuteen tähtäävissä koulutusohjelmissa että kyberturvallisuuden erikoistumisopintoja sisältävissä koulutusohjelmissa. Yliopistoissa kyberturvallisuutta opetetaan suhteellisen vähän osaajapulaan nähden. Useimmiten kyberturvallisuus on integroitu osaksi koulutusohjelmien tutkintorakennetta, eikä yliopistot tarjoa tutkintoon tähtääviä kyberturvallisuuden koulutusohjelmia muutamia poikkeuksia lukuun ottamatta juuri ollenkaan. (Lehto 2023.)

Kyberturvallisuusosaamisen merkitys osana Suomen kokonaisturvallisuutta on ollut perusteena opetus- ja kulttuuriministeriöllä myöntäessään rahoitusta kyberturvallisuusalan koulutuksen kehittämiseen ja tarjonnan lisäämiseen. Tästä on muodostunut laaja korkeakoulujen verkosto, joka koordinoi koulutustarjontaa ja koulutuksen kehittämistä. Tämä on yksi uusimmista edistysaskeleista kohti laadukkaampaan korkeakoulutasoista kyberturvallisuusosaamiskoulutusta. (Kyberturvallisuusalan koulutusta kehitetään korkeakoulujen yhteistyönä – myös informaatiopsykologista tutkimusta vahvistetaan 2022.)

Kyberturvallisuus alana on erittäin laaja. Siihen liittyy myös erilaisia erikoistumisosaamisen alueita, joihin vaaditaan spesifimpää tietojen, taitojen ja kykyjen osaamista. Yleistasoisella koulutuksella pystytään kuitenkin saamaan tietty perusosaamistaso, jonka pohjalta voidaan sitten syventää osaamista kohti asiantuntijuutta muun muassa erilaisten täydennys- ja erikoistumiskoulutusten kautta. (Lehto 2023.) Erilaisten kyberturvallisuuden perusosaamisen kehittämiseen liittyvien koulutusten lisäksi myös organisaatioiden tulee panostaa työntekijöidensä kouluttamiseen. Koulutussisältö tulisi räätälöidä eri ammattilaisten työnkuvan mukaisesti ja jatkuvan oppimisen ja osaamisen kehittämisen periaatteita noudattaen. Aihetta tulisi lähestyä kokonaisvaltaisesti kyberturvallisuuden eri osa-alueet huomioiden. (Jerry-Egemba 2023.)

Ihmisen ollessa suurin kyberturvallisuusriski (mm. Cartwright 2023; Blek & Solankallio-Vahteri 2022; Jalali ym. 2020; Kruse ym. 2017), se korostaa sosiaali- ja terveysalan ammattilaisen tietoisuuden ja osaamisen kehittämisen tärkeyttä. Jokaisen tulee osata toimia niin, ettei arkaluontoiset tiedot ja turvallisuus vaarannu. Tulisi myös alleviivata, että kyberturvallisuus ulottuu laajalle, koko toimintaympäristöön, ei pelkästään teknologiaan. Koulutusohjelmien kehittäminen on tärkeää, jotta voidaan tehokkaasti vastata uusiin uhkiin ja riskeihin, omaksua ajantasaiset toimintatavat ja varmistaa parhaiden käytäntöjen hyödyntäminen. Jatkuva koulutus ja osaamisen vahvistaminen

ovat keskeisiä tavoitteita sosiaali- ja terveysalan ammattilaisten valmiuksien ylläpitämisessä ja kehittämisessä jatkuvasti muuttuvassa kybertoimintaympäristössä. (Jerry-Egemba 2023.)

3.4 Kyberturvallisuuden tulevaisuudennäkymät

Sosiaali- ja terveydenhuollon organisaatioihin kohdistuvat kyberhyökkäykset ovat ajankohtainen ja jatkuva huolenaihe. Organisaatioiden kyberresilienssiä tulisi tarkastella kokonaisvaltaisesti, huomioiden tietoisuuden ja osaamisen lisääminen, hankintojen kyberturvallisuus, asianmukaiset työvälineet sekä kyberturvallisten toimintatapojen johdonmukainen noudattaminen. Kyberturvallisuudessa on tärkeää löytää tasapaino tietoturvan, yksityisyyden suojan ja käytettävyyden välillä. Kaikkien osapuolten on tehtävä yhteistyötä potilaiden terveyden ja tietojen suojaamiseksi. (Al-Qarni 2023; Argaw ym. 2020.) Organisaatioiden tulisi myös kohdentaa resursseja ennemmin ennakointiin kuin reaktiiviseen toimintaan (Argaw ym. 2020).

Kyberturvallisuus tulisi nähdä osana kokonaisturvallisuutta eikä jälkeenpäin liitettävänä osana (Argaw ym. 2020). Se edellyttää kokonaisvaltaista lähestymistapaa, jossa huomioidaan koko järjestelmä yksittäisten uhkien sijaan. Organisaatioiden tulee huolehtia omasta kyberturvallisuudestaan, mutta myös toimialakohtainen yhteistyö voi tuoda merkittäviä etuja kyberuhkien torjunnassa. Yhteistyö mahdollistaa osaamisen jakamisen ja yhteisten uhkien tehokkaamman hallinnan. Kyberuhkien kansainvälinen luonne korostaa myös rajat ylittävän yhteistyön merkitystä. Suomessa Viestintäviraston Kyberturvallisuuskeskus koordinoi monialaista yhteistyötä, jonka tavoitteena on vahvistaa kansallista kyberturvallisuutta ja varautumiskykyä. (Norri-Sederholm ym. 2019.)

Kyberuhkia voidaan lähestyä monella tapaa; ensisijaista on kuitenkin uhkien tunnistaminen ja torjuminen. Terveysalan kyberturvallisuuden parantaminen on kaikkien kansalaisten etu, sillä se vaatii vahvaa ymmärrystä sekä tietoturvasta että terveydenhuollon toimintatavoista. Siksi on olennaista, että tietoisuutta lisätään ja henkilöstöä koulutetaan säännöllisesti. (Norri-Sederholm ym. 2019.) Sosiaali- ja terveysalan organisaatioissa verkkorikollisia kiinnostavia tietoja käytetään laajasti niin eri ammattiryhmien käsitteleminä kuin eri ohjelmistoissa ja sovelluksissa. Arkaluontoisia tietoja käsitellään sosiaali- ja terveysalan henkilöstön toimesta muun muassa potilastietojärjestelmissä, sähköisissä lääkemääräyksissä, potilaan etäseurantasovelluksissa sekä laboratoriotietojärjestelmissä. Lisäksi tietoja voi käsitellä esimerkiksi sihteerit ja muut toimijat, jotka ovat välillisesti tekemisissä potilastietojen kanssa. Kyberturvallisuutta lisääviä toimenpiteitä tulee siis kohdentaa

laajasti niin erilaisiin toimintaympäristöihin kuin niiden käyttäjiin. (Argaw ym. 2020; Kruse ym. 2017.)

Tulevaisuudessa on äärimmäisen tärkeää, että puututaan yhä tehokkaammin kyberturvallisuutta parantaviin toimiin kaikkialla sosiaali- ja terveysalan kontekstissa. Tutkimusten mukaan tehokkain keino kyberturvallisuuden parantamisessa on laadukas koulutus kaikilla organisaation tasoilla. Koulutuksen tulisi olla jatkuvaa ja säännöllistä. Tärkeimmät yksittäiset toimet liittyvät erilaisten verkkopohjaisten huijausten tunnistamiseen, salasanojen laatuun ja siihen, miten kukin pystyy toimimaan mahdollisimman kyberturvallisesti. (Cartwright 2023.)

Sosiaali- ja terveysala kohtaa yhä enenevässä määrin erilaisia uhkatekijöitä, joten tarvitaan muutosta kyberturvallisempaan suuntaan. Tämä vaatii yksilön käyttäytymisen, teknologian ja prosessien kehittämistä, jotta saavutetaan kokonaisvaltainen muutos. Kyberturvallisuuden lisääminen tulee olla suunnitelmallista alusta alkaen, esimerkiksi silloin, kun otetaan käyttöön uusia laitteita tai järjestelmiä. Muutosta tarvitaan myös yleiseen kyberturvallisuuskulttuuriin, jonka tulee koskettaa organisaation kaikkia toimijoita. Tavoitetilana on rakentaa ”ihmislähtöinen palomuuri”, jossa jokainen toimii osana kyberturvallisuuden suojaverkostoa. (Coventry & Branley 2018.)

4 Tutkimuksen tarkoitus, tavoitteet ja tutkimuskysymykset

Tämän opinnäytetyön tarkoituksena oli selvittää Jyväskylän ammattikorkeakoulun (JAMK) järjestämän “Kyberturvallisuutta sosiaali- ja terveysalan ammattilaisille” -täydennyskoulutukseen osallistujien näkökulmia kyberturvallisuudesta sosiaali- ja terveysalalla. Koulutus oli osa laajempaa hanketta, jossa JAMK oli mukana. Tavoitteena oli tarkastella osallistujien näkökulmasta niitä kyberturvallisuuden seikkoja, jotka vaikuttavat kyberturvallisuutta lisäävästi sosiaali- ja terveysalan kontekstissa. Lisäksi opinnäytetyössä tarkasteltiin sitä, miten täydennyskoulutus on vaikuttanut osallistujien kyberturvallisuusosaamiseen. Tavoitteena oli vahvistaa olemassa olevaa tietoa ja tuoda uutta näkökulmaa aiheeseen. Tuloksia voidaan hyödyntää tulevaisuudessa suunniteltaessa sosiaali- ja terveysalalle kohdennettuja kyberturvallisuuteen liittyviä kokonaisuuksia esimerkiksi organisaation perehdytysohjelmat ja osaamisen kehittäminen, täydennyskoulutukset sekä koulutusohjelmien kehittäminen.

Opinnäytetyössä pyrittiin hakemaan vastauksia edellä esitettyihin asioihin seuraavien tutkimuskysymysten avulla:

> Mitkä tekijät lisäävät kyberturvallisuutta sosiaali- ja terveysalalla täydennyskoulutukseen osallistujien näkökulmasta?
>
> Miten täydennyskoulutus vaikuttaa kyberturvallisuusosaamiseen osallistujien näkökulmasta?

5 Toteutus

5.1 Tutkimusmenetelmä

Opinnäytetyön tavoitteita lähdettiin saavuttamaan laadullisen eli kvalitatiivisen tutkimuksen metodin mukaisesti. Laadullinen tutkimus menetelmänä ei ole yksiselitteinen. Se ikään kuin kokoaa monenlaisia lähestymistapoja ja tutkimusperinteitä. Laadullista tutkimusta voidaan selventää pohtimalla sille tyypillisiä piirteitä, sen yhteyttä teoriaan sekä sitä, miten erilaiset näkökulmat vaikuttavat tuotettuun tietoon. (Vuori 2021.) Yhtenä keskeisenä piirteenä voidaan kuvata sen perustuvan ihmisten subjektiivisten kokemusten ja näkemysten tarkasteluun (Puusa & Juuti 2020). Tässä opinnäytetyössä toteutetaan mitä suuremmassa määrin juuri tuota laadullisen tutkimuksen ominaispiirrettä, koska aineistona on ihmisen, oppijan, omin sanoin kertomat kokemukset.

Hirsjärven ja muiden (2009) mukaan kvalitatiiviselle tutkimukselle on tyypillistä, että tietoa kerätään kokonaisvaltaisesti ja aineistonkeruun lähteenä on ihminen (Hirsjärvi, Remes & Sajavaara 2009). Tämän opinnäytetyön aineisto saatiin täydennyskoulutukseen osallistujien reflektiotehtävän avoimista kysymyksistä. Kysely onkin yksi monista laadullisen tutkimuksen moninaisista aineistonkeruumenetelmistä. Muita menetelmiä voivat olla muun muassa erityyppiset haastattelut (strukturoitu/puolistrukturoitu haastattelu, teemahaastattelu, avoin haastattelu, syvähaastattelu, reflektiivinen haastattelu, ryhmähaastattelu), havainnointi (tutkijan rooli: osallistuva, osallistuva havainnoija tai ulkopuolinen havainnoija) tai erilaisista dokumenteista koottu tieto. Kaikkia näitä menetelmiä voidaan käyttää yksin tai yhdessä tutkittavan kohteen mukaan. (Puusa & Juuti 2020; Tuomi & Sarajärvi 2018.)

Laadullisessa tutkimuksessa pyritään selventämään ratkaistavaa ongelmaa kokonaisvaltaisesti. Voidaan ajatella, että laadullisessa tutkimuksessa pyritään löytämään tai paljastamaan tosiasioita eikä tarkoituksena ole todentaa jo olemassa olevia totuuksia. Tutkija pyrkii induktiivisen analyysin avulla osoittamaan jo olemassa olevaa, eikä tavoitteena ole teorian tai hypoteesin testaaminen. (Hirsjärvi ym. 2009; Eskola & Suoranta 1998.) Puusa ja Juuti (2020) kuvaavat laadullisen tutkimuksen pyrkimyksiä eräänlaisina ihannemalleina tai teoreettisina yleistyksinä. Teorioita ei muodosteta siinä mielessä kuin niitä on yleisesti totuttu ymmärtämään luonnontieteissä. Ne ovat esimerkinomaisia tietoja tai tyypittelyjä eli ihannemalleja tai yleistyksiä, joita voidaan käyttää tutkimuksessa teorioiden tapaan. (Puusa & Juuti 2020.)

Laadullista tutkimusta voidaan lähestyä monen eri metodologian kautta. Laadukkaassa tutkimuksessa tutkijan on hyödyllistä perehtyä laadullisen tutkimuksen perusteisiin, prosessiin ja ominaispiirteisiin. Lisäksi erilaisiin metodologisiin lähestymistapoihin tutustuminen on tärkeää, jotta tutkimuksen uskottavuus ja luotettavuus säilyvät. Huolellinen perehtyminen perusteisiin helpottaa tutkimuksen suunnittelua, analyysia ja tutkittavan ilmiön ymmärtämistä. (Puusa & Juuti 2020.)

Puusa ja Juuti (2020) alleviivaavat laadullisen tutkimuksen hermeneuttisuutta. Hermeneuttinen metodologia tutkimuksessa keskittyy muun muassa aineiston (tekstit, puheet, toiminnat, kokemukset) ymmärtämiseen ja tulkintaan sekä iteratiiviseen kehämäisyyteen (hermeneuttinen kehä). Lisäksi hermeneutiikkaan liittyy vahvasti myös tutkijan esiymmärryksen merkitys suhteessa tutkittavaan ilmiöön. Esiymmärryksellä tarkoitetaan tutkijan omakohtaista tai toisen kautta (esim. kirjallisuus) saatua tietoa, näkemystä tai kokemusta ilmiöstä tutkimusprosessin alkuvaiheessa. Esiymmärrystä voidaan käyttää tutkimuksen hyväksi laajentamalla näkökulmaa ilmiöstä tai esiymmärrys voi jopa vääristää tuloksia. Tällöin joudutaan pohtimaan tutkijan näkemysten ja esiymmärryksen vaikutuksia tutkimustulosten tulkinnassa. (Puusa & Juuti 2020.)

Huhtinen ja Tuominen (2020) taas haastavat pohtimaan myös fenomenologisen lähestymistavan näkökulmaa laadullisessa tutkimuksessa. Laadullinen tutkimus tarkastelee ihmisten subjektiivisia kokemuksia ja näkemyksiä. Fenomenologian pyrkimyksenä on lisätä ymmärrystä ilmiöstä tutkittavan näkökulman kautta. (Huhtinen & Tuominen 2020.) Tämän opinnäytetyön metodologinen lä-

hestymistapa mukailee fenomenologista lähestymistapaa. Opinnäytetyössä tarkasteltiin nimenomaan yksilöiden subjektiivisia näkemyksiä ja tavoitteena oli lisätä ymmärrystä tietystä ilmiöstä eli kyberturvallisuudesta sosiaali- ja terveysalalla.

Tämän opinnäytetyön lähestymistapa mukailee fenomenologiaa ja aineiston analyysissa hyödynnetään induktiivista sisällönanalyysia. Fenomenologinen lähestymistapa pyrkii lisäämään ymmärrystä tutkittavasta ilmiöstä sekä pyrkii ymmärtämään ihmisten subjektiivisia kokemuksia eli lisäämään ymmärrystä ilmiöstä tutkittavan näkökulman kautta. Fenomenologiassa keskeistä on kokemusten merkitysten tavoittaminen ja ilmiön ymmärtäminen sellaisena kuin se ilmenee tutkittavalle. Fenomenologiassa tieto ja ymmärrys rakentuvat kokemukseksi vähitellen vastavuoroisuudessa ympäröivän todellisuuden kanssa. Siinä lähestytään tutkittavaa ilmiötä vailla ennakkokäsityksiä ja pyritään siihen, että aiemmat käsitykset eivät ohjaa analyysia. Analyysia syvennetään tulkitsemalla merkityksiä ja kokemuksia. (Huhtinen & Tuominen 2020.) Tässä opinnäytetyössä fenomenologinen ote näkyy siinä, että läpi koko prosessin tutkija pyrkii tietoisesti ohittamaan kaikki mahdolliset ennakkokäsitykset ja kokemukset. Fenomenologiaa tukee myös se, että analyysivaiheessa keskitytään pelkästään aineistoon ja siitä saatuihin päätelmiin.

5.2 Aineistonkeruu ja kuvaus

Jyväskylän ammattikorkeakoulu (JAMK) järjesti kyberturvallisuuteen liittyvän täydennyskoulutuksen sosiaali- ja terveysalan ammattilaisille. Koulutuksen laajuus oli 3 opintopistettä eli laskennallisesti yhteensä 81 tuntia opiskelijan työtä (yksi opintopiste vastaa 27 tuntia opiskelijan työtä). Kaikki koulutukseen osallistujat olivat sosiaali- ja terveysalan ammattilaisia. Tässä opinnäytetyössä sosiaali- ja terveysalan ammattilainen tarkoittaa laissa sosiaali- ja terveydenhuollon järjestämisestä (L612/2021) määriteltyä sosiaali- ja terveydenhuollon parissa työskentelevää henkilöä, joka on osallistunut aineiston lähteenä olevaan täydennyskoulutukseen (L612/2021). Koulutus on kohdennettu juuri heille, joten oletuksena on, että heillä kaikilla on vaihteleva määrä kokemusta sosiaali- ja terveysalalta. Opinnäytetyön kannalta oleellista on ainoastaan se, että osallistujat ovat alan ammattilaisia eikä esimerkiksi heidän kokemuksensa määrä ole merkityksellistä.

Osallistujien kyberturvallisuustietoisuuden ja -osaamisen taso vaihteli, mikä kävi ilmi aineistosta, vaikka heidän taustaosaamistaan ei erikseen kysytty. Jokaisella oli kuitenkin jonkinlaista työn

kautta kertynyttä näkemystä siitä, millä tasolla heidän tietoisuutensa ja osaamisensa on kyberturvallisuuden suhteen. Opinnäytetyössä ei kuitenkaan pyritty arvioimaan osallistujien lähtötason osaamista tai sen vaikutusta, vaan keskiössä olivat osallistujien koulutuksen jälkeiset näkemykset kyberturvallisuutta edistävistä tekijöistä sekä koulutuksen tuomat oppimiskokemukset.

Koulutukseen osallistujien viimeisenä opintojakson osiona oli reflektiotehtävä, jossa opiskelijoilta kysyttiin erilaisia koulutukseen liittyviä kysymyksiä. Kysymykset sisälsivät sekä strukturoituja että avoimia kysymyksiä. Avoimet kysymykset koskivat osallistujien näkemyksiä kyberturvallisuuteen sosiaali- ja terveysalalla, sosiaali- ja terveysalalla vaadittavaa kyberturvallisuusosaamista sekä omaa oppimista täydennyskoulutuksen aikana. Avoimista kysymyksistä saatuja vastauksia käytettiin tämän opinnäytetyön aineistona.

Opinnäytetyön aineisto kerättiin siis opintojakson viimeisen tehtävän reflektio-osuudesta, jossa opiskelijat muun muassa pohtivat opintojakson sisältöä suhteessa kyberturvallisuuteen, sosiaali- ja terveysalan ammattilaisen osaamisen tarpeita sekä omaa oppimistaan. Opiskelijat vastasivat viimeisen tehtävän kysymyksiin samoin kuin olivat tehneet muutkin opintojakson tehtävät eli opiskelijoiden digitaalisessa oppimisympäristössä. Koulutukseen osallistujilta ei siis vaadittu mitään ylimääräistä vaivannäköä, joka ei olisi kuulunut opintojaksoon. Ainoa opinnäytetyöhön viittaava asia oli heidän suostumuksensa tai kielteinen päätöksensä siitä, voitiinko avoimiin kysymyksiin annettuja vastauksia käyttää tässä opinnäytetyössä.

Täydennyskoulutus oli osa laajempaa hanketta, jonka puitteissa JAMK:lla oli tutkimuslupa koulutukseen liittyvien tiettyjen osa-alueiden hyödyntämisestä tutkimuskäyttöön. Osallistujilta kysytyn hankkeen tutkimusluvan lisäksi heiltä siis pyydettiin vielä erikseen suostumusta reflektiotehtävän avointen kysymysten käyttöön aineistona juuri tässä opinnäytetyössä. Osallistujilla oli mahdollisuus hyväksyä tai hylätä pyyntö osallistumisesta opinnäytetyöhön.

Suostumuspyyntölomake laadittiin Webropol-sovellukseen ja linkki saatekirjeineen lähetettiin kaikille osallistujille sähköpostilla opintojakson vastuuopettajien toimesta. Myönteisiä vastauksia saatiin yhteensä 12 opiskelijalta. Myönteisen vastauksen antaneiden opiskelijoiden reflektiotehtävän vastaukset anonymisoitiin vastuuopettajien toimesta. Anonymisoinnissa siis poistettiin kaikki se tieto, joka voisi paljastaa jotain vastaajasta tai vaikkapa hänen työskentelyorganisaatiostaan (Kuula

2011). Anonymisoinnin jälkeen vastaukset toimitettiin sähköpostitse Word-tiedostona opinnäytetyötä varten.

5.3 Aineiston analyysi

Laadullisin menetelmin analysoitaessa aineistoa voidaan lähestyä teorialähtöisesti, teoriasidonnaisesti tai aineistolähtöisesti riippuen tutkijan suhteesta teoriaan (Eskola 2018). Tässä työssä sisällönanalyysin tavaksi muodostui aineistolähtöisyys, koska tarkoituksena oli nimenomaan selvittää, minkälaisia aiheita aineistosta nousi esiin. Haluttiin selvittää, toistuuko selkeästi tietyt teemat tai aihepiirit vai koetaanko kyberturvallisuus esimerkiksi vielä liian abstraktina asiana sosiaali- ja terveysalan kontekstissa. Analyysia ei haluttu sitoa tiettyyn teoriaan ja haluttiin säilyttää kvalitatiiviselle aineiston analyysitekniikalle ominainen avoimuus. Aineiston analyysin tavoitteena oli ilmiön kuvaaminen, tulkitseminen ja ymmärtäminen tutkimuksen näkökulmasta. (Puusa & Juuti 2020.)

Tämän opinnäytetyön kohdalla oli selkeää, että aineistoa lähdettiin analysoimaan induktiivisesti, koska haluttiin selvittää mitä asioita aineistosta nousee esiin ilman teoreettista taustaa tai laajempaa esiymmärrystä. Laadullisessa tutkimuksessa ei kuitenkaan ole olemassa yksiselitteistä ohjeistusta oikean tai sopivimman analyysimenetelmän valintaan. Aineiston käsittelytavat vaihtelevat tutkimuksittain. Laadullisessa tutkimuksessa on kaiken kaikkiaan vain vähän vakiintuneita tapoja aineiston analyysiin. Mikään analyysitapa ei ole toistaan parempi, vaan analyysitapa tulee valita tarkoituksenmukaisesti tutkimuksen tavoitteet ja aineiston kokonaisuus huomioiden. (Puusa & Juuti 2020.)

Laadullisen tutkimuksen analyysissa yhdistyy analyysi ja synteesi. Tutkija siis erittelee ja yhdistelee aineistoa. Tällä tarkoitetaan sitä, että kerätty aineisto jaetaan osiin valitun menetelmän mukaan, jonka jälkeen tutkija tekee aineiston perusteella synteesejä ja kokoaa sen uudelleen. (Puusa & Juuti 2020.) Myös tämä opinnäytetyö nojautuu tuohon ajatukseen erittelystä ja yhdistelystä. Aineisto pilkottiin ensin pieniin analyysiyksiköihin, jotka sitten lopulta koottiin yhdistäviin luokkiin.

Aineisto koostui opintojakson reflektiotehtävän kyselyn kolmen avoimen kysymyksen vastauksista. Kaiken kaikkiaan vastauksia saatiin 12 opiskelijalta, vastauskokonaisuuksia oli siis yhteensä 36. Avoimet kysymykset oli laadittu koulutuksen vastuuopettajien toimesta opintojakson sisällön näkökulmasta. Opinnäytetyön tekijällä ei ole ollut mahdollisuutta vaikuttaa kysymysten sisältöön tai

muotoon. Avoimet kysymykset palvelivat ennen kaikkea opettajien intentioita esimerkiksi arvioitaessa opintojakson tarkoituksenmukaisuutta tai sen mahdollisia kehittämistarpeita. Opinnäytetyön tekijä ei ole siis voinut vaikuttaa saatuun aineistoon esimerkiksi suuntaamalla kysymyksiä tiettyyn suuntaan. Tämä opinnäytetyön tekijän läsnäolottomuus aineiston keruuvaiheessa teki sen, että aineisto oli hyvin paljas ja raaka tekijän näkökulmasta. Aineiston sisältö oli opinnäytetyön tekijälle täysin odottamaton. Minkäänlaisia ennakkokäsityksiä tai rajoituksia ei myöskään päässyt syntymään ennen analysointivaihetta. Avoimista kysymyksistä kaksi antoi näkökulmia opinnäytetyön tavoitteeseen löytää kyberturvallisuutta edistäviä tekijöitä ja viimeisen kysymyksen vastaukset selvensivät tavoitetta selventää täydennyskoulutuksen vaikutuksia kyberturvallisuusosaamiseen.

Aineistoon pureuduttiin induktiivisen sisällönanalyysin mukaisesti. Analyysi jaettiin Elo ja Kyngäs (2008) mukaisesti kolmeen päävaiheeseen: valmistelu-, analyysi- ja raportointivaihe. Aivan aluksi aineisto luettiin läpi muutamaan kertaan, jotta kokonaisuudesta saatiin yleisnäkemys. Tämä oli ikään kuin esivalmistelua varsinaiselle analyysille. (Elo & Kyngäs 2008.) Näiden ensimmäisten lukukertojen aikana aineistosta havaittiin selkeitä ja yhteneväisiä osakokonaisuuksia, joiden perusteella pystyttiin muodostamaan analyysiyksiköt varsinaista analyysia varten.

Aineistolähtöisessä sisällönanalyysissa pyritään muodostamaan vastaus tutkimustehtävään yhdistelemällä käsitteitä. Menetelmässä edetään empiirisestä aineistosta kohti käsitteellisempää näkemystä tutkittavasta ilmiöstä ja se perustuu tutkijan tulkintaan ja päättelyyn. Koko analyysin ajan aineistossa tulee kuitenkin säilyttää polku alkuperäisdataan. Aineiston analyysin tavoitteena on järjestää tutkittavasta ilmiöstä saatu data selkeään ja tiiviiseen muotoon säilyttäen sen ydin. Hajanaisesta tiedosta pyritään kokoamaan yhtenäinen, mielekäs ja looginen kokonaisuus tutkittavasta ilmiöstä. (Tuomi & Sarajärvi 2018; Eskola & Suoranta 1998.) Tässä opinnäytetyössä pidettiin erityisen tärkeänä sitä, että alkuperäisdatan sisältö oli läsnä koko ajan. Analysoidessa haluttiin varmistua siitä, että aineiston ydin saadaan pysymään mukana muuttumattomana. Tämä varmistettiin sillä, että aineiston autenttiset ilmaukset olivat nähtävillä koko analyysin ajan.

Valmisteluvaiheeseen liittyy analyysiyksiköiden muodostaminen, jotta aineiston analyysi on systemaattista ja yhdenmukaista. Analyysiyksikkö valitaan sen mukaan mitä halutaan tutkia. Yksikkö voi olla esimerkiksi sana, teema tai lause. Se kannattaa kuitenkin valita niin, että se on yksiselitteinen,

ettei analyysiprosessista tule liian mutkikas yksikön monimerkityksellisyyden takia. Toisaalta analyysiyksikön ei kannata olla liian kapea, ettei aineisto pirstaloidu liikaa. (Elo & Kyngäs 2008.)

Valmisteluvaiheessa analyysiyksiköksi päätettiin ajatuskokonaisuudet ”kyberturvallisuutta lisäävät tekijät” sekä ”täydennyskoulutuksen vaikutus kyberturvallisuusosaamiseen”. Tässä kohtaa varmistettiin vielä se, että tutkimuskysymykset olivat asetettu niin, että niihin saadaan vastaukset aineistosta. Tässä vaiheessa tutkimuskysymyksiä hienosäädettiin vielä hieman parempaan muotoon.

Seuraavaksi aineisto siirrettiin Word-tiedostosta Exceliin taulukkomuotoon käsittelyn helpottamiseksi. Aineisto taulukoitiin muotoon: vastaus (autenttinen ilmaus), yksi analyysiyksikkö (autenttinen ilmaus), pelkistys, alaluokka, yläluokka ja pääluokka. Alla olevassa kuvassa (kuvio 1) näkyy analyysiluokkien ryhmittely ja yksittäinen esimerkki analyysin ensimmäisessä vaiheessa.

Vastaus (autenttinen ilmaisu)	Yksi analyysiyksikkö (autenttinen ilmaisu)	Pelkistys	Alaluokka	Yläluokka	Pääluokka
Vastaajan teksti kokonaisuudessaan	…potilastietojärjestelmien tietosuoja on oltava luotettava…	Potilastietojärjestelmien tietosuojan on oltava luotettava.	Luotettava potilastietojärjestelmien tietosuoja.	Terveydenhuollon järjestelmien tietoturvallisuus.	Tietoturvalliset asiakasjärjestelmät.

Kuvio 1. Aineiston analyysiluokat ja yksittäinen analyysiesimerkki pääluokkaan asti.

Ensimmäiseen sarakkeeseen laitettiin koko vastaus (eli yksittäisen vastaajan koko vastaus yhteen kysymyksistä), toiseen sarakkeeseen poimittiin vastauksesta yksi analyysiyksikön mukainen ilmaisu, kolmanteen sarakkeeseen ilmaus pelkistettiin, neljänteen sarakkeeseen muodostettiin alaluokka, viidenteen yläluokka ja viimeiseksi kokoava pääluokka. Koko ajan haluttiin pitää mukana alkuperäinen, autenttinen teksti kokonaisuudessaan. Lisäksi haluttiin säilyttää yksittäinen autenttinen ilmaisu (analyysiyksikkö), jotta reitti alkuperäisdataan pysyi jatkuvasti läsnä. Tämä varmisti sen, että autenttisen ilmaisun ydin ei muutu analyysin aikana (Puusa & Juuti 2020). Tässä analyysiyksikön löytämisessä, pelkistämisessä ja luokkien muodostamisessa tapahtuu Puusan ja Juutin (2020) kuvailemaa aineiston erittelyä ja yhdistelyä (Puusa & Juuti 2020). Alla olevasta kuvasta (kuvio 2) havainnollistetaan kyberturvallisuutta lisäävien tekijöiden analysointi autenttisesta ilmaisusta pääluokkaan asti.

Yksi analyysiyksikkö (autenttinen ilmaisu)	Pelkistys	Alaluokka	Yläluokka	Pääluokka
Ensinnäkin jokaisen työntekijän pitäisi tunnistaa tämä (kyberturvallisuus) oikeaksi ja tärkeäksi asiaksi, myös sote-alan tehtävissä.	Jokaisen työntekijän pitäisi tunnistaa kyberturvallisuus oikeaksi ja tärkeäksi asiaksi, myös sote-alan tehtävissä.	Kyberturvallisuuden tunnistaminen merkittäväksi teemaksi sote-alalla.	Kyberturvallisuuden tunnistaminen osana sote-alan toimintaympäristöä.	Ymmärrys kyberturvallisuudesta sote-alalla.
Sosiaali- ja terveysalan ammattilaisen tulisi hallita perustoimenpiteet kyberturvallisuuteen liittyen.	Sosiaali- ja terveysalan ammattilaisen tulisi hallita perustoimenpiteet kyberturvallisuuteen liittyen.	Sosiaali- ja terveysalan ammattilaisen kyberturvallisuusosaamisen perusteet hallinnassa.	Henkilöstön tulisi osata kyberturvallisuuden perusasiat.	Henkilöstön kyberturvallisuuden perusosaaminen.
…ammattilaisten… tulisi… ymmärtää, mitä tietoja ovat velvollisia suojelemaan ja miksi.	Ammattilaisten tulisi ymmärtää, mitä tietoja ovat velvollisia suojelemaan ja miksi.	Ymmärrys, mitä tietoja tulee suojella ja miksi.	Tietojen suojelemisen tärkeyden ymmärtäminen.	Tietoturva- ja tietosuojaosaaminen.
Sote-ammattilaisten tulisi tietää, miten luodaan ja ylläpidetään vahvoja salasanoja.	Sote-ammattilaisten tulisi tietää, miten luodaan ja ylläpidetään vahvoja salasanoja.	Tietämys vahvojen salasanojen merkityksestä.	Osaaminen tietosuojasta ja tietoturvasta.	
… miten tunnistaa haittaohjelmia ja välttää niiden leviämistä organisaatiossa.	Miten tunnistaa haittaohjelmia ja välttää niiden leviämistä organisaatiossa.	Haittaohjelmien tunnistaminen ja niiden leviämisen välttäminen organisaatiossa.	Ymmärrys laitteiden ja ohjelmistojen kyberuhkista.	Osaamisen lisääminen kyberuhkiin liittyen.
Henkilöstön tulisi tunnistaa kyberhyökkäysten reitit… sähköpostien linkit…	Henkilöstön tulisi tunnistaa kyberhyökkäysten reitit, kuten sähköpostien linkit.	Kyberhyökkäysten reittien tunnistaminen.	Kyberuhkien tunnistaminen.	

Kuvio 2. Kyberturvallisuutta lisäävien tekijöiden analysointia pääluokkaan asti.

Koko aineisto (36 erillistä vastausta) käytiin läpi edellä mainitun sisällön analyysin mukaisesti. Pääsääntöisesti aineisto oli erittäin yksityiskohtaista ja käytännönläheistä. Aineistosta näki, että vastaajat olivat reflektoineet opintojakson teemoja omaan työympäristöön ja työnkuvaansa. Vastausten pituus vaihteli parista lauseesta pariin kymmeneen lauseeseen. Vastausten sisältö suhteessa tutkittavaan asiaan oli vaihtelevaa. Yhden vastauksen sisältä saattoi löytää jopa 20 erillistä analyysiyksikköä. Toisaalla sitten yhdestä vastauksesta saattoi löytyä vain yksi soveltuva analyysiyksikkö.

Abstrahointia eli ryhmittelyä tai yhdistelevää luokittelua jatketaan niin kauan kuin se on tutkimuksen tarkoituksen ja tutkimuskysymysten kannalta merkityksellistä (Elo, Kajula, Tohmola & Kääriäinen 2022). Tässä opinnäytetyössä vastausten yksityiskohtaisuus ja käytännönläheisyys johti siihen, että muodostuneet pääluokat eivät olleet vielä riittävän koottuja ensimmäisellä analyysikerralla. Kuten edellä olevasta analyysiesimerkistä (kuvio 2) voidaan havaita, saavutetut pääluokat jäävät vielä liian yksityiskohtaisiksi, joten analysointia oli tarpeen tarkastella vielä lisää. Tässä vaiheessa koko aineisto käytiin läpi huolellisesti vielä kertaalleen, jotta jokainen luokittelu on tehty samojen

perustelujen mukaan suhteessa niin analyysiyksiköihin kuin tutkimuskysymyksiin. Tällä varmistuttiin se, että aineistosta on huomioitu juuri ne asiat, mitä on haluttu ottaa mukaan tähän opinnäytetyöhön.

Analyysissa saavutetut pääluokat eivät siis olleet vielä riittävän kokoavia, joten abstrahointia jatkettiin pidemmälle. Pääluokan jälkeen lisättiin vielä Elo ja Kyngäs (2008) mukaisesti yksi yhdistävä luokka, jotta uudelleen kootusta aineistosta pystyttiin tekemään päätelmiä. Sisällönanalyysin perimmäisenä tavoitteena on kuitenkin järjestää aineisto tiiviiksi, selkeäksi ja yhtenäiseksi kokonaisuudeksi, jotta raportointivaiheessa pystytään tekemään johtopäätöksiä tutkittavasta ilmiöstä. (Elo & Kyngäs 2008.) Seuraavassa kuvassa (kuvio 3) näkyy, että kun esimerkkianalyysia (kuvio 2) kyberturvallisuutta lisäävistä tekijöistä jatkettiin, löydettiin kaikkia kuvion pääluokkia kokoava yhdistävä luokka, osaaminen ja ymmärrys.

Yksi analyysiyksikkö (autenttinen ilmaisu)	Pelkistys	Alaluokka	Yläluokka	Pääluokka	Yhdistävä luokka
Ensinnäkin jokaisen työntekijän pitäisi tunnistaa tämä (kyberturvallisuus) oikeaksi ja tärkeäksi asiaksi, myös sote-alan tehtävissä.	Jokaisen työntekijän pitäisi tunnistaa kyberturvallisuus oikeaksi ja tärkeäksi asiaksi, myös sote-alan tehtävissä.	Kyberturvallisuuden tunnistaminen merkittäväksi teemaksi sote-alalla.	Kyberturvallisuuden tunnistaminen osana sote-alan toimintaympäristöä.	Ymmärrys kyberturvallisuudesta sote-alalla.	Osaaminen ja ymmärrys
Sosiaali- ja terveysalan ammattilaisen tulisi hallita perustoimenpiteet kyberturvallisuuteen liittyen.	Sosiaali- ja terveysalan ammattilaisen tulisi hallita perustoimenpiteet kyberturvallisuuteen liittyen.	Sosiaali- ja terveysalan ammattilaisen kyberturvallisuusosaamisen perusteet hallinnassa.	Henkilöstön tulisi osata kyberturvallisuuden perusasiat.	Henkilöstön kyberturvallisuuden perusosaaminen.	
...ammattilaisten... tulisi... ymmärtää, mitä tietoja ovat velvollisia suojelemaan ja miksi.	Ammattilaisten tulisi ymmärtää, mitä tietoja ovat velvollisia suojelemaan ja miksi.	Ymmärrys, mitä tietoja tulee suojella ja miksi.	Tietojen suojelemisen tärkeyden ymmärtäminen.	Tietoturva- ja tietosuojaosaaminen.	
Sote-ammattilaisten tulisi tietää, miten luodaan ja ylläpidetään vahvoja salasanoja.	Sote-ammattilaisten tulisi tietää, miten luodaan ja ylläpidetään vahvoja salasanoja.	Tietämys vahvojen salasanojen merkityksestä.	Osaaminen tietosuojasta ja tietoturvasta.		
... miten tunnistaa haittaohjelmia ja välttää niiden leviämistä organisaatiossa.	Miten tunnistaa haittaohjelmia ja välttää niiden leviämistä organisaatiossa.	Haittaohjelmien tunnistaminen ja niiden leviämisen välttäminen organisaatiossa.	Ymmärrys laitteiden ja ohjelmistojen kyberuhkista.	Osaamisen lisääminen kyberuhkiin liittyen.	
Henkilöstön tulisi tunnistaa kyberhyökkäysten reitit... sähköpostien linkit...	Henkilöstön tulisi tunnistaa kyberhyökkäysten reitit, kuten sähköpostien linkit.	Kyberhyökkäysten reittien tunnistaminen.	Kyberuhkien tunnistaminen.		

Kuvio 3. Kyberturvallisuutta lisäävien tekijöiden analysointia yhdistävään luokkaan asti.

Analyysi tehtiin siis vielä systemaattisesti uudelleen, kun uusi yhdistävä luokka lisättiin mukaan. Haluttiin varmistaa analyysin tarkkuus ja analyysin laadun tasaisuus läpi koko aineiston. Yhdistävän luokan avulla analyysia voitiin koota ja tiivistää eteenpäin. Tämä mahdollisti perusteltujen päätel-

mien tekemisen ja syvemmän käsitteellisen ymmärryksen saavuttamisen tutkittavasta ilmiöstä tutkimuksen pohdintaosuudessa. Sisällönanalyysi toimii siis käytännössä menetelmänä, joka auttaa jäsentämään empiiristä aineistoa tulkintaa varten. (Puusa & Juuti 2020.) Alla olevassa kuvassa (kuvio 4) havainnollistetaan vielä lisää aineiston analyysia. Siinä tarkastellaan kyberturvallisuutta lisääviä tekijöitä autenttisesta ilmaisusta yhdistävään luokkaan asti.

Yksi analyysiyksikkö (autenttinen ilmaisu)	Pelkistys	Alaluokka	Yläluokka	Pääluokka	Yhdistävä luokka
...hyvät tietoturvakäytänteet olisivat luonnollinen osa työtehtävää...	Hyvät tietoturvakäytänteet luonnollinen osa työtehtävää.	Työtä tehdään tietoturvakäytänteiden mukaisesti.	Tietoturvakäytänteet osa työtehtävää.	Tietoturvallinen työskentelytapa.	Yksilön vastuullinen toiminta
Itse olen aina pitänyt tärkeänä hyvästä... tietotuvasta huolehtimisen...	Itse olen aina pitänyt tärkeänä hyvästä tietoturvasta huolehtimisen.	Hyvästä tietoturvasta huolehtiminen oman toiminnan kautta.	Vastuu omasta tietoturvallisesta toiminnasta.		
Potilaat... odottavat, että heidän tietonsa pysyvät ...yksityisinä.	Potilaat odottavat, että heidän tietonsa pysyvät yksityisinä.	Potilaiden odotus yksityisyydensuojasta.	Tietoturvan mukainen työskentely.		
Jokaiseen niistä (eri järjestelmät) kohdistuu kyberuhkia, joiden torjumisessa työntekijöiden rooli käyttäjinä korostuu.	Jokaiseen järjestelmään kohdistuu kyberuhkia, joiden torjumisessa työntekijöiden rooli käyttäjinä korostuu.	Työntekijän korostunut rooli järjestelmien käyttäjänä kyberuhkien torjumiseksi.	Työntekijän vastuullinen toiminta kyberuhkien torjumisessa.	Työntekijän vastuu kyberturvallisesta toiminnasta.	
Jos voin omalla toiminnallani, vaikkapa käyttämällä vahvaa salasanaa, torjua rikollisuutta, se on sen vaivan väärti.	Jos voin omalla toiminnallani torjua rikollisuutta, se on sen vaivan väärti.	Oman toiminnan merkitys (kyber-)rikollisuuden torjumiseksi.			

Kuvio 4. Kyberturvallisuutta lisäävien tekijöiden analyysia.

Laadullisessa tutkimuksessa on myös mahdollista käyttää kvantifiointia. Sillä tarkoitetaan tietyn asian (lause, sana, yksikkö, koodi) laskemista aineistosta eli esiintymistiheyttä (Puusa & Juuti 2020). Kvantifioinnilla voidaan osoittaa jonkin asian suurempaa esiintymistiheyttä, mikä voi tuoda uutta näkökulmaa raportointivaiheessa. Kvantifioinnilla voidaan myös korostaa tietyn asian merkityksellisyyttä. (Elo ym. 2022.) Tässä opinnäytetyössä kvantifioinnin avulla haluttiin syventää tulosten analysointia pohdintaosuudessa. Kvantifiointia hyödynnettiin siinä vaiheessa, kun synteesiä oli jatkettu pääluokasta vielä pidemmälle yhdistävään luokkaan eli, kun lopulliset tulokset on saatu analysoitua. Kyberturvallisuutta lisääviä tekijöitä analysoitaessa havaittiin, että aineistosta ilmeni selkeästi yksi enemmän esiintyvä teema, kaksi muuta suunnilleen yhtä monta kertaa mainittua teemaa ja kaksi vähemmän, mutta merkittävästi, mainintoja saanutta teemaa. Täydennyskoulutuksen vaikutuksia tarkasteltaessa tunnistettiin kolme kokonaisuutta, joiden kvantifiointi osoitti selkeitä määrällisiä eroja. Tuloksia tarkastellaan syvemmin pohdintaosuudessa.

6 Tulokset

6.1 Kyberturvallisuutta lisääviä tekijöitä

Opinnäytetyön tavoitteena oli selvittää, mitkä tekijät lisäävät kyberturvallisuutta sosiaali- ja terveysalalla täydennyskoulutukseen osallistujien näkökulmasta. Analyysin perusteella löydettiin viisi yhdistävää luokkaa (kuvio 5), jotka kuvaavat kyberturvallisuutta lisääviä teemoja. Nämä kokonaisuudet ovat *osaaminen ja ymmärrys*, *yksilön vastuullinen toiminta*, *organisaation panostus kyberturvallisuuteen*, *organisaation kyberturvallisuuskäytänteet* sekä *järjestelmien ja laitteiden turvallisuus*.

Kuvio 5. Kyberturvallisuutta lisäävät tekijät.

Opinnäytetyön tulokset tarjoavat kattavan kuvan tekijöistä, jotka vaikuttavat kyberturvallisuuden lisäämiseen sosiaali- ja terveysalalla täydennyskoulutukseen osallistuvien näkökulmasta. Nämä kyberturvallisuutta lisäävät tekijät korostavat osaamisen, organisaation käytänteiden sekä työntekijän roolin merkitystä kyberturvallisuutta lisäävinä teemoina. Teemat limittyvät osin toisiinsa, mutta muodostavat silti selkeät kokonaisuudet.

6.1.1 Osaaminen ja ymmärrys

Analyysin perusteella merkittävimmäksi kyberturvallisuutta lisääväksi tekijäksi nousi kyberturvallisuusosaamiseen liittyvät asiat. Osaaminen ja siihen liittyvät tekijät, kuten tietoisuus, ymmärrys ja koulutus, korostuivat aineistossa eri näkökulmista. Kyberturvallisuusosaaminen nähtiin keskeisessä roolissa turvallisen kybertoimintaympäristön ylläpitämisessä. Henkilöstön tietoisuuden ja osaamisen lisääminen auttaa ymmärtämään kyberuhkien vaikutuksia ja toimimaan tehokkaasti niiden torjumiseksi. Pelkät toimivat ja turvalliset järjestelmät ja laitteet eivät riitä takaamaan toimintaa, vaan tarvitaan osaavaa ja tietoista henkilöstöä, joka kykenee varmistamaan, että toiminta pysyy turvallisena.

> *…tietoisuuden ja henkilöstön koulutuksen lisääminen on tärkeää monesta näkökulmasta…*

> *…erittäin tärkeä kiinnittää huomiota kyberturvallisuuteen monesta eri syystä… potilastietojen suojelu… toiminnan jatkuvuus…*

> *Sosiaali- ja terveysalan ammattilaisen tulisi hallita perustoimenpiteet kyberturvallisuuteen liittyen.*

Kyberturvallisuutta lisää se, että henkilöstöllä on riittävä perusosaaminen kyberturvallisuudesta ja, että heillä on mahdollisuus osaamisen päivittämiseen ja syvällisempään osaamisen kehittämiseen. Kyberturvallisuutta lisäävänä tekijänä pidettiin osaamisen kehittämisessä koulutuksen jatkuvuutta, säännöllisyyttä ja ajantasaisuutta. Henkilöstölle tarjottavat koulutukset eivät saa olla yksittäisiä, vaan osaamisen kehittämisen tulee olla jatkuvaa ja säännöllistä. Tämä takaa sen, että henkilöstö pysyy perillä kyberturvallisuuden käytännöistä sekä uusista uhkista, ja osaa toimia tehokkaasti uhkien torjumiseksi. Kyberturvallisuus kehittyy ja muuntuu jatkuvasti, joten osaamisen ylläpito on välttämätöntä.

> *Kyberturvallisuus… perusosaaminen kuuluisi tärkeänä osana hoitoalan koulutusta…*

> *…kyberturvallisuus on jatkuvasti muuttuva alue… säännöllinen ja systemaattinen ammattilaisten kouluttaminen sekä ymmärryksen lisääminen on tärkeää.*

Säännölliset kyberturvallisuuskoulutukset, koska kaikki muuttuu…

…tulisi olla säännöllisesti tietosuoja- ja tietoturvakoulutusta.

Kyberturvallisuutta lisäävinä tekijöinä pidettiin myös sitä, että henkilöstölle tarjotaan kohdennettua koulutusta niin organisaatiossa kuin sosiaali- ja terveysalan laajemmassa kontekstissa. Erityisesti sosiaali- ja terveysalalle räätälöity koulutus on tärkeää, muun muassa sen takia, että ala käsittelee sensitiivisiä tietoja ja vaatii vankkaa tietosuojaa. Lisäksi ala kohtaa erityisiä riskejä, kuten monimutkaiset järjestelmät ja verkottuneet laitteet. Näiden tekijöiden vuoksi vastaajat kokivat, että kyberturvallisuuden jatkuva päivittäminen on elintärkeää.

Sosiaali- ja terveysalalla käsitellään hyvin arkaluonteisia potilastietoja…

…laitteiden (lääketieteelliset laitteet) haavoittuvuudet voivat altistaa ne hakkereiden hyökkäyksille, jotka voivat aiheuttaa vakavia riskejä potilaiden turvallisuudelle.

Kyberhyökkäykset voivat aiheuttaa valtavia… toiminnallisia… ongelmia terveydenhuollon organisaatioille.

Kyberturvallisuuden eri osa-alueiden hallinta edistää kyberturvallisuusosaamista. Aineiston analyysin perusteella kyberturvallisuusosaamisen ymmärrys itsessään oli yksi merkittävistä oivalluksista kyberturvallisuutta lisäävänä tekijänä. Tällä tarkoitetaan sitä, että sosiaali- ja terveysalalla toimivat ymmärtävät kyberturvallisuuden olemassaolon tärkeyden ja sen moninaisuuden. Kyberturvallisuus on yhtä lailla tärkeä osa toimintaympäristön kokonaisturvallisuutta kuin esimerkiksi potilasturvallisuus tai kriittisten toimintojen huoltovarmuus.

…tulee tunnistaa, kuinka ison uhkan kanssa olemme tekemisissä ja että se uhka on arkitodellisuutta.

…jokaisen työntekijän pitäisi tunnistaa tämä (kyberturvallisuus) oikeaksi ja tärkeäksi asiaksi, myös sote-alan tehtävissä.

Usein… ei nähdä sen (kyberturvallisuus) merkitystä omaan työhön tai asiakkaisiin.

…kyberturvallisuus on tärkeää potilaiden yksityisyyden ja turvallisuuden, terveydenhuollon jatkuvuuden, luottamuksen ylläpidon ja laajemman yhteiskunnallisen vakauden kannalta.

Kyberturvallisuusosaaminen ei rajoitu pelkästään tietoturva- ja tietosuojaosaamiseen, vaan siihen liittyy osaamista niin laitteista, järjestelmistä kuin riskien tunnistamisesta. Aineiston perusteella kyberturvallisuutta lisäävänä tekijänä on se, että henkilöstö tuntee ja ymmärtää organisaation kyberturvariskit ja -uhkat. Riskien tunnistaminen ja niihin varautuminen on ensisijaisen tärkeää. Myös kyberturvallisuusosaamisen soveltamista omaan työympäristöön tai organisaatioon pidettiin merkittävänä. Kyberturvallisuusosaamisen ajantasaisuus ja sen toteutuminen käytännön työssä ovat avaintekijöitä, jotka varmistavat organisaation kyberturvallisuuden.

…sosiaali- ja terveysalan ammattilaisten tulisi olla tietoisia kyberturvallisuuden periaatteista ja käytännöistä sekä osata soveltaa niitä päivittäisessä työssään varmistaakseen potilastietojen ja terveydenhuollon järjestelmien turvallisuuden.

Huolehtimalla henkilöstön riittävästä tietoturvaosaamisesta… kyberhyökkäyksiä voidaan välttää.

…sote-ammattilaisten tulisi sitoutua jatkuvaan oppimiseen ja uusimpien uhkien ja torjuntakeinojen seuraamiseen.

Ammattilaisten pitää osallistua koulutuksiin ja olla tietoisia riskeistä ja miten toimia jos epäilee tietoturvaloukkausta.

Tulosten perusteella yhteenvetona voidaan todeta, että henkilöstön kyberturvallisuusosaamisen kehittäminen on keskeinen tekijä kyberturvallisuuden parantamisessa sosiaali- ja terveysalalla. Koulutuksen tulee kattaa perusasiat, tietoturva- ja tietosuojaosaaminen sekä lainsäädäntö ja käytännöt. Henkilöstön tulee ymmärtää kyberuhkien luonne ja osata reagoida niihin tehokkaasti. Täy-

dennyskoulutukseen osallistuvien näkökulmasta henkilöstön säännöllinen ja ajankohtainen koulutus sekä kyberturvallisuuden integroiminen työnkuvaan ovat elintärkeitä kyberturvallisuutta edistäviä tekijöitä.

6.1.2 Yksilön vastuullinen toiminta

Tuloksista käy ilmi, että osallistujat näkivät kyberturvallisuutta lisäävinä tekijöinä kaksi osapuolta: organisaatio ja yksilö. Organisaatio voi panostuksellaan ja painotuksellaan lisätä kyberturvallisuutta esimerkiksi erilaisten ohjeiden muodossa ja yksilö voi lisätä kyberturvallisuutta toimimalla ohjeiden mukaisesti. Yksilön vastuullisella toiminnalla viitataan siis siihen mitä yksilö voi tehdä kyberturvallisuuden lisäämiseksi organisaatiossa. Yksinkertaistettuna se on sitä, että yksilö tunnistaa kyberturvallisuuden olemassaolon ja sen tärkeyden. Lisäksi, että hän toimii olemassa olevien ohjeiden ja käytäntöjen mukaisesti sekä pyrkii aina toimimaan kyberturvallisesti.

> *…hyvät tietoturvakäytänteet olisivat luonnollinen osa työtehtävää…*

> *…sosiaali- ja terveysalan ammattilaisten tulisi olla tietoisia kyberturvallisuuden periaatteista ja käytännöistä sekä osata soveltaa niitä päivittäisessä työssään…*

> *Kyberturvallisuudesta huolehtiminen on jokaisen työntekijän tehtävä.*

Yksilön vastuullinen toiminta ilmenee tuloksissa myös kyberturvallisuusosaamisen integroimisena omaan työnkuvaan. Henkilöstön tietoisuus kyberuhkien lisääntymisestä sosiaali- ja terveysalalla ja ymmärrys niiden vaikutuksista organisaatiolle ovat avaintekijöitä kyberturvallisuuden parantamisessa. Vastuullisella toiminnalla viitataan myös siihen, että yksilöllä on merkittävä osuus organisaation kyberhyökkäysten havaitsemisessa ja tietoturvapoikkeamien hallinnassa. Kyberturvallisuustietoisuuden tulisi olla luonnollinen osa työnkuvaa ja kokonaisvaltaista turvallisuutta. Ammattilaisten tulisi ymmärtää, että heidän oma toimintansa on merkittävässä roolissa kyberturvallisuutta lisäävänä tekijänä.

> *Jos voin omalla toiminnallani, vaikkapa käyttämällä vahvaa salasanaa, torjua (kyber)rikollisuutta, se on sen vaivan väärti.*

…sote-ammattilaisten tulisi sitoutua jatkuvaan oppimiseen ja uusimpien uhkien ja torjuntakeinojen seuraamiseen.

…omalla toiminnalla voit vaikuttaa niin positiivisesti kuin negatiivisesti tietoturvan toteutumiseen.

…työntekijän rooli, se miten pystyn itse vaikuttamaan organisaationi kyberturvallisuuteen.

Osallistujat toivat esiin, että yksilön vastuullisen toiminnan mahdollistamiseen vaikuttivat organisaation sitoutuminen ja tuki. Organisaation panostukset kyberturvallisuuteen vaikuttavat suoraan siihen, miten yksilöt suhtautuvat kyberturvallisuuteen ja toimivat vastuullisesti. Kun yksilö ottaa kyberturvallisuuden vakavasti ja toimii sen mukaisesti, se vahvistaa merkittävästi koko organisaation turvallisuutta.

6.1.3 Organisaation panostus kyberturvallisuuteen

Aineistosta nousi esiin kyberturvallisuutta lisäävänä tekijänä se, että koko organisaatio ja sen kaikki toimijat ovat sitoutuneet kyberturvalliseen toimintaan. Kyberturvallisuutta lisää se, että ymmärretään sen olevan osa kokonaisturvallisuutta eikä kyberturvallisuus ole erillinen osa. Vastaajat kokivat, että organisaation selkeä kyberturvallisuussuunnitelma ja positiivinen panostus kyberturvallisuuteen lisää kokonaisturvallisuutta. Organisaation riittävä resurssien kohdentaminen kyberturvallisuuteen viestii sen arvostuksesta ja siitä, kuinka merkityksellisenä kyberturvallisuutta pidetään.

Kyberturvallisuus on huomioitava organisaatioiden kaikissa toiminnoissa.

Riittävällä (kyber)turvallisuudella saadaan myös lisättyä luottamusta terveydenhuoltoon.

… kyberturvallisuudella turvataan hoidon ja palvelun laatu ja tehokkuus.

Aineiston perusteella riittävä resursointi nähtiin keskeisenä kyberturvallisuutta lisäävänä tekijänä. Kyberturvallisuuteen sijoittaminen ei ole vain tekninen kysymys, vaan myös taloudellinen ja organisatorinen sitoumus. Organisaatioiden on varattava riittävästi resursseja kyberturvallisuuteen, mukaan lukien henkilöstön koulutus, teknologian päivittäminen ja tietoturvasuunnitelmien ylläpito. Organisaation riittävä resursointi kyberturvallisuuteen on välttämätöntä kyberturvallisuuden parantamiseksi. Organisaation on varattava riittävät resurssit niin taloudellisesti kuin henkilöstömäärällisesti kyberturvallisuuden kehittämiseen.

> *Talouden näkökulmasta on edullisempaa kouluttaa henkilöstöä kyberturvalliseen työtapaan kuin korjata syntyneitä virheitä.*

> *Huolehtimalla henkilöstön riittävästä tietoturvaosaamisesta kyberhyökkäyksiä voidaan välttää.*

> *…työnantajalta koulutusta kyberturvallisuuteen liittyen…*

> *Kyberturvallisuudesta huolehtiminen vaikuttaa talouteen… hyökkäykset aiheuttavat organisaatioille taloudellisia vahinkoja.*

Vastauksissa korostui se, että organisaation panostusta pidettiin merkittävänä kyberturvallisuutta lisäävänä tekijänä. Riittävä panostus voi esimerkiksi suojata organisaatiota kyberhyökkäysten mahdollisilta taloudellisilta menetyksiltä tai vaikkapa mainehaitalta. Organisaation panostus kyberturvallisuuteen on myös osa organisaation toiminnan laatua ja kokonaisturvallisuutta.

6.1.4 Organisaation kyberturvallisuuskäytänteet

Organisaation kyberturvallisuuskäytänteet nousivat hyvin yksiselitteisesti esiin analyysissa kyberturvallisuutta lisäävänä tekijänä. Organisaation kyberturvallisuuskäytänteet ovat ikään kuin perustoja tai peruskiviä, joita organisaatio tarjoaa kyberturvallisuuden lisäämiseksi. Toisin sanoen jotain sellaista, mitä organisaatio voi konkreettisesti ja näkyvästi tehdä kyberturvallisuuden lisäämiseksi. Vastaajat korostivat, että selkeät tietoturvakäytänteet ja toimintamallit ovat keskeisiä tekijöitä kyberturvallisuuden hallinnassa ja kyberturvallisuutta lisäävänä tekijänä. Ohjeiden tulisi olla helposti

omaksuttavia ja vaivattomasti saatavilla, kun niitä tarvitaan. Selkeitä toimintamalleja tarvitaan esimerkiksi silloin, kun havaitaan epätyypillistä toimintaa turvallisuuteen liittyen. Tilanteet saattavat tulla eteen nopeasti ja silloin suoraviivaiset ja yksiselitteiset toimintamallit ovat ensisijaisen tärkeitä.

> *… tieto siitä keneen pitää olla yhteydessä, mikäli poikkeavaa toimintaa havaitsee.*
>
> *…miten toimia häiriötilanteessa…*
>
> *Miten tietoturvapoikkeamista tulisi ilmoittaa organisaation sisällä… (mihin) ottaa yhteyttä, jos epäilee hakkerointia.*

Selkeät ja ajankohtaiset kyberturvallisuuskäytänteet ovat elintärkeitä myös organisaation kokonaisturvallisuuden kannalta. Käytännön ohjeiden ja toimintamallien tulisi olla helposti omaksuttavissa ja toteutettavissa työympäristössä. Organisaation on varmistettava, että tietoturvakäytänteet ovat kaikkien tiedossa ja noudatettuja, jotta niistä saadaan haluttu hyöty.

> *Mikäli asianmukaista ohjeistusta ei ole saatavilla toimivat ihmiset yleensä "helpoimman" mukaan, joka yleensä ei ole se turvallisin vaihtoehto.*
>
> *pitää tuntea… organisaation omat tietoturvakäytänteet.*
>
> *Työntekijän tulisi käydä läpi työpaikkansa tietoturvaohjeet ja noudattaa niitä.*

Tuloksissa vastaajat siis peräänkuuluttivat organisaation selkeitä kyberturvallisuuskäytänteitä. Ne ohjaavat toimintaa poikkeustilanteissa ja varmistavat, että työntekijät tietävät, miten toimia oikein. Selkeät ja ajankohtaiset käytänteet tukevat koko organisaation kyberturvallisuuskulttuuria, joka parantaa organisaation valmiuksia kyberuhkien hallintaan.

6.1.5 Järjestelmien ja laitteiden turvallisuus

Järjestelmien ja laitteiden turvallisuuteen liittyy niin organisatoriset näkökulmat kuin niitä käyttävät yksilöt. Aineistossa esiintyi nämä molemmat puolet kyberturvallisuutta lisäävinä tekijöinä. Nähtiin merkittävänä organisaation tarjoamat laadukkaat ja ajantasaiset järjestelmät ja laitteet. Lisäksi korostettiin, että järjestelmien ja laitteiden turvallisuuteen vaikuttaa myös käyttäjän toiminta. Ei siis riitä, että on saatavilla toimintaa tehostavia verkottuneita laitteita tai verkossa toimivia järjestelmiä vaan tarvitaan myös tietämystä ja käsitystä siitä, miten laitteet toimivat ja minkälaisia riskejä sisältyy laitteiden ja järjestelmien verkottumiseen.

> *…tunnistaa laitteisiin liittyvät kyberuhkat… koska, haittaohjelmat voivat päästä verkon kautta esim. lääkinnällisiin laitteisiin.*

> *…huomioimaan erilaiset kyberhyökkäykset kuten laitteen poikkeava käytös…*

> *Laitteiden kanssa toimiessa tulisi osata epäillä kyberhyökkäystä, jos laitteessa on poikkeavaa toimintaa.*

Järjestelmien tietoturvallisuus ja kyberturvallisuusohjelmistojen ylläpito ovat kriittisiä tekijöitä kyberturvallisuutta lisäävinä tekijöinä. Organisaation on huolehdittava järjestelmien ja laitteiden toimintavarmuudesta ja ajantasaisuudesta. Tämä sisältää järjestelmien säännöllisen päivityksen ja ylläpidon. Henkilöstön tietoisuus teknologian ylläpidosta ja ajantasaisuudesta vaikuttavat organisaation kyberturvallisuuteen. Henkilöstön on ymmärrettävä, miksi säännöllinen ohjelmistojen päivitys ja järjestelmien huolto ovat tärkeitä. Ymmärrys laitteiden ja ohjelmistojen kyberuhkista sekä niiden päivittämisen tärkeydestä ovat keskeisiä osa-alueita kyberturvallisuutta lisäävänä tekijänä.

> *Sote-ammattilaisten ymmärrys siitä, miksi laitteiden ja ohjelmistojen päivittäminen on tärkeää…*

> *Päivitykset ajan tasalla…*

Ammattilaisten pitää myös noudattaa ohjeistusta ohjelmien päivittämisestä, jos organisaatiossa se ei tapahdu automaattisesti.

Sosiaali- ja terveydenhuollossa käytetään runsaasti erilaisia verkottuneita laitteita ja järjestelmiä. Laitesuojauksen ja laiteturvallisuusosaamisen merkitys korostuu erityisesti juuri terveydenhuollon ympäristössä, jossa käsitellään arkaluonteisia tietoja. Kyberturvallisuutta lisää niin laitteiden ja järjestelmien käytön osaaminen kuin ymmärrys niiden mahdollisista kyberuhkista ja -riskeistä. Aineistosta kävi ilmi, että laitteiden ja järjestelmien käyttäjät eivät aina ole tietoisia niiden aiheuttamista kyberturvallisuusriskeistä.

…tulee tunnistaa laitteisiin liittyvät kyberuhkat.

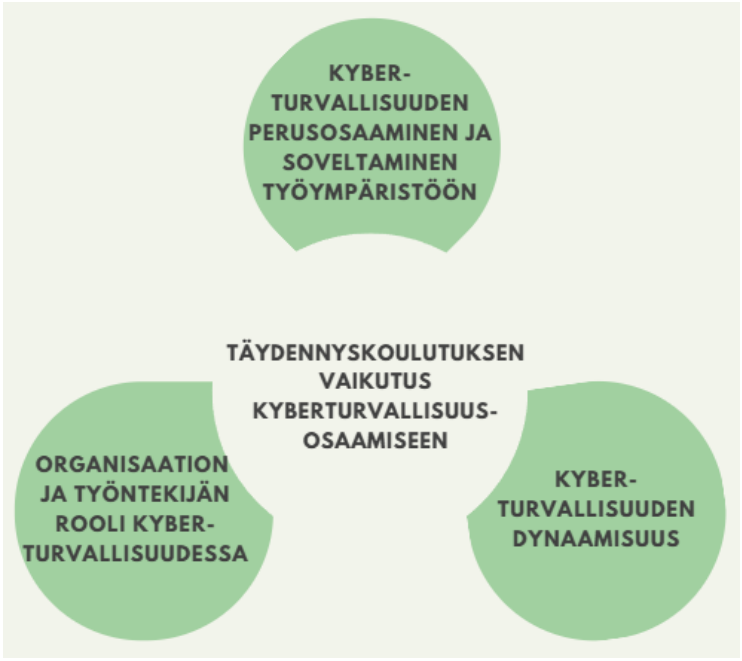
Henkilöstön tulisi tunnistaa kyberhyökkäysten reitit.

Vastaajat painottivat sitä, että järjestelmien ja laitteiden turvallisuus liittyy vahvasti kyberturvallisuutta lisääviin tekijöihin. Kaikki verkottuneet laitteet ja järjestelmät ovat potentiaalisia kyberhyökkäysten kohteita. Tulosten perusteella kyberturvallisuutta lisää erityisesti se, että laitteet ja järjestelmät ovat ajantasaisia ja niitä käyttävä henkilöstö toimii vastuullisesti.

6.2 Täydennyskoulutuksen vaikutus kyberturvallisuusosaamiseen

Tässä opinnäytetyössä selvitettiin myös sitä, miten täydennyskoulutus on vaikuttanut osallistujien kyberturvallisuusosaamiseen. Aineistosta selvisi, että koulutus on vaikuttanut monipuolisesti osallistujien tietoisuuteen ja osaamiseen kyberturvallisuudesta. Tulokset korostavat myös sitä, että vastaajien ymmärrys kyberturvallisuuden dynaamisuudesta on lisääntynyt.

Täydennyskoulutuksen vaikutuksista nousi esiin kolme kokonaisuutta. Nämä kokonaisuudet on kuvattu alla olevassa kuvassa (kuvio 6).



Kuvio 6. Täydennyskoulutuksen vaikutukset kyberturvallisuusosaamiseen.

Tärkeimpänä täydennyskoulutuksen vaikutuksena kyberturvallisuusosaamiseen pidettiin kyberturvallisuuden *perusasioiden oppimista, kertaamista sekä tietojen soveltamista käytäntöön*.Toisena kokonaisuutena ilmeni *ymmärrys kyberturvallisuuden dynaamisuudesta*. Sillä tarkoitetaan niin kyberturvallisuustietoisuuden jatkuvaa päivittymistä ja muovautumista kuin kyberturvallisuuden kanssa operoivan yksilön jatkuvan oppimisen ajattelutapaa. Kyberturvallisuustieto evolvoituu eli kehittyy ja muuttuu jatkuvasti; se ikään kuin sopeutuu uusiin uhkiin, teknologioihin ja toimintaympäristöihin. Se vaatii siten säännöllistä tietojen päivittämistä, omaksumista ja uuden tiedon soveltamista omaan toimintaympäristöön.

Kolmantena kokonaisuutena tuloksista nousi esiin *organisaation ja yksilön roolien ymmärrys kyberturvallisuuden toteuttajina*. Molemmilla on yhtä tärkeä rooli kyberturvallisuuden toteutumiseksi parhaalla mahdollisella tavalla organisaatiossa. Täydennyskoulutukseen osallistujat kokivat saaneensa paremman käsityksen kyberturvallisuuden yhteisvastuullisuudesta organisaatiossa.

6.2.1 Kyberturvallisuuden perusosaaminen ja soveltaminen työympäristöön

Kyberturvallisuuden perusosaaminen ja sen soveltaminen työympäristöön oli yleisimmin esiintynyt teema. Täydennyskoulutuksella on siis ollut suurin vaikutus perusosaamisen kehittämiseen ja sen soveltamiseen työssä. Aineistossa toistui neljä keskeistä kyberturvallisuuden perusosaamisen osa-aluetta, joissa täydennyskoulutus on edistänyt osallistujien osaamista. Nämä aiheet olivat *käsitteet*, *kyberuhkien tunnistaminen ja niiden hallinta*, *laitteet ja järjestelmät* sekä *tietoturva ja tietosuoja*.

Monet olivat oppineet tai saaneet kertausta kyberturvallisuuden peruskäsitteistä ja termeistä. Keskeiset termit ja käsitteet ovatkin äärimmäisen tärkeää hallita, jotta kaikki tietävät mistä puhutaan. Kyberturvallisuus saatetaan myös kokea hankalana ja abstraktina asiana, joten käsitteiden ja termien ymmärrys vähentää pelkoa kohdata kyberturvallisuuteen liittyviä asioita. Käsitteet ja termit ovat osa kyberturvallisuuden perustietoutta ja niiden ymmärtäminen on ensisijaista osaamisessa.

> *…keskeisten käsitteiden selkeytyminen…*

> *Opintojakso oli erittäin hyvää kertausta…*

> *Opin paljon uutta termistöä… myös aikaisemmin hankalan kuuloiset asiat selvenivät kurssin myötä.*

Vastaajat korostivat, että täydennyskoulutus on parantanut heidän kykyään tunnistaa ja käsitellä kyberturvallisuuspoikkeamia. Esimerkiksi järjestelmien ja laitteistojen kyberturvallisuuspoikkeamien havaitseminen nousi esiin merkittävänä oppimiskokemuksena. Koulutus on siis onnistunut lisäämään ymmärrystä teknisistä uhkista ja niiden ennaltaehkäisystä, mikä on keskeistä, kun ajatellaan potilasturvallisuutta ja tietosuojaa.

> *Aikaisemmin on luottanut järjestelmien aukottomuuteen ja turvallisuuteen. Opin kiinnittämään huomiota ohjelmistojen ja laitteistojen toimivuuteen ja niiden mahdollisiin vikatiloihin.*

Oma ymmärrykseni kasvoi etenkin lääkinnällisten laitteiden kyberturvallisuuden osalta… tätä en aiemmin ole edes ajatellut.

…opintojakson jälkeen, tärkeintä työssäni on tietää, mitä pitää tehdä, kun haavoittuvuus tunnistetaan ohjelmistossa.

Erilaisten lääkinnällisten laitteiden, järjestelmien ja ohjelmistojen kyberturvallisuuden ymmärtäminen on erityisen tärkeää terveydenhuollon kontekstissa, jossa monet laitteet toimivat verkon kautta ja voivat altistua kyberuhkille. Aineistosta havaittiin, että näiden osa-alueiden kohdalla osaaminen on lisääntynyt täydennyskoulutuksessa. Lisäksi aineistosta ilmeni, että koulutus on lisännyt ymmärrystä siitä, miten tietoturva ja kyberturvallisuus voidaan huomioida päivittäisessä työskentelyssä sosiaali- ja terveysalalla. Tämä käytännönläheinen näkökulma on erityisen tärkeä, koska kyberturvallisuusuhkat voivat ilmetä arjen työtilanteissa, kuten potilastietojen käsittelyssä tai laitteiden käytössä.

… tuli ymmärrys lääkintälaitteiden kyberturvallisuudesta…

Oma ymmärrykseni kasvoi eteenkin lääkinnällisten laitteiden kyberturvallisuuden osalta.

Kurssin myötä osaan kiinnittää enemmän huomiota työpaikalla tietoturva-asioihin…

…osaan arvioida myös omaa toimintaani tietosuoja- ja tietoturva-asioissa...

Aineisto osoitti, että nimenomaan ymmärrys on lisääntynyt tietoturvaan ja -suojaan liittyvissä asioissa. Ei pelkästään se, että suoritetaan tiettyjä toimintoja turvallisuuden lisäämiseksi, vaan myös se, että ymmärretään, miksi näin tehdään. Vastaajat kokivat pystyvänsä toimimaan turvallisemmin omassa työympäristössään täydennyskoulutuksen jälkeen.

6.2.2 Kyberturvallisuuden dynaamisuus

Kyberturvallisuuden dynaamisuudella viitataan siihen, että kyberturvallisuus on jatkuvassa muutoksessa ja siihen liittyvät asiat muuttuvat ja muovautuvat koko ajan. Tämä aineistosta ilmennyt kokonaisuus korostaa sitä, että myös osaamisen tulee olla dynaamista. Se ei pysy muuttumattomana, vaan muokkautuu ja jalostuu jatkuvasti ympäristön ja tilanteiden mukaan. Dynaamisen luonteen vuoksi myös yksilöltä vaaditaan ajan tasalla olemista ja kiinnostusta siihen, että halutaan tietää uusimmista muutoksista. Yksilöltä edellytetään jatkuvaa tietojen päivittämistä, uuden tiedon omaksumista sekä soveltamista omaan toimintaympäristöön. Yksilön ymmärrys tietouden ja osaamisen päivittämisen merkityksestä osoittautui merkittäväksi teemaksi. Täydennyskoulutukseen osallistujille kirkastui käsitys siitä, miten keskeistä on säännöllinen ja ajantasainen osaamisen päivittäminen.

> *Tietoturvan jatkuva kehittäminen on myös olennainen osa sosiaali- ja terveydenhuolto työtä.*

> *Kyberturvallisuuden täydennyskoulutukset tulisi olla mielestäni säännöllistä ja jatkuvaa.*

> *…(kyberturvallisuus)koulutusten lisääminen työyhteisön säännölliseen koulutuskalenteriin olisi tarpeen.*

Täydennyskoulutukseen osallistujat olivat oivaltaneet sen, että osaamisen on oltava muuttuvaa ja aktiivista. Yksilön on pystyttävä kehittymään kyberturvallisuuden muuttuessa. Dynaamisuus kyberturvallisuuden kontekstissa vaatii panostusta ja tahtoa niin yksilöltä kuin organisaatiolta.

6.2.3 Organisaation ja työntekijän rooli kyberturvallisuudessa

Useat vastaajat toivat esiin henkilöstön ja työnantajan roolin kyberturvallisuuden toteutumisessa. Täydennyskoulutus on edistänyt ymmärrystä kyberturvallisuuden yhteisvastuullisesta luonteesta ja korostanut jokaisen työntekijän merkitystä. Täydennyskoulutuksen avulla osallistujat ovat saaneet laajemman ymmärryksen siitä, miten organisaatiotasolla voidaan vaikuttaa muun muassa kyberuhkien hallintaan. Organisaation sekä henkilöstön roolin korostuminen on tärkeää erityisesti

tilanteissa, joissa kyberuhkat voivat vaikuttaa koko organisaation toimintaan. Koulutus on auttanut vastaajia ymmärtämään, miten he voivat omalla toiminnallaan edistää kyberturvallisuutta organisaatiossa. Lisäksi he ovat ymmärtäneet miten työnantajan tuki voi vahvistaa tätä osaamista.

> *…jokainen omalta osaltaan huolehtii tietoturvasta ja tietosuojasta, jolloin ammattilaiset tekevät organisaatiosta turvallisen ja luotettavan asiakkaille.*

> *…työntekijän rooli, se miten pystyn itse vaikuttamaan organisaationi kyberturvallisuuteen.*

> *…yksittäisen työntekijän rooli tietosuojan/-turvan toteuttamisessa valtavan suuri.*

Täydennyskoulutus toi myös uutta ymmärrystä ja näkökulmaa organisaation ja yksilön roolista kyberturvallisuutta toteuttava tahona. Organisaatioilla tulee olla selkeä kyberturvallisuussuunnitelma. Kyberturvallisuuden implementoinnissa on jokaisella työntekijällä myös oma merkittävä roolinsa. Organisaatio on ikään kuin fasilitaattori ja kyberturvallisuuden mahdollistaja ja työntekijä on kriittinen osa kyberturvallisuuden toteuttajana.

> *Aiemmin olin ajatellut kyberturvallisuuden enemmänkin organisaation tietojärjestelmiin, kuten potilastietojärjestelmään liittyväksi.*

> *Henkilöstön roolin ja työnantajan roolin hahmottuminen kokonaiskuvaksi ja varsinaisen ydintehtävän ympärille suojaamaan ja varautumaan.*

Aineiston analyysi paljasti, että täydennyskoulutus on ollut keskeisessä osassa muuttamassa yksilöiden asenteita ja käsityksiä kyberturvallisuutta kohtaan. Aineistosta heijastui vastaajien aito kokonaisvaltainen osaamisen kehittyminen. Vastaajat kokivat, että täydennyskoulutus on ollut tehokas väline vahvistamaan tietoutta, osaamista ja koko kyberturvallisuuskulttuuria.

7 Pohdinta

Tässä opinnäytetyössä selvitettiin sosiaali- ja terveysalan ammattilaisille suunnatun kyberturvallisuutta käsittelevän täydennyskoulutuksen osallistujien arvioita siitä, mitkä tekijät lisäävät kyberturvallisuutta sekä miten täydennyskoulutus on vaikuttanut heidän kyberturvallisuusosaamiseensa. Opinnäytetyön tavoitteena oli vahvistaa olemassa olevaa tietoa ja tuottaa tietoa kyberturvallisuutta vahvistavista tekijöistä sekä täydennyskoulutuksen vaikutuksista kyberturvallisuusosaamiseen. Näiden asioiden selvittäminen on tärkeää, jotta niitä voidaan vahvistaa ja kehittää yhä paremmiksi.

Sosiaali- ja terveydenhuollon ammattilaisen oma näkökulma aiheeseen on tärkeä, jotta koulutuksen tarpeita ja motivaatiota voidaan selvittää kohteilta itseltään. Tulokset voivat toimia perustana uusille koulutusohjelmille, alan kyberturvallisuusohjeistuksille tai jopa teknologisille kehitysratkaisuille. Ammattilaisten kokemusten ymmärtäminen yhdistää teorian ja käytännön, mikä lisää tutkimuksen vaikuttavuutta. Laajemmin ajateltuna ammattilaisten omat arviot kyberturvallisuusosaamisen merkittävyydestä omassa roolissa, työympäristössä ja organisaatiossa on tärkeää saada tietoon, jotta voidaan ikään kuin oikeuttaa täydennyskoulutuksen tarve. Ammattilaisesta itsestä lähtöisin tuleva tarve kyberturvallisuusosaamisen lisäämiseksi on jo selkeä merkki siitä, että aihe on ymmärretty ja tarve on tullut esiin. Tällöin henkilön voidaan ajatella olevan hyvässä vaiheessa suhteessa sisäiseen motivaatioon oppia lisää aiheesta; on ymmärretty aiheen tärkeys, tarpeellisuus ja ajankohtaisuus.

Tutkimalla ammattilaisten kokemuksia täydennyskoulutuksesta voidaan vaikuttaa sen sisällöllisiin tarpeisiin, laatuun ja vaikuttavuuteen tulevaisuudessa, mikä hyödyttää sekä organisaatioita että yksilöitä. Ammattilaisten näkökulma aiheeseen on merkityksellistä, sillä heiltä saatu tieto auttaa kohdentamaan tarvittavat toimenpiteet paremmin. Argaw ja muut (2020) vahvistavat artikkelissaan, että koulutuksen sisällön kohdentamiseksi ja laadun parantamiseksi olisi tärkeää, että koulutusta suunniteltaessa tulisi olla perusteltu arvio eli ammattilaisen näkemys siitä, minkälaista koulutusta tarvitaan ja mitä puutteita osaamisessa on (Argaw ym. 2020). Tällöin mahdollistetaan kohdennettu osaamisen vahvistaminen, tiedon syventäminen ja keskittyminen niihin osa-alueisiin, jotka ovat kriittisiä, tässä tapauksessa, kyberturvallisuuden kannalta. Ammattilaisten näkemykset auttavat myös ymmärtämään, miten kyberturvallisuustoimenpiteet voidaan sovittaa arkeen siten, että ne ovat toteutettavissa ja vaikuttavia.

Opinnäytetyöstä saatuja tuloksia voidaan hyödyntää kehittämällä sosiaali- ja terveysalan erityispiirteet huomioivia kyberturvallisuuteen liittyviä kokonaisuuksia, esimerkiksi organisaation perehdytysohjelmat ja täydennyskoulutukset. Tulosten perusteella voidaan myös tehdä päätelmiä teemoista, joiden kautta sosiaali- ja terveysalan kyberturvallisuuskulttuuria on mahdollista parantaa. Tulokset tarjoavat myös arvokasta tietoa siitä, miten kyberturvallisuuskulttuuria voidaan vahvistaa integroimalla kyberturvallisuus osaksi arjen toimintatapoja ja edistämällä tietoisuutta sekä ymmärrystä organisaatiossa.

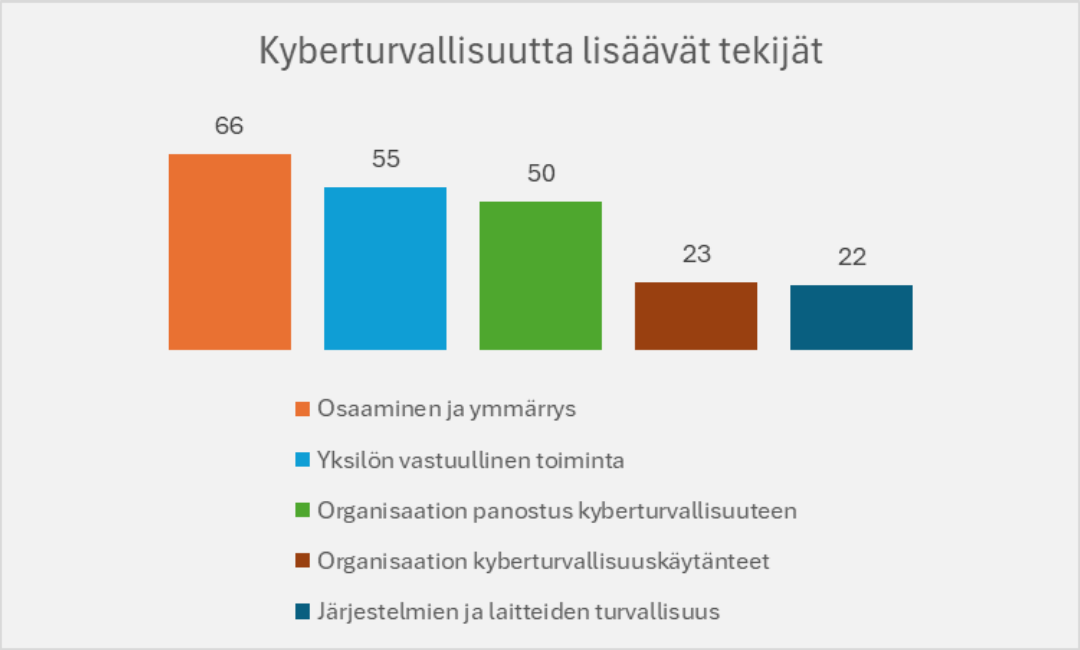
7.1 Kyberturvallisuuden vahvistaminen

Opinnäytetyössä tehdyn analyysin perusteella löydettiin viisi kyberturvallisuuteen liittyvää kokonaisuutta, jotka koettiin lisäävän sosiaali- ja terveysalan kyberturvallisuutta. Nämä kokonaisuudet ovat *osaaminen ja ymmärrys*, *yksilön vastuullinen toiminta*, *organisaation panostus kyberturvallisuuteen*, *organisaation kyberturvallisuuskäytänteet* sekä *järjestelmien ja laitteiden turvallisuus*. Tulosten analyysin syventämiseksi hyödynnettiin kvantifiointia.

Laadullisen tutkimuksen yhteydessä kvantifioinnin käyttö on perusteltua tulosten analysoinnin täydentämiseksi. Kvantifioinnilla tarkoitetaan tietyn asian (lause, sana, yksikkö, koodi) laskemista aineistosta eli esiintymistiheyttä. (Puusa & Juuti 2020.) Kvantifioinnilla voidaan osoittaa jonkin asian suurempaa esiintymistiheyttä, mikä voi tuoda uutta näkökulmaa. Kvantifioinnilla voidaan myös korostaa tietyn asian merkityksellisyyttä. (Elo ym. 2022.)

Tässä opinnäytetyössä kvantifiointia hyödynnettiin siinä vaiheessa, kun synteesiä oli jatkettu pääluokasta vielä pidemmälle yhdistävään luokkaan eli laskettiin yhdistävien luokkien esiintymistiheyttä. Kyberturvallisuutta lisääviä tekijöitä analysoitaessa havaittiin, että aineistosta ilmeni selkeästi yksi enemmän esiintyvä teema, kaksi muuta suunnilleen yhtä monta kertaa mainittua teemaa ja kaksi vähemmän, mutta merkittävästi, mainintoja saanutta teemaa.

Alla olevassa kuvassa (kuvio 7) on pylväskaavio, jossa kuvataan aineistosta analysoidut yhdistävät luokat ja kuinka monta kertaa kukin luokka on esiintynyt.



Kuvio 7. Kyberturvallisuutta lisäävien tekijöiden esiintymistiheys aineistossa.

Kvantifioimalla havaittiin, että osaaminen ja ymmärrys teeman ympärille kerääntyi eniten havaintoja. Tämä osoittaa sen, että kyberturvallisuuden perusosaamista ja ymmärrystä pidettiin merkittävimpänä kyberturvallisuutta lisäävänä asiana. Tämä on linjassa aiempien tutkimusten kanssa siten, että nimenomaan osaamisen vahvistamisella pystytään lisäämään tietoisuutta ja sitä kautta kyberturvallisuutta (Argaw ym. 2020).

Yksilön vastuullinen toiminta sekä organisaation panostus kyberturvallisuuteen kokonaisuuksien ympäriltä löytyi seuraavaksi eniten ja toistensa kanssa suunnilleen yhtä paljon mainintoja. Nämä teemat ovat myös merkittävässä roolissa kyberturvallisuutta lisäävinä tekijöinä. Aiemmissa tutkimuksissa on myös havaittu samankaltaisia löydöksiä esimerkiksi organisaatioiden kyberresilienssiin liittyen. Organisaation tulisi panostaa kestävään kyberturvallisuuteen kokonaisvaltaisesti niin osaamisen lisäämisen kuin vaikkapa resursoinnin kautta. Myös yksilöstä itsestä johtuvan kyberuhkien lisäämisen estämiseksi tarvitaan vastuullista toimintaa. (Nifakos ym. 2021; Argaw ym. 2020.)

Vaikka havaintoja tehtiin vähiten organisaation kyberturvallisuuskäytänteistä ja järjestelmien ja laitteiden turvallisuudesta, näitä teemoja voitiin silti pitää merkityksellisinä kokonaisuuden kan-

nalta. Aiemmissa tutkimuksissa on selkeästi mainittu, että kyberhyökkäysten lisääntyessä digitaalisten toimintaympäristöjen ja niiden käyttäjien kyberturvallisuuteen tulee kohdentaa parantavia ja edistäviä toimenpiteitä (Argaw ym. 2020; Kruse ym. 2017).

Kaikki analyysin perusteella muodostetut luokat linkittyvät vahvasti toisiinsa ja näyttäytyvät myös limittäin. Esimerkiksi järjestelmien ja laitteiden turvallisuus on vahvasti sidoksissa osaamiseen sekä toisaalta myös organisaation panostukseen taloudellisen resurssoinnin kautta (esim. uusien laitteiden hankinta). Saadut tulokset korostavat, että kyberturvallisuus on moniulotteinen alue, joka vaatii laajaa lähestymistapaa. Kyberturvallisuusosaamisen kehittäminen, organisaation tuki, järjestelmien ylläpito, riittävä resursointi ja henkilöstön tietoisuus ovat keskeisiä tekijöitä, jotka yhdessä parantavat kyberturvallisuutta.

7.1.1 Osaaminen ja ymmärrys sekä yksilön vastuullinen toiminta kyberturvallisuutta lisäävinä tekijöinä

Analyysin perusteella kyberturvallisuutta lisäävistä tekijöistä merkittävin on osaamiseen ja ymmärrykseen liittyvät näkökulmat. Sosiaali- ja terveysalan ammattilaisilla tulisi olla riittävä määrä perusosaamista ja tietoutta kyberturvallisuudesta sekä ymmärrystä siitä, miten sitä tulisi hyödyntää omassa toimintaympäristössä. Samansuuntaisia havaintoja on tehty myös aiemmissa tutkimuksissa, joissa korostetaan koulutuksen tärkeyttä sekä osaamisen integroimista käytäntöön (Cartwright 2023; Lehto 2023; Kruse ym. 2017).

Osaamiseen ja etenkin ymmärrykseen liittyy vahvasti myös yksilön toiminta kyberturvallisuuteen liittyvissä asioissa. Yksilön vastuullinen toiminta olikin toisiksi merkittävin kyberturvallisuutta lisäävä kokonaisuus analyysin perusteella. Inhimilliset virheet ovat keskeinen kyberturvallisuusriskien lähde (Cartwright 2023; Blek & Solankallio-Vahteri 2022; Jalali ym. 2020; Kruse ym. 2017). Sosiaali- ja terveysalan ammattilaiset kohtaavat kyberturvallisuuteen liittyviä käytännön haasteita, jolloin heidän osaamisellaan ja toiminnallaan on keskeinen merkitys kyberturvallisuuden toteutumisessa. Ammattilaisen vastuullisuus on yksi avaintekijöistä kyberturvallisuuden onnistumisessa. Heidän on ymmärrettävä, että jokapäiväiset valinnat ja toiminta vaikuttaa suoraan organisaation kyberturvaan. (Argaw ym. 2020.) Alan luonteenomainen kiireisyys, monimuotoisuus ja tiukat sääntelyvaatimukset (mm. tietosuojalait, terveydenhuoltolait, standardit, eettiset ohjeet) tekevät siitä erityisen haavoittuvan kyberuhkille.

Vastuuta yksilön kyberturvallisesta toiminnasta voisi verrata sosiaali- ja terveysalan kontekstissa yleisesti tiedossa olevaan aseptiseen omatuntoon. Aseptisella omatunnolla tarkoitetaan yksilön sitoutuneisuutta oikeanlaisten ja sovittujen käytänteiden mukaiseen aseptiseen työskentelytapaan, myös silloin kun kukaan ei näe. Sen edellytyksenä on vankka tietämys aiheesta sekä kykyä soveltaa uusinta tietoutta vaihtuvissa ympäristöissä ja tilanteissa. Virheiden sattuessa omatunto ohjaa toimimaan oikein niiden korjaamiseksi. (Karhumäki, Jonsson & Saros 2016.) Aseptisen omatunnon tavoin yksilöllä tulisi olla kestävä kyberturvallinen omatunto. Yksilöllä tulisi olla sisäistetty kyberturvallinen toimintatapa, jonka pohjalta yksilö navigoi verkottuneessa toimintaympäristössä. Yksilöllä tulisi olla riittävästi kyberturvallisuuden perusosaamista, ajankohtaista tietoutta sekä kykyä soveltaa niitä omassa toimintaympäristössä. Yksilön tulisi myös osata ja ymmärtää reagoida asianmukaisesti, kun kohtaa kyberuhkia tai kun ne ovat realisoituneet kyberhäiriöksi.

7.1.2 Organisaatio kyberturvallisuutta lisäävänä tekijänä

Tämän opinnäytetyön tuloksista kävi ilmi organisaation merkittävä rooli kyberturvallisuutta lisäävänä osapuolena. Tällä tarkoitetaan sitä, että yksilön lisäksi organisaatiolla on valtava vastuu kyberturvallisuuden toteutumisessa. Organisaation tulee panostuksellaan luoda asianmukaiset edellytykset, jotta kyberturvallisuus mahdollistetaan riittävällä laajuudella. Organisaatioiden tulee olla valmiita investoimaan työntekijöiden osaamisen kehittämiseen kyberturvallisuus monipuolisesti huomioiden (Jerry-Egemba 2023). Opinnäytetyö korostaa, että kyberturvallisuus on dynaaminen prosessi, joka vaatii jatkuvaa panostusta ja kehittämistä, jotta organisaatiot pysyvät ajan tasalla ja valmiina kohtaamaan uusimmat kyberuhkat.

Organisaation riittävän panostuksen lisäksi, sillä tulee olla selkeät ja ajankohtaiset kyberturvallisuuskäytänteet, jotka ovat elintärkeitä organisaation kokonaisturvallisuuden kannalta. Organisaation on varmistettava, että tietoturvakäytänteet ovat kaikkien tiedossa ja noudatettuja, jotta niistä saadaan haluttu hyöty. Selkeät ohjeet ja toimintamallit auttavat työntekijöitä ymmärtämään rooliaan kyberturvallisuuden varmistamisessa ja organisaatio voi tukea heitä tässä merkittävästi. Organisaation tuki on erityisen tärkeää, sillä kyberuhkat kehittyvät jatkuvasti, mikä edellyttää ammattilaisilta ajan tasalla pysymistä sekä uusien uhkien että niiden torjuntakeinojen osalta.

Kyberturvallisuuden tulee olla integroitu osaksi kokonaisturvallisuutta ja laatutyötä. Kyberturvallisuus ei ole erillinen osa, vaan se on keskeistä organisaation kokonaisvaltaisessa turvallisuusstrategiassa. Tämä lähestymistapa auttaa varmistamaan, että henkilöstö näkee kyberturvallisuuden tärkeänä osana koko organisaation toiminnan laatua ja turvallisuutta.

7.2 Täydennyskoulutus lisää kyberturvallisuutta

Tässä opinnäytetyössä selvitettiin sosiaali- ja terveysalan ammattilaisille suunnatun kyberturvallisuutta käsittelevän täydennyskoulutuksen osallistujien arvioita siitä, miten täydennyskoulutus on vaikuttanut osallistujien kyberturvallisuusosaamiseen. Saadun tiedon avulla voidaan pohtia koulutuksen vaikuttavuutta ja merkittävyyttä.

Täydennyskoulutuksen vaikutuksia tarkasteltaessa tunnistettiin kolme kokonaisuutta, jotka ovat *kyberturvallisuuden perusosaaminen ja soveltaminen työympäristöön*, *organisaation ja työntekijän rooli kyberturvallisuudessa* sekä *kyberturvallisuuden dynaamisuus*. Kyberturvallisuutta lisäävien tekijöiden tapaan myös tähän haluttiin tuoda uutta aspektia kvantifioimalla saadut yhdistävät luokat.

Täydennyskoulutuksen vaikutuksesta kyberturvallisuusosaamiseen saatiin näkökulmia vain yhden avoimen kysymyksen perusteella. Luonnollisesti tämän takia havaintojen määrä on kokonaisuudessaan selkeästi pienempi kuin kyberturvallisuutta lisäävissä tekijöissä, joissa näkökulmia saatiin kahdesta avoimesta kysymyksestä. Täydennyskoulutus vaikutti eniten kyberturvallisuuden perusosaamiseen ja soveltamiseen työympäristössä. Toiseksi eniten täydennyskoulutuksen koettiin vaikuttavan ymmärrykseen organisaation ja työntekijän rooleista kyberturvallisuudessa. Kyberturvallisuuden dynaamisuuden ymmärrykseen täydennyskoulutus vaikutti kolmanneksi.

Perusosaamiseen ja sen soveltamiseen liittyviä havaintoja oli selkeästi eniten. Tämä oli linjassa vastaajien näkemysten kanssa tarkastellessa kyberturvallisuutta lisääviä tekijöitä, jossa osaamiseen liittyviä tekijöitä havaittiin eniten. Organisaation ja työntekijöiden rooleihin liittyviä havaintoja oli noin puolet vähemmän ja kyberturvallisuuden dynaamisuus esiintyi vähiten, mutta merkittävästi kokonaisuutta ajatellen.

Alla olevassa kuvassa (kuvio 8) havainnollistetaan, kuinka usein kukin kyberturvallisuuden osa-alue on mainittu aineistossa.

Kuvio 8. Kyberturvallisuusosaamiseen liittyvien havaintojen esiintymistiheys aineistossa.

Kyberturvallisuuden perusosaaminen ja soveltaminen työympäristöön oli yleisimmin esiintynyt teema, mikä osoittaa, että täydennyskoulutuksella on suurin vaikutus perusosaamisen kehittämiseen ja sen soveltamiseen työssä. Tietoutta on siis jalostettu ja sovellettu käytännön tilanteisiin. Tällainen syvempi ymmärrys on osoitus osaamisen kehittymisestä täydennyskoulutuksen aikana. Asianmukainen koulutus onkin tutkitusti vaikuttavin tapa kehittää kyberturvallisuusosaamista (Kruse ym. 2017). Aiempien tutkimusten mukaan kyberturvallisuuden kehittämisessä on pyritty siirtymään ennaltaehkäisevään ja ennakoivaan ajattelutapaan. Tällöin kyberturvallisuutta tarkastellaan riskienhallinnan ja kyberresilienssin kautta. Tämän lähestymistavan tavoitteena on tunnistaa, lieventää, välttää ja hyväksyä riskejä. (Argaw ym. 2020.) Tämän ajattelutavan ja toiminnan saavuttamiseksi on äärimmäisen tärkeää, että täydennyskoulutus lisää perusosaamista, antaa valmiuksia syventää osaamista sekä lisää kykyä soveltaa osaamista käytäntöön. Täydennyskoulutuksella saavutettu osaaminen kyberturvallisuuden käsitteistä, kyberuhkien tunnistamisesta ja niiden hallinnasta, laitteista ja järjestelmistä sekä tietoturvasta ja tietosuojasta, ovat perusta sille, että osaamista pystytään syventämään. Lehto (2023) toteaa artikkelissaan, että kybertoimintaympäris-

tön haavoittuvuuteen voi vaikuttaa henkilöstön osaamattomuus tai tietämättömyys kyberturvallisista toimintatavoista (Lehto 2023). Siksi onkin tärkeää, että oikeanlaisen koulutuksen avulla voidaan poistaa kaikki mahdolliset kyberuhkia lisäävät tekijät.

Organisaation ja työntekijän rooli kyberturvallisuudessa korostaa yhteistä vastuuta organisaation ja yksilön välillä. Koska sosiaali- ja terveysala kohtaa yhä enemmän erilaisia uhkatekijöitä, tarvitaan muutosta kyberturvallisempaan suuntaan. Sen toteutukseen tarvitaan muutosta kokonaisvaltaisesti niin yksilön käyttäytymiseen, teknologian ja prosessien kehittämiseen kuin myös yleiseen kyberturvallisuuskulttuuriin. Muutostavoite koskettaa organisaation kaikkia toimijoita. (Coventry & Branley 2018.) Tutkimusten mukaan sosiaali- ja terveydenhuollon organisaatioihin kohdistuu yleisimmin kyberuhkia tietotekniikan sekä yksilön toiminnasta johtuvien haavoittuvuuksien takia (Nifakos ym. 2021; Coventry & Branley 2018). Siksi onkin tärkeää, että organisaation ja yksilön tavoitteet ja tehtävät kyberturvallisuuden lisäämiseksi ovat molemmilla osapuolilla tiedossa ja hyödynnettävissä. Myös opinnäytetyön tulosten perusteella korostui se, että kyberturvallisuudessa on tärkeää ymmärtää molempien osapuolten vastuut ja roolit turvallisuuden varmistamisessa. Useat vastaajat toivat esiin henkilöstön ja työnantajan roolin kyberturvallisuuden toteutumisessa. Tämä heijastaa koulutuksen merkitystä paitsi yksilön oppimisessa myös organisaation laajemmassa kokonaisturvallisuudessa. Täydennyskoulutus on edistänyt ymmärrystä kyberturvallisuuden yhteisvastuullisesta luonteesta ja korostanut jokaisen työntekijän merkitystä. Tämä osoittaa, että täydennyskoulutuksen avulla osallistujat ovat saaneet laajemman ymmärryksen siitä, miten organisaatiotasolla voidaan vaikuttaa muun muassa kyberuhkien hallintaan.

Kolmantena teemana havaittu kyberturvallisuuden dynaamisuus ilmeni vähiten, mutta sen merkitys ei ole kuitenkaan vähäpätöinen ja se nousi kuitenkin selkeäksi omaksi kokonaisuudeksi. Dynaamisuus viittaa siihen, että kyberturvallisuus on jatkuvasti kehittyvä prosessi, jossa sekä organisaation että henkilöstön on pysyttävä ajan tasalla uusista uhkista ja muutoksista. Se viittaa sellaiseen osaamiseen, joka on muuttuvaa, kehittyvää ja aktiivista. Se kuvaa prosessia, jossa kyberturvallisuusosaaminen ei ole staattista, vaan jatkuvasti kehittyvää ja reagoivaa uusiin uhkiin, haavoittuvuuksiin ja teknologisiin muutoksiin. Dynaamisuus kyberturvallisuuden kontekstissa vaatii panostusta ja tahtoa niin yksilöltä kuin organisaatiolta. Cartwright (2023) korostaa artikkelissaan, että sosiaali- ja terveysalalla on erityisen tärkeää kiinnittää huomiota siihen, että kyberturvallisuutta

lisääviä toimia tehostetaan yhä enemmän. Hän korostaa koulutuksen jatkuvuutta ja säännöllisyyttä, koska uusia uhkia ja riskitekijöitä ilmenee jatkuvasti. (Cartwright 2023.) Myös Jerry-Egemba (2023) tähdentää sosiaali- ja terveysalan ammattilaisten valmiuksien ylläpitämistä ja kehittämistä alati muuttuvassa kybertoimintaympäristössä (Jerry-Egemba 2023).

Saadut tulokset osoittavat, että kyberturvallisuuden parantaminen täydennyskoulutuksen kautta vaatii monipuolista lähestymistapaa. Koulutuksen tulee kattaa henkilöstön osaamisen kehittäminen, selkeät käytänteet, järjestelmien ylläpito, riittävä resursointi ja tietoisuus kyberuhkista. Näiden tekijöiden tehokas yhdistäminen auttaa organisaatioita parantamaan kyberturvallisuutta ja suojaamaan potilastietoja tehokkaasti. Jerry-Egemba (2023) korostaa artikkelissaan, että koulutusten kehittäminen on tärkeää uusien uhkien ja riskien huomioimiseksi, ajantasaisten toimintatapojen sisäistämiseksi sekä parhaiden käytäntöjen hyödyntämiseksi (Jerry-Egemba 2023).

Kokonaisuudessaan opinnäytetyö osoittaa, että kyberturvallisuuden lisääminen sosiaali- ja terveysalalla edellyttää systemaattista koulutusta, organisaation tukea ja henkilöstön aktiivista roolia. Nämä tekijät yhdessä luovat vahvan pohjan kyberturvallisuudelle ja varmistavat potilastietojen ja -järjestelmien turvallisuuden. Koulutuksen ja osaamisen kehittämisen jatkuvuus on erityisen tärkeää muuttuvassa kyberuhkien kentässä. Opinnäytetyön tulokset osoittavat, että kyberturvallisuus on monitahoinen haaste, joka vaatii sitoutumista ja jatkuvaa kehittämistä. Koulutuksen merkitys on myös korostunut, sillä se tarjoaa ammattilaisille tarvittavat valmiudet tunnistaa erilaisia kyberuhkia ja kykyä reagoida niiden tuomiin haasteisiin.

7.3 Tutkimuksen luotettavuus

Tutkimuksen luotettavuuden pohdinta kuuluu olennaisena osana opinnäytetyön kokonaisuuden arviointiin. Laadullisen tutkimuksen luotettavuuden arviointiin ei ole olemassa tiettyä ohjetta tai kriteeristöä (Tuomi &Sarajärvi 2018). Sen sijaan arvioinnin kohteena ovat erityisesti tutkijan tekemät valinnat, tulkinnat ja johtopäätökset. Luotettavuuden arviointia tapahtuu siis koko ajan, joten merkittävää on se, miten hyvin tutkija on pystynyt avaamaan tutkimuksen etenemistä ja tekemiään ratkaisuja. (Vilkka 2015.) Hirsjärvi ym. (2009) toteavat, että laadullisessa tutkimuksessa on tärkeä huomioida nimenomaan laadullisen tutkimuksen luonne. Tällä tarkoitetaan esimerkiksi sitä, että tuloksia ei esitetä kritiikittömästi eikä niitä sepitetä tai kaunistella. Joskus tämä tarkoittaa sitä,

että myös tutkimuksen puutteet tai tuloksiin pääsemättömyys on kerrottava avoimesti. (Hirsjärvi ym. 2009.)

Laadullisen tutkimuksen luotettavuudella tarkoitetaan sitä, että työssä kuvailtu tutkimusprosessi avaa tutkimuksen etenemistä ja päätöksentekoa uskottavasti ja, että niiden perusteella on saatu luotettavaa tietoa tutkittavasta asiasta. Saatujen tutkimustulosten tulisi siis ilmaista mahdollisimman totuudellisesti tutkittavaa ilmiötä. Luotettavuusnäkökulma alkaa jo niistä perusteluista, kun päätetään aineiston hankinnasta ja se jatkuu läpi koko tutkimuksen. Tutkijan pitää osata perustella kaikki valinnat, mitä on tehnyt tutkimuksen edetessä. (Hakala 2024.) Tässä tutkimuksessa tämä on näkynyt esimerkiksi siinä, että prosessin eteneminen on kuvattu tarkasti ja tehdyt päätökset on dokumentoitu systemaattisesti. Tämä varmistaa, että tutkimuksen tulokset kuvastavat mahdollisimman totuudellisesti osallistujien näkemyksiä kyberturvallisuudesta.

Tuomi ja Sarajärvi (2018) ovat avanneet luotettavuuden arviointia tutkimuksen eri osa-alueiden kautta. Osa-alueet käsittävät muun muassa tutkimuksen kohteen ja tarkoituksen, aineiston keruun ja analyysin sekä eettisyyden ja raportoinnin. Tutkimuksen luotettavuutta tulisi kuitenkin arvioida kokonaisuutena ei pelkkinä osa-alueina. Tällöin arvioidaan sitä, miten tutkimuksen sisäinen johdonmukaisuus (koherenssi) toteutuu eri osa-alueissa ja niiden välillä. (Tuomi & Sarajärvi 2018.)

Tämän tutkimuksen raportoinnissa on panostettu selkeyteen ja systemaattisuuteen. Esitetyt asiat on haluttu esittää siten ja siinä järjestyksessä, kun ne on toteutuneet. Tutkimuksen eri osa-alueet muodostavat kokonaisuuden, jossa sisäinen johdonmukaisuus (koherenssi) toteutuu. Tämän ansiosta tutkimuksen prosessi ja tulokset ilmenevät uskottavasti ja todenmukaisesti. Tutkimuksen aihe, tarkoitus ja tavoitteet on sidottu tähän hetkeen ja aiheen ajankohtaisuus ja tarpeellisuus on ilmeistä. Aineiston käsittelyssä ja koko tutkimuksessa on myös huomioitu eettiset näkökulmat sekä hyvän tieteellisen käytännön menettelytavat. Raportoinnissa tutkimusprosessi sekä tutkimustulokset on kuvattu loogisesti ja tarkasti, jotta lukijalle on annettu riittävästi tietoa tutkimuksen tulosten arvioimista varten (Tuomi & Sarajärvi 2018). Kaikki nämä edellä mainitut seikat vahvistavat tutkimuksen luotettavuutta.

Laadullisen tutkimuksen luotettavuus kiteytyy usein nimenomaan tutkimusprosessin luotettavuuteen; miten tarkasti perustellen ja läpinäkyvästi tutkija on kuvaillut prosessin etenemisen (Eskola &

Suoranta 1998). Lukija tulisi ikään kuin saada mukaan siihen samaan prosessiin ja matkaan, mitä tutkijakin on kulkenut. Lukija pystyy tällöin ymmärtämään ilmiötä ja tutkimuksen kokonaisuutta paremmin sekä tällöin pystytään arvioimaan niin prosessin kuin päätelmien uskottavuutta ja luotettavuutta. (Puusa & Juuti 2020.)

Laadullisen tutkimuksen luotettavuutta lisää siis se, että tutkimuksen eri vaiheet on raportoitu selkeästi ja läpinäkyvästi. Luotettavuuden lisäämiseksi tulisi myös pohtia ja perustella, miksi on päädytty tiettyihin ratkaisuihin tai tulkintoihin esimerkiksi sisällönanalyysia tehdessä. (Elo ym. 2022; Hirsjärvi ym. 2009.) Tässä opinnäytetyössä läpinäkyvyys ja perusteltavuus ovat läsnä erityisesti aineistonkeruun, aineiston analyysin ja tutkimuksen raportoinnin aikana. Työssä on dokumentoitu analyysin vaiheet huolellisesti, jotta lukija voi ymmärtää, miksi on päädytty esimerkiksi tiettyihin tulkintoihin yhdistävistä teemoista analysoidessa kyberturvallisuutta lisääviä tekijöitä. Tämä lisää tutkimuksen luotettavuutta, sillä lukijalle tarjotaan mahdollisuus seurata ja arvioida analyysin etenemistä.

Laadullisen tutkimuksen luotettavuutta on kyseenalaistettu muun muassa aineiston käsittelyn moninaisuuden takia (Puusa & Juuti 2020) sekä siksi, että luotettavuuden käsitystä ei ole voitu määritellä yksiselitteisesti (Tuomi & Sarajärvi 2018). Standardoituja analyysitapoja on vain vähän eikä yksiselitteisiä ohjeita ole voitu tehdä. Luotettavuutta lisää tutkimuksen systemaattisuus, avoimuus, tarkistettavuus sekä perusteltavuus. (Puusa & Juuti 2020.) Viimeisin mainittu on ehkä kaikista tärkein, johon tutkija voi vaikuttaa tarkalla dokumentaatiolla ja prosessimaisella tutkimusotteella koko tutkimuksen ajan. Tässä opinnäytetyössä on pyritty selvittämään kaikki tutkimuksen vaiheet mahdollisimman avoimesti ja yksiselitteisesti, jotta luotettavuuden periaatteet toteutuvat.

7.4 Tutkimuksen eettisyys

Kaikissa tutkimuksissa on tärkeää noudattaa hyvän tieteellisen käytännön mukaisia menettelytapoja koko tutkimuksen ajan. Ohjenuorana voidaan pitää tekemisen luotettavuutta, rehellisyyttä, arvostusta ja vastuullisuutta. Ne antavat tukevan raamin laadukkaalle kehittämistyölle. (Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2023; Tuomi & Sarajärvi 2018.)

Tutkimusten eettisiä kysymyksiä ja tutkimusetiikan edistämistä ohjaa Opetus- ja kulttuuriministeriön asettama Tutkimuseettinen neuvottelukunta (TENK). Sen toiminta rakentuu vahvasti yhteistyölle suomalaisen tiede- ja tutkimusyhteisön kanssa. Jokaisessa tutkimuksessa tulee ottaa huomioon myös tutkimuksen aihepiirin mukaisesti kohdennetut tutkimuseettiset toimielimet. Tässä opinnäytetyössä on siten huomioitava myös valtakunnallisen sosiaali- ja terveysalan eettisen neuvottelukunnan (ETENE) ohjeistukset ja huomiot. (Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa 2023.)

Tämän opinnäytetyön näkökulma on sosiaali- ja terveydenhuollon ammattilaisten näkemykset kyberturvallisuuteen liittyvistä seikoista. Perimmiltään kyse on ammattilaisten kyvykkyydestä tehdä työtään laadukkaasti alati muuttuvissa toimintaympäristöissä. Tämä liittyy vahvasti ETENE:n eettisiin suosituksiin koskien niin ammattihenkilöstön toiminnan laatua kokonaisuudessaan kuin vastuullista toimintaa ja toimintakulttuuria. Sosiaali- ja terveysalan ammattilaisten tulee osata toimia laadukkaasti ja eettisesti kestävästi niin suorassa kontaktissa kohteen (esim. asiakas tai potilas) kanssa kuin myös vaikkapa kybertoimintaympäristössä, kuten tässä opinnäytetyössä. (Sosiaali- ja terveysalan eettinen perusta 2011.)

Tutkimuksessa on lisäksi otettava huomioon organisaation omat eettiset ohjeet eli tässä työssä JAMK:n eettiset periaatteet. Nämä periaatteet perustuvat vahvasti TENK:n ohjeisiin sekä lisäksi ammattikorkeakoululakiin ja JAMK:n tutkintosääntöön. Eettiset periaatteet ohjaavat muun muassa toimimaan puolueettomasti ja totuudellisesti. Tässä opinnäytetyössä tekijä on sitoutunut alusta asti toimimaan JAMK:n eettisten periaatteiden mukaisesti. Tämä näkyy muun muassa siinä, että läpi koko opinnäytetyöprosessin toimintaa ohjaa hyvän tieteellisen käytännön periaatteet, kuten vastuullisuus, luotettavuus ja rehellisyys. Opinnäytetyössä ei myöskään tehdä vilppiä missään muodossa. Kaikki tekeminen on läpinäkyvää, toistettavaa ja perusteltua. (Jyväskylän ammattikorkeakoulun eettiset periaatteet 2024.)

Laadullisen tutkimuksen tutkimusetiikkaan voidaan suhtautua monin eri tavoin. Kaikkea Suomessa tehtyä tutkimusta verhoaa TENK:n periaatteet, jotka korostavat tutkimuksen rehellisyyttä ja rehtiyttä. Tutkimusetiikka saatetaan jossain tapauksissa ymmärtää ikään kuin teknisenä suorittamisena, jossa huolehditaan esimerkiksi tutkimuksen kohteena olevien informoimisesta, anonymiteetistä,

aineiston analyysin luotettavuudesta eli kaikista tutkijan käyttämien keinojen eettisistä ratkaisuista. Toisaalta tutkimusetiikka voi olla metodologinen seikka, jolloin tutkimuksen suunnittelussa, toteutuksessa ja tulosten analysoinnissa otetaan huomioon eettiset kysymykset. Tällöin yhtenä keskeisenä tutkimusta ohjaavana seikkana on eettiset valinnat kaikissa tutkimuksen vaiheissa eikä eettisyyttä nähdä ikään kuin erillisenä osana. Laadullisen tutkimuksen eettinen kestävyys on osa tutkimuksen laatua. Tällä tarkoitetaan niin tutkimuksen eettistä johdonmukaisuutta kuin tutkijan tapaa toimia eettisten periaatteiden mukaisesti. (Tuomi & Sarajärvi 2018.)

Tässä opinnäytetyössä selvitettiin täydennyskoulutukseen osallistuvien sosiaali- ja terveysalan ammattilaisten näkökulmia kyberturvallisuudesta. Täydennyskoulutus on osa laajempaa hanketta, jonka puitteissa sen järjestäjällä eli JAMK:lla on tutkimuslupa koulutukseen liittyvien tiettyjen osa-alueiden käyttämisestä tutkimuskäyttöön. Täydennyskoulutukseen osallistujilta kysyttiin hankkeen tutkimusluvan lisäksi vielä erikseen suostumusta viimeisen tehtävän reflektio-osuuden avointen kysymysten käyttöön aineistona juuri tässä opinnäytetyössä. Osallistujilla oli mahdollisuus hyväksyä tai hylätä pyyntö osallistumisesta opinnäytetyöhän. Suostumuspyyntölomake laadittiin Webropol-sovellukseen ja linkki saatekirjeineen lähetettiin kaikille osallistujille sähköpostilla opintojakson vastuuopettajien toimesta.

Yksi tärkeimmistä tutkimuseettisistä normeista on tunnistettavuuden estäminen. Tällä tarkoitetaan kaikkien tunnisteiden poistamista tai muuttamista aineistosta eli anonymisointia. Kuitenkin on tärkeä ymmärtää tutkimuksen aineiston ja julkaisun anonymisoinnin ero. Jossain tapauksissa aineistossa on perusteltua säilyttää tunnistetietoja, vaikka julkaisussa niitä ei enää ole näkyvissä. Oleellista on, että jos aineisto kerätään suoraan tutkittavilta, anonymisointiratkaisuihin vaikuttaa tutkittaville annettu tieto aineiston käsittelystä ja sen käytöstä. (Kuula 2011.) Tässä opinnäytetyössä ei ollut merkittävää se, että tutkijalla olisi ollut käytössä tunnisteellinen aineisto. Tämän takia kysyttäessä lupaa opiskelijoilta avointen kysymysten käyttämisestä tässä opinnäytetyössä painotettiin aineiston anonymisointia.

Myönteisen vastauksen antaneiden opiskelijoiden reflektiotehtävän vastaukset anonymisoitiin vastuuopettajien toimesta. Vastauksista siis poistettiin kaikki se tieto, mikä voisi paljastaa jotain vastaajasta tai vaikkapa työskentelyorganisaatiosta (Kuula 2011). Anonymisoinnin jälkeen vastauk-

set lähetettiin tutkijalle sähköpostitse word-tiedostona analysoitavaksi opinnäytetyötä varten. Aineisto säilytetään salasanakoodattuna tietokoneen kovalevyn kansiossa, jossa on ajantasainen suojausohjelmisto. Tämän lisäksi aineiston varmuuskopio on tallennettu erilliselle muistitikulle. Kovalevyn kansioon ei ole pääsyä ulkopuolisilla ja muistitikku säilytetään paloturvallisessa lukitussa kaapissa. JAMK:n opinnäytetyöohjeiden mukaisesti aineistoa säilytetään kaksi vuotta, jonka jälkeen se tuhotaan lopullisesti (Liukko & Perttula 2024).

Laadukasta tutkimusta ohjaa siis eettinen sitoutuneisuus. Laadukkaasti toteutettu eettinen aspekti tulee kulkea mukana koko tutkimuksen ajan. Myös tässä opinnäytetyössä on pyritty huolehtimaan eettisestä pohdinnasta alusta loppuun. Eettisyys näkyi opinnäytetyössä muun muassa osallistumisen vapaaehtoisuutena ja aineiston anonymiteetin säilyttämisenä. Aineistoa myös käsiteltiin ja analysoitiin siten, ettei havaintoja vääristelty tai muunneltu, vaan ne esitettiin rehellisesti. Lisäksi tulokset esitettiin totuudenmukaisesti ja läpinäkyvästi. Kokonaisuudessaan opinnäytetyö tehtiin vastuullisesti ja eettisten periaatteiden mukaisesti.

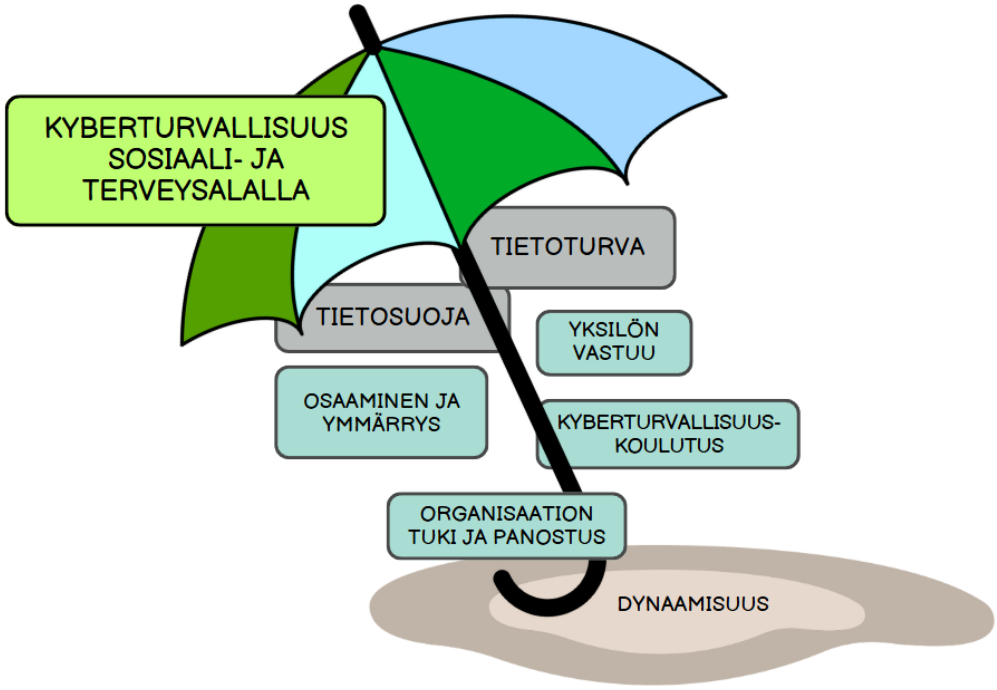
7.5 Johtopäätökset

Kyberturvallisuus on aiheena ajankohtainen, jättiläismäinen, dynaaminen, merkityksellinen ja ennen kaikkea kaikkia koskettava teema. Aiheesta käydään dialogia jatkuvasti ja globaalisti. Tutkimuksia ja erilaisia kirjoituksia laaditaan kiihtyvällä tahdilla, koska tietoa tulee koko ajan lisää ja se kehittyy jatkuvasti. Sosiaali- ja terveysalan asiakasrajapinnassa toimivien ammattilaisten näkökulmasta kyberturvallisuuteen on herätty vasta viime vuosina. Aiemmin on puhuttu lähinnä tietoturvasta ja -suojasta, mutta onneksi aihepiiriä on laajennettu kyberturvallisuuden suuntaan. (McLeod & Dolezel 2018; Kruse ym. 2017.) Kyberturvallisuus käsittää digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuuden sekä näiden toimintoihin kohdistuvat riskit. Siihen sisältyy erilaisia toimenpiteitä, joiden tavoitteena on ennakoida, hallita ja tarvittaessa kestää kyberuhkia ja niiden seurauksia. (Kyberturvallisuuden sanasto 2018.)

Tämän opinnäytetyön perusteella on selvää, että kyberturvallisuuden parantaminen sosiaali- ja terveysalalla vaatii monipuolista lähestymistapaa, jossa yhdistyvät henkilöstön osaamisen kehittäminen, organisaation rooli, yksilön vastuu ja tietoisuuden lisääminen. Laadukkaan ja kohdennetun kyberturvallisuuskoulutuksen rooli on myös keskeistä ja sen tulee kattaa kyberturvallisuus kaikilla tasoilla ja työtehtävissä.

Tietoturvaan ja -suojaan liittyvät asiat ovat yleisesti jo aiemmin mielletty osaksi sosiaali- ja terveysalan kyberturvallisuutta. Yksinkertaistettuna kyberturvallisuus kattaa tietoturvan ja tietoturvaan sisältyy tietosuojan varmistaminen. (Järvinen 2018; Lönnqvist & Moilanen 2017; Tepa-termipankki n.d; Suomen kyberturvallisuusstrategia 2013.) Tietoturvaan ja -suojaan liittyvät asiat pitäisi olla itsestäänselvyyksiä jokaiselle sosiaali- ja terveysalan ammattilaisille. Heidän tietoturvallista toimintaansa säätää muun muassa Euroopan unionin yleinen tietosuoja-asetus sekä useat lait, esimerkiksi tietosuojalaki ja laki potilaan asemasta ja oikeuksista (Potilas- ja asiakastietojen ja henkilötietojen käsittely n.d). Myös laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (L784/2021) säätelee asiakastietojen tietoturvallista käsittelyä. Sen tavoitteena on huolehtia tiedon saatavuudesta ja käytettävyydestä sekä varmistettava, että tiedot pysyvät eheinä ja muuttumattomina niiden säilytysajan. Organisaatioilla tulee myös olla tietoturvasuunnitelma, jossa selvennetään, miten tietosuojan piirissä olevia tietoja käsitellään ja varmistetaan tietoturvan toteutuminen. (L784/2021.) Tietoturvan ja -suojan tulisi siis olla osa sosiaali- ja terveysalan ammattilaisen substanssiosaamista jo lain puitteissa, jota sitten täydentää organisaatioiden tietoturvasuunnitelmat, toimintamallit ja ohjeistukset.

Tämän opinnäytetyön myötä kyberturvallisuuden näkökulmaa laajennettiin tietoturvan ja -suojan lisäksi vastaamaan saatuja tuloksia ja koottiin kyberturvallisuuden sateenvarjo (kuvio 9).



Kuvio 9. Kyberturvallisuuden sateenvarjo.

Kyberturvallisuuden sateenvarjo haluttiin luoda tähän opinnäytetyöhön havainnollistamaan kyberturvallisuuden monipuolisuutta ja korostamaan merkittävimpiä tuloksia. Se kattaa siis tietoturvan ja -suojan lisäksi tästä opinnäytetyöstä saadut keskeiset tulokset. Tietoturvaan ja -suojaan liittyvät asiat on kuvattu sateenvarjon alla osana jokaisen sosiaali- ja terveysalan ammattilaisen substanssiosaamista. Ne näyttäytyvät kuvassa (kuvio 9) sateenvarjon alla harmaana ja stabiilina. Sillä ei kuitenkaan tarkoiteta, että niiden sisältämä tieto olisi muuttumatonta vaan, että ne muodostavat ikään kuin perustan, jota ohjataan jo laillakin. Tämän tutkimuksen myötä tuota ajattelutapaa halutaan laajentaa ja kohdentaa koskemaan kyberturvallisuutta monipuolisemmin ja sis lisätä siihen tutkimuksen tuloksista nousseet tärkeimmät asiat.

Tärkeimmiksi nousseet teemat koskevat yksilön kyberturvallisuusosaamista ja ymmärrystä, adekvaattia osaamista kehittävää koulutusta, yksilön vastuullista kyberturvallista toimintaa sekä organisaation tukea ja riittävää panostusta kyberturvallisuuden mahdollistamiseksi. Nämä asiat on kuvattu kuvassa (kuvio 9) sinivihreänä, vielä hieman uutena, mutta tärkeäksi nousevana osana kokonaisuutta. Kuvion sateenvarjo symboloi kyberturvallisuuden laaja-alaista roolia sosiaali- ja terveysalalla, jossa perustavanlaatuiset tietoturva- ja tietosuojakäytännöt täydentyvät uusilla painopisteillä. Näiden uusien painopisteiden tavoitteena on rakentaa entistä kattavampaa ja dynaamisempaa lähestymistapaa kyberturvallisuuteen, joka huomioi sekä yksilön että organisaation vastuun ja roolin. Opinnäytetyössä ilmenee, että kyberturvallisuuden dynaamisuus kytkeytyy jollakin tavalla lähes kaikkeen. Se näkyy tuloksissa vahvimmin kyberturvallisuuden ajankohtaisuutena ja jatkuvassa muutoksessa olevana. Kuvassa (kuvio 9) dynaamisuus on kuvattu laajalle levinneenä varjona, joka ulottuu kaikkiin kyberturvallisuuden osa-alueisiin.

Kaikkia opinnäytetyöstä saatuja päätelmiä verhoaa siis jollakin tavalla kyberturvallisuuden dynaamisuus. Se ei viittaa ainoastaan teknologian jatkuvaan kehitykseen, vaan myös siihen, miten organisaatiot ja yksilöt mukautuvat uusiin uhkiin, muutoksiin ja tarpeisiin. Kyberturvallisuus on prosessi, joka vaatii jatkuvaa osaamisen kehittämistä, päivittämistä ja kykyä ennakoida tulevia riskejä. Opinnäytetyön tulosten mukaan tämä dynaamisuus näkyy sekä yksilön toiminnassa että organisaation kyberturvallisuuskulttuurissa.

Yksilöiden osalta dynaamisuus ilmeni tarpeena päivittää osaamista säännöllisesti ja mukautua työympäristön muuttuviin vaatimuksiin. Tämä näkyi esimerkiksi siinä, että täydennyskoulutuksen

osallistujat ymmärsivät kyberturvallisuuden olevan tärkeä teema ja, että se on jatkuvasti kehittyvä osaamisalue. Siinä pitää hallita perusteet sekä on oltava valmius soveltaa opittua omaan toimintaympäristöön. Tämä liittyy vahvasti myös yksilön vastuulliseen toimintaan. Jokainen on itse vastuussa siitä, toimiiko kyberturvallisesti vai ei. Vastuullisen toimijan tulee olla valmis muutoksiin ja muuttamaan toimintaansa tilanteen mukaan.

Organisaation tasolla dynaamisuus korostui siinä, että organisaatioiden on kyettävä reagoimaan teknologian ja toimintaympäristön muutoksiin. Se tarkoittaa investointeja osaamisen kehittämiseen, selkeisiin ohjeistuksiin ja teknologisiin ratkaisuihin. Tämä on jatkuva prosessi, jossa organisaation tulee aktiivisesti tukea henkilöstön osaamisen kehittymistä ja panostuksellaan mahdollistaa kyberturvallisuuden toteutumisen.

Kyberturvallisuuden dynaamisuus on keskeinen lähtökohta kaikelle toiminnalle. Se vaatii sekä ammattilaisia että organisaatioita sitoutumaan jatkuvaan kehitykseen ja proaktiiviseen asenteeseen kyberturvallisuuden ylläpitämisessä. Tarvitaan siis ennakoivaa otetta, yhteistyötä ja valmiutta sopeutua muuttuviin haasteisiin, jotta voidaan varmistaa turvallinen kybertoimintaympäristö sosiaali- ja terveysalalla.

7.6 Kehittämisehdotukset

Opinnäytetyötä tehdessä havaittiin, että useiden tutkimusten mukaan tehokkain ja vaikuttavin tapa lisätä kyberturvallisuutta on asianmukainen koulutus. Myös opinnäytetyön tulokset korostavat osaamisen, ymmärryksen ja koulutuksen merkittävyyttä kyberturvallisuutta lisäävinä tekijöinä. Erilaisia täydennyskoulutuksia on kuitenkin melko vähän tarjolla suhteessa aiheen laajuuteen ja merkitykseen kokonaisturvallisuuden kannalta.

Jatkotutkimusaiheena olisi mielenkiintoista kehittää sosiaali- ja terveysalan organisaatiolle kohdennettua ja juuri johonkin tiettyyn organisaatioon räätälöityä koulutusta. Koulutus sisältäisi muun muassa perusosaamiseen liittyviä osa-alueita, osaamisen soveltamista työympäristöön sekä erityisesti simuloituja kyberturvallisuuden harjoituksia. Näihin simuloituihin harjoituksiin voisi sisältyä esimerkiksi kalastelusähköpostien tunnistaminen ja tietoturvapoikkeamatilanteiden ratkaiseminen, jotka tarjoavat realistisen ja käytännönläheisen tavan arvioida työntekijöiden kyberturvallisuusosaamista.

Simulaatioharjoitukset eivät mittaisi ainoastaan teknisiä taitoja, vaan myös työntekijöiden käyttäytymistä, kuten varovaisuutta, päätöksentekokykyä ja kykyä noudattaa ohjeita uusissa tilanteissa. Harjoitusten jälkeen annettava palaute olisi olennainen osa oppimisprosessia, sillä se vahvistaisi oikeita toimintatapoja ja tarjoaisi mahdollisuuden korjata virheellisiä toimintamalleja. Lisäksi simulaatioista saatua palautetta ja havaintoja osaamistarpeista voitaisiin hyödyntää koulutusohjelmien kehittämisessä ja räätälöinnissä tulevaisuudessa.

Koulutuksen vaikuttavuus edellyttäisi kuitenkin myös organisaation tukea ja sitoutumista jatkuvan oppimisen ajatusmalliin. Jatkuva oppiminen ja säännöllinen seuranta (esim. osaamista arvioiva mittari) voisivat varmistaa, että koulutus vastaa dynaamisen kyberturvallisuuden haasteisiin ja edistää myös organisaation kyberturvallisuutta ja resilienssiä. Koulutuksen kautta saavutettu yksilöiden lisääntynyt osaaminen ja kyberturvallisuustietoisuus heijastuisivat siis suoraan organisaation kokonaisturvallisuuteen, mikä tekisi koulutuksesta arvokkaan investoinnin.

Toisena kehittämisehdotuksena on kyberturvallisuuden sateenvarjon (kuvio 9) hyödyntäminen jatkotutkimuksen lähtökohtana. Voisi esimerkiksi pohtia, miten eri osa-alueet ilmenevät eri organisaatioissa tai eri ammattilaisryhmissä. Olisi myös kiinnostavaa tutkia miten organisaatiot voivat hyödyntää näitä elementtejä käytännössä ja miten ne vaikuttavat kyberturvallisuuteen. Tämä antaisi tarkempaa tietoa siitä, mikä osa-alue tarvitsee erityistä huomiota tai kehitystä.

Kuvan osa-alueisiin voisi myös syventyä vielä tarkemmin; miten ne liittyvät toisiinsa ja muodostavat kokonaisuuden. Tällöin pohdittaisiin sitä, miten eri osa-alueiden välinen yhteistyö ja vuorovaikutus voidaan optimoida, jotta niistä saataisiin paras hyöty. Jatkotutkimuksessa voisi myös tarkastella sitä, millaisia resursseja ja panostuksia organisaatiot tarvitsevat eri osa-alueiden tehokkaan hyödyntämisen varmistamiseksi. Voisi esimerkiksi mallintaa osa-alueittain mitä organisaatiolta vaaditaan, että jokaista elementtiä saadaan vahvistettua organisaation kyberturvallisuuskulttuurissa.

Lähteet

AlDaajeh, S., Saleous, H, Alrabaee, S., Barka, E., Breitinger, F. & Choo, K.-K. R. 2022. The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754. Viitattu 23.3.2024. https://janet.finna.fi, Science Direct (Elsevier).

Al-Qarni, E. A. 2023. Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. International Journal of Advanced Computer Science and Applications, 14, 5. https://janet.finna.fi, ProQuest.

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B. & Flahault, A. 2020. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20, 146. Viitattu 23.3.2024. https://janet.finna.fi, ProQuest.

Blek, T. & Solankallio-Vahteri, T. 2022. Information and cybersecurity competence of healthcare care personnel. Finnish Journal of EHealth and EWelfare, 14, 4, 352–363. Viitattu 6.11.2024. https://doi.org/10.23996/fjhw.115829.

Cartwright, A. 2023. The elephant in the room: Cybersecurity in healthcare. Journal of Monitoring and computing, 37, 1123–1132. Viitattu 6.11.2024. https://janet.finna.fi, Pubmed.

Coventry, L. & Branley, D. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. Viitattu 29.11.2024. https://janet.finna.fi, Science Direct (Elsevier).

Direktiivi 2022/2555/EU. Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi). Euroopan unionin virallinen lehti 27.12.2022. Viitattu 6.12.2024. https://eur-lex.europa.eu/eli/dir/2022/2555.

Elo, S., Kajula, O., Tohmola, A. & Kääriäinen, M. 2022. Laadullisen sisällönanalyysin vaiheet ja eteneminen. Hoitotiede, 34, 215–225. Viitattu 26.9.2024. https://janet.finna.fi, Cinahl.

Elo, S. & Kyngäs, H. 2008. The qualitative content analysis process. Journal of Advanced Nursing, 62, 107–115. Viitattu 26.9.2024. https://janet.finna.fi, Cinahl.

Eskola, J. 2018. Laadullisen tutkimuksen juhannustaiat. Laadullisen tutkimuksen analyysi vaihe vaiheelta. Kirjassa Aaltola, J & Valli, R. (toim.). Ikkunoita tutkimusmetodeihin 2. Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. Jyväskylä: PS-kustannus. Viitattu 25.9.2024. https://janet.finna.fi, Ellibslibrary.

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino. Viitattu 25.9.2024. https://janet.finna.fi, Ellibslibrary.

Hakala, J. T. 2024. Laadullisen tutkimuksen ABC: menetelmäopas opinnäytteen tekijälle. Helsinki: Gaudeamus. Viitattu 24.10.2024. https://janet.finna.fi, Ellibslibrary.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uud. p. Helsinki: Tammi.

Huhtinen, A.-M. & Tuominen, J. 2020. Fenomenologia. Ihmisten kokemukset tutkimuksen kohteena. Kirjassa Puusa, A. & Juuti, P. (toim.). 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus. Viitattu 26.9.2024. https://janet.finna.fi, Ellibslibrary.

Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. 2023. Helsinki: Tutkimuseettisen neuvottelukunnan julkaisuja 2/2023. Viitattu 17.10.2024. https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf.

Jalali, M.S., Bruckers, M., Westmattelmann, D. & Schewe, G. 2020. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. Journal Of Medical Internet Research. Viitattu 6.11.2024. https://janet.finna.fi, ProQuest.

Jyväskylän ammattikorkeakoulun eettiset periaatteet. 2024. JAMKin eettinen toimikunta. Viitattu 17.10.2024. https://www.jamk.fi/fi/media/41106.

Jerry-Egemba, N. 2023. Safe and sound: Strengthening cybersecurity in healthcare through robust staff educational programs. Healthcare management forum, 37, 21–25. Viitattu 29.11.2024. https://janet.finna.fi, SAGE Journals.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Jyväskylä: Docendo.

Karhumäki, E., Jonsson, A. & Saros, M. 2016. Mikrobit hoitotyön haasteena. 4. uudistettu painos. Helsinki: Edita.

Kuula, A. 2011. Tutkimusetiikka: aineistojen hankinta, käyttö ja säilytys. 2. uud. p. Tampere: Vastapaino.

Kruse, C. S., Frederick, B., Jacobson, T. & Monticone, D. K. 2017. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25, 1–10. Viitattu 11.10.2024. https://janet.finna.fi, Pubmed.

Kyberturvallisuuden kehittämisohjelma. 2021. Liikenne- ja viestintäministeriön julkaisuja 2021:7. Viitattu 23.3.2024. https://julkaisut.valtioneuvosto.fi/handle/10024/163219.

Kyberturvallisuuden sanasto. 2018. Huoltovarmuuskeskuksen, Turvallisuuskomitean ja Sanastokeskus TSK:n yhteisjulkaisu. Viitattu 1.12.2023. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf.

Kyberturvallisuusalan koulutusta kehitetään korkeakoulujen yhteistyönä – myös informaatiopsykologista tutkimusta vahvistetaan. 2022. Opetus- ja kulttuuriministeriö. Tiedote. Viitattu 24.2.2024. https://okm.fi/-/kyberturvallisuusalan-koulutusta-kehitetaan-korkeakoulujen-yhteistyona-myos-informaatiopsykologista-tutkimusta-vahvistetaan.

L612/2021. Laki sosiaali- ja terveydenhuollon järjestämisestä. Viitattu 23.1.2024. https://www.finlex.fi/fi/laki/alkup/2021/20210612.

L784/2021. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Viitattu 5.12.2024. https://www.finlex.fi/fi/laki/alkup/2021/20210784.

Lehto, M. 2023. Kyberturvallisuuden ammattilaisten koulutus. Cyberwatch Finland Magazine, 2, 19–23. Viitattu 24.2.2024. https://www.cyberwatchfinland.fi/post/uusin-cyberwatch-magazine-on-my%C3%B6s-ilmestynyt.

Liukko, S. & Perttula, S. 2024. Opinnäytetyön raportointi. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 14.1.2021. https://help.jamk.fi/raportointi/.

Lönnqvist, I. & Moilanen, P. 2017. Kyberin taskutieto - keskeisin kybermaailmasta jokaiselle. Jyväskylän yliopisto. Maanpuolustuskoulutusyhdistys. Viitattu 1.12.2023. https://jyx.jyu.fi/bitstream/handle/123456789/53510/978-951-39-7009-3.pdf.

McLeod, A. & Dolezel, D. 2018. Cyber-analytics: modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57–68. Viitattu 11.10.2024. https://janet.finna.fi, Science Direct (Elsevier).

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E. & Bonacina, S. 2021. Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21, 15, 5119. Viitattu 29.1.2024. https://doi.org/10.3390/s21155119.

NIS2 - Euroopan unionin kyberturvallisuusdirektiivi. 2024. Artikkeli Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen sivustolla. Viitattu 6.12.2024. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi.

Norri-Sederholm, T., Laitinen, T., Lehto, M., & Kari, M. J. 2019. Health care and cyber threats. Finnish Journal of EHealth and EWelfare, 11, 1–2, 86–99. https://doi.org/10.23996/fjhw.74183.

Potilas- ja asiakastietojen ja henkilötietojen käsittely. N.d. Artikkeli. Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira. Viitattu 5.12.2024. https://valvira.fi/sosiaali-ja-terveydenhuolto/potilas-ja-asiakastietojen-ja-henkilotietojen-kasittely.

Puusa, A. & Juuti, P. (toim.) 2020. Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus. Viitattu 26.9.2024. https://janet.finna.fi, Ellibslibrary.

Sosiaali- ja terveysalan eettinen perusta. 2011. Helsinki: Valtakunnallinen sosiaali- ja terveysalan eettinen neuvottelukunta ETENE-julkaisuja 32. Viitattu 17.10.2024. http://urn.fi/URN:ISBN:978-952-00-3195-4.

Suomen kyberturvallisuusstrategia. 2013. Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitean julkaisu. Viitattu 23.1.2024. https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf.

Suomen kyberturvallisuusstrategia 2019. 2019. Valtioneuvoston periaatepäätös 3.10.2019. Turvallisuuskomitean julkaisu. Viitattu 23.1.2024. https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/.

Suomen kyberturvallisuusstrategia 2024–2035. 2024. Valtioneuvoston kanslian julkaisuja 2024:11. Viitattu 28.11.2024. https://julkaisut.valtioneuvosto.fi/handle/10024/165860.

Tepa-termipankki. Erikoisalojen sanastojen ja sanakirjojen kokoelma – Sanastokeskus. N.d. Viitattu 1.12.2023. https://termipankki.fi.

Tietoturvan vuosi 2023. 2024. Kyberturvallisuuskeskuksen julkaisu. Liikenne- ja viestintävirasto Traficom. Viitattu 23.3.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_Tietoturvan-vuosi-2023_web.pdf.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu laitos. Helsinki: Tammi. Viitattu 24.10.2023. https://janet.finna.fi, Ellibslibrary.

VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta riskiviestintään. 2022. Digi- ja väestötietovirasto. Viitattu 31.1.2024. https://dvv.fi/documents/16079645/110183105/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf/6d71d86f-c7bc-6683-9b36-c55d16d4c1f0/VAHTI-riskienhallintasanasto+digitaaliseen+toimintaymp%C3%A4rist%C3%B6%C3%B6n.pdf.

Vilkka, H. 2021. Tutki ja kehitä. 5. päivitetty painos. Jyväskylä: PS-kustannus, 2021. Viitattu 26.10.2024. https://janet.finna.fi, Ellibslibrary.

Vuori, J. (toim.). 2021. Laadullisen tutkimuksen verkkokäsikirja. Tampere: Yhteiskuntatieteellinen tietoarkisto. Viitattu 24.10.2023. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/.