FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS
VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Terveydenhuollon hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen

Tiina Blek, Tytti Solankallio-Vahteri

Jyväskylän ammattikorkeakoulu, Hyvinvointiyksikkö, Jyväskylä

Tiina Blek, TtM, Jyväskylän ammattikorkeakoulu, Hyvinvointiyksikkö, PL 207, 40101 Jyväskylä, FINLAND. Sähköposti: tiina.blek@jamk.fi

Tiivistelmä

Tämä tutkimus on osa laajempaa, terveydenhuollon organisaatioiden kyberturvallisuusosaamista, -koulutustarpeita sekä henkilöstön oman organisaation tietoturvaa koskevia näkemyksiä, selvittävää tutkimusta. Tutkimus toteutettiin syksyn 2020 ja kevään 2021 välisenä aikana.

Artikkelissa raportoidaan hoitohenkilöstöä koskevan aineiston tuloksia. Tutkimuskysymyksenä oli: Miten terveydenhuollon organisaatioissa työskentelevä hoitohenkilöstö arvioi tieto- ja kyberturvallisuusosaamistaan? Tutkimusaineisto kerättiin strukturoidulla kyselylomakkeella. Harkinnanvarainen otos suunniteltiin yhteistyössä kahden sairaanhoitopiirin ja yhden perusterveydenhuollon organisaation kanssa. Kukin kohdeorganisaatio määritteli kohderyhmän tai kohderyhmät sekä sen, kuka ja millä tavoin kyselylinkki jaetaan. Tutkijoiden arvion mukaan kohderyhmään kuului noin 3500 vastaajaa, joista kyselyyn vastasi 383 henkilöä. Hoitotyön tehtävissä olevia vastaajia oli 194 (n=194).

Aineisto analysoitiin Webropol-kyselyohjelman data-analyysityökaluilla. Avoimia vastauksia käytettiin suorina lainauksina tulosten havainnollistamiseksi. Kyberturvallisuuden käsite oli tuttu 80 %:lle vastaajista. Suurin osa vastaajista (74 %) arvioi, että heillä on riittävät tieto- ja kyberturvallisuustaidot tehtäviensä hoitamiseen. Ikäryhmään 50-64 vuotta kuuluvat vastaajat arvioivat taitonsa muita ikäryhmiä useammin riittämättömiksi ($p<0.01$). Oman arvionsa mukaan, 83 % vastaajista, tietää, miten toimia tietojärjestelmähäiriön sattuessa. Eniten tiedon puutteita esiintyi alle 30-vuotiailla vastaajilla ($p<0.01$).

Vastaajista yhdeksän prosenttia totesi, että salasanan voi antaa puhelimitse tietohallinnolle ja 14 prosenttia luovuttaisi sen puhelimitse viranomaiselle. Vastaajista 16 % piti potilaan tietojen siirtämistä sähköpostitse jatkohoitopaikkaan mahdollisena ja kahdeksan prosenttia oli sitä mieltä, että opiskelija voi käyttää ohjaajansa käyttäjätunnuksia. Yhdeksän prosenttia vastaajista kertoi käyttäneensä työkaverin käyttäjätunnusta.

Tietoisuus kyberhyökkäyksen mahdollisuudesta ja sen vaikutuksista potilastietojärjestelmiin, lääkintä - ja etäseurantalaitteisiin tulisi kuulua jokaisen alalla toimivan perusosaamiseen. Sekä työssä olevan että ammattiin valmistuvan hoitohenkilöstön koulutukseen tarvitaan lisää tieto- ja kyberturvallisuuteen liit-

tyviä sisältöjä. Nykyinen osaaminen on puutteellista eikä aihealuetta huomioida hoitotyön koulutuksessa riittävästi.

Avainsanat: hoitohenkilöstö, osaaminen, tietoturva, kyberturvallisuus

Abstract

This study is part of a broader study on the cybersecurity competence, training needs and personnel's views of data security of the own organization. The study was conducted between autumn 2020 and spring 2021.

This article reports the results of nursing staff. The research question was: How do nursing staff working in healthcare organizations assess their information and cybersecurity competence? The research data was collected using a structured questionnaire. The discretionary sample was designed in cooperation with two hospital districts and one primary health care organization. Each target organization defined the target group(s) and who and how the survey link would be shared. According to the researchers' estimate, the target group included approximately 3500 respondents, of which 383 answered the survey. There were 194 respondents in nursing positions.

The data was analyzed using the data analysis tools of the Webropol survey program. Open-ended responses were used as direct quotes to illustrate the results. The concept of cybersecurity was familiar to 80% of respondents. The majority of respondents (74%) believe that they have sufficient information and cybersecurity skills to perform their duties. Most inadequate skills were reported from respondents belonging to the age group of 50-64 years ($p<0.01$). According to their own estimates, 83% of respondents know how to act in the event of an information system failure. Respondents in the youngest age group (under 30 years old) reported the most uncertainty regarding how to act in a disruption ($p<0.01$).

Nine per cent of the respondents would give their passwords by phone to the information administration and 14 per cent would hand it over by phone to the authority. Sixteen per cent of the respondents considered it possible to transfer the patient's data by e-mail to a place of further treatment, and eight per cent thought that the student could use their supervisor's usernames. Nine per cent of the respondents said that they had used a co-worker's username.

Awareness of the possibility of a cyberattack and its impact on patient information systems, medical and remote monitoring devices should be part of the basic competence of everyone in the field. More contents related to information and cyber security are needed for the nursing education curriculum and continuing education of nursing. The current competence is deficient, and the subject area is not sufficiently considered in nursing education.

Keywords: nursing staff, know-how, data security, cyber security

Johdanto

Suomessa on toistaiseksi uutisoitu muutamista terveydenhuollon järjestelmiin kohdistuneista kyberhyökkäyksistä. Kansainvälisesti tilanne on kuitenkin huolestuttava. Terveydenhuollon organisaatioihin kohdistuva kyberrikollisuus yleistyy jatkuvasti ja hyökkäysten määrä on viisinkertaistunut COVID-19 pandemian aikana [1.] Kyberhyökkäyksistä on tullut kansainvälinen uhka potilaiden hoidolle ja turvallisuudelle. Hyökkäykset vaikuttavat negatiivisesti terveydenhuoltopalvelujen saatavuuteen ja haastavat terveydenhuollon organisaatioita terveystietojen luottamuksellisuuden ja eheyden suojelussa [2].

Terveydenhuollon järjestelmät kiinnostavat kyberrikollisia useista eri syistä. Henkilötunnus, vakuutus- ja laskutustiedot sekä geneettiset- ja terveystiedot ovat tietoja, joita ei voida muuttaa yhtä helposti, kuin esimerkiksi luottokorttitietoja [3]. Tästä syystä terveystietojen arvo pimeässä verkossa on 10–20 kertaa suurempi kuin luottokorttitietojen [1]. Muita terveydenhuollon järjestelmiin kohdistuvien kyberhyökkäysten syitä ovat muun muassa käytössä olevien laitteiden suuri määrä ja vanhentunut tekniikka, lääkinnälliset laitteet, joihin verkkorikolliset pääsevät helposti sisään sekä henkilökunta, jolla ei aina ole riittävää osaamista verkkoriskeistä [4].

Terveydenhuollon tietojärjestelmiin kohdistuvat yleisimmät kyberuhkat muodostuvat tietoturvaloukkauksista (data breach), tietojenkalastelusta (phishing, vhishing, spoofing) kiristyshaittaohjelmista (ransomware) sekä palvelunestohyökkäyksistä (denial of service, DoS) [2]. Yleisimpiä tietoturvaloukkauksia ovat käyttäjätunnusten ja salasanojen väärinkäyttö, tietomurto sekä tietojen varastaminen. Kiristyshaittaohjelma on hyökkäys, jossa salataan tai manipuloidaan laitteella olevia tietoja ja vaaditaan käyttäjältä lunnaita tietojen salauksen purkamisesta. Palvelunestohyökkäys on toimintaa, jossa tietoverkkoa kuormitetaan ja lamaannutetaan niin, ettei palvelu tai tietojärjestelmä toimi enää normaalisti [5]. Tietojenkalastelun tarkoituksena on huijata henkilöitä tai organisaatioita joko paljastamaan luottamuksellisia tietoja tai lataamaan tietokoneelle haitallista toimintaa. Tietojenkalastelussa käytetään usein jakelukanavana sähköpostia [6].

Coventry ja muut (2020) toteavat tietoturvaan liittyvän piittaamattoman käytöksen olevan terveysalalla yleistä. Myös tietoisuus omaan toimintaan liittyvien riskien laajuudesta on usein vähäistä [7]. Tietoturvalliseen tai vastaavasti tietoturvasta piittaamattomaan käytökseen vaikuttavat muun muassa asenteet tietoturvaohjeita kohtaan, ulkoiset tekijät (esim. sosiaalinen paine) sekä omaan käyttäytymiseen liittyvien riskien arviointi ja arvio siitä, onko tietoturvalliseen toimintaan käytetty aika ja vaiva kannattavaa [8]. Käyttäytymiseen vaikuttavat myös halu toiminnan järkevöittämiseen ja ajan säästämiseen [9] ja tieto- ja kyberturvallisuutta koskevan tiedon ja koulutuksen puute. [10] Taanilan ja Jylhän (2022) mukaan toimintaympäristöllä ja kohdennetulla ohjeistuksella on merkittävä vaikutus terveydenhuollon tietosuojan toteutumiseen [11].

Suomalaisen yleissairaanhoitajan osaamisvaatimuksiin kuuluu osa-alue ”informaatioteknologia ja kirjaaminen”. Osaamisvaatimus pitää sisällään tietoturvaan ja -suojaan, rakenteiseen kirjaamiseen, tietojärjestelmien ja terveysteknologialaitteiden käyttöön sekä sosiaalisessa mediassa toimimiseen liittyviä osaamisia [12]. Kyberturvallisuusosaaminen ei näihin sairaanhoitajan osaamisvaatimuksiin vielä kuulu. Aiemmassa kansallisessa tutkimuksessa sairaanhoitajat ovat arvioineet hallitsevansa hyvin tai erittäin hyvin muun muassa tietosuojan ja tietoturvan periaat-

teet [13]. Myös digitaalisen osaamisen perustaidot on arvioitu hyviksi [14].

Terveydenhuollon laitteita ja järjestelmiä käyttävän henkilöstön tulisi tunnistaa reitit, joita kautta kyberhyökkäys voi levitä järjestelmiin. Näitä kriittisiä portteja ovat esimerkiksi työasemat, kopiokoneet, viivakoodilukijat, mobiililaitteet (älypuhelimet, kannettavat tietokoneet, tabletit), pilvipohjaiset sovellukset, etäkirjautuminen, työntekijöiden omat laitteet, kolmansien osapuolien (esim. potilaat, vierailijat, opiskelijat) laitteet sekä suojaamattomat Wi-Fi yhteydet. Myös lääkinnälliset- ja etäseurantalaitteet voivat toimia porttina haittaohjelmien leviämiseen [15].

Terveydenhuollon henkilöstöllä tulisi olla kykyä havaita tietojärjestelmään, lääkintälaitteeseen tai sovellukseen liittyvä poikkeava toiminta ja tietää kuinka kyseiseen tilanteeseen reagoidaan [16]. Henkilöstön tehtäviin kuuluu kiinteästi myös potilaiden ohjaaminen lääkintä- ja etäseurantalaitteiden tietoturvalliseen käyttöön [17].

Terveydenhuollon henkilöstön tietoturva- ja kyberuhkia koskeva koulutus jää usein puutteelliseksi [10]. Henkilöstö on terveydenhuollon tietoturvan viimeinen puolustuslinja, ja sen merkitystä pidetään yhtä tärkeänä kuin teknistä turvallisuutta. Henkilöstöllä tulisi siis olla asianmukainen osaaminen tieto- ja kyberturvallisuudesta huolehtimiseen [18].

Tämän tutkimuksen tarkoituksena oli selvittää terveydenhuollon organisaatioissa työskentelevän hoitohenkilöstön tieto- ja kyberturvallisuuteen liittyvää osaamista. Tutkimuksen tavoitteena oli tuottaa tietoa, jota voidaan hyödyntää terveydenhuollon organisaatioissa työskentelevän henkilöstön tarpeita vastaavan kyber- ja tietoturvakoulutuksen suunnittelussa.

Aineisto ja menetelmät

Tutkimusaineisto kerättiin strukturoidulla kyselylomakkeella, Webropol-kyselyohjelmaa hyödyntäen.

Tutkimuksen kohderyhmänä oli kahden sairaanhoitopiirin ja yhden perusterveydenhuollon organisaation henkilöstö. Harkinnanvarainen otos suunniteltiin yhteistyössä kohdeorganisaatioiden kanssa. Kunkin kohdeorganisaation kanssa määriteltiin kohderyhmä(t) sekä se, kuka ja millä tavoin kyselylinkki jaetaan. Kohderyhmää lähestyttiin joko suorilla sähköpostiviesteillä tai esihenkilöiden kautta välitetyillä viesteillä. Kyselyn jakamisesta vastasivat kohdeorganisaatioiden määrittämät yhteyshenkilöt. Lisäksi kyselylinkki julkaistiin yhden organisaation sisäisessä verkossa. Tutkijoiden arvion mukaan, kyselylomake lähetettiin noin 3500 sähköpostiosoitteeseen. Sisäisen verkon kautta julkaistu linkki oli koko organisaation henkilöstön (N~7000) saavutettavissa.

Kyselylomake

Kyselylomake perustui teoriatiedon [16,19] lisäksi ISO27000X-standardisarjaan, Haukilahti (2019) -tutkimukseen [20] sekä Duodecim -oppiportin tietosuojaan liittyvään materiaaliin.

Kyselylomake koostui kaikille vastaajille yhteisistä taustakysymyksistä (organisaatio, ikä, sukupuoli, koulutustausta, työnkuva), IT-henkilöstön kysymyksistä (kysymykset 8–30), (ei raportoida tässä artikkelissa), kysymyksistä muille kuin IT-henkilöstölle (kysymykset 31–43), (tässä artikkelissa raportoidaan hoitohenkilöstöä koskevat tulokset) ja kysymykset esimiehille (kysymys 44) (ei raportoida tässä artikkelissa). Kysely toteutettiin teknisesti niin, että valittu tehtäväkuva ohjasi vastaajan hänelle suunnattuihin kysymyksiin.

Kyselylomake oli pääosin strukturoitu. Vastaajien mielipiteitä, asenteita ja kokemuksia mitattiin viisiportaisen (esimerkiksi: täysin samaa mieltä – täysin eri mieltä, en osaa sanoa) Likertin -asteikon avulla. Lomakkeella oli kolme dikotomisen vastausvaihtoehdon kysymystä (esimerkiksi: Oletko lukenut organisaatiosi tietoturvaohjeet?) ja kolme sekamuotoista kysymystä (esimerkiksi vastausvaihtoehtoa täydentävä jatkokysymys ”Perustele toimintaasi”). Avoimia kysymyksiä oli yksi. Yhteensä hoitohenkilöstölle suunnattuja kysymyksiä tai väittämiä oli 58. Lisäksi lomakkeella oli viisi taustatietoja selvittävää kysymystä.

Kyselylomake esitestattiin. Esitestauksen perusteella lomakkeeseen ei tehty muutoksia.

Aineiston analysointi

Strukturoitu aineisto analysoitiin Webropol-kyselyohjelman data-analyysityökaluilla. Analyysimenetelminä käytettiin prosenttijakaumia ja ristiintaulukointia. Ristiintaulukointia varten Likertin asteikollisia vastausvaihtoehtoja yhdistettiin. Esimerkiksi vastausvaihtoehdot ”täysin samaa mieltä” ja ”jokseenkin samaa mieltä” muodostavat vaihtoehdon ”samaa mieltä”. Avoimien kysymysten vastauksia käsiteltiin Webropol- kyselyohjelman Text Mining -työkalulla. Laadullista aineistoa käytetään artikkelissa täydentämään sekamuotoisten kysymysten vastauksia sekä havainnollistavina suorina lainauksina.

Tulokset

Kyselyyn vastasi 194 hoitotyön tehtävissä työskentelevää henkilöä. Suurin osa vastanneista (48 %) kuului 50–64-vuotiaiden ikäryhmään. Alle 40-vuotiaita oli 26 % vastaajista. Noin puolella (49 %) vastaajista korkeakoulututkinto) ja puolella (51 %) opistoasteen tutkinto, ammatillinen tai toisen asteen koulutus. Lähes kaikki vastaajat olivat naisia (91 %).

Hoitotyön arjen tietoturva- ja tietosuojaosaaminen

Organisaationsa tietoturvaohjeet kertoivat lukeneensa 87 % vastaajista. Yleisimpiä syitä lukematta jättämiseen olivat kiire sekä epätietoisuus siitä, missä ohjeet ovat luettavissa. Muina syinä mainittiin mm. luettavien ohjeiden runsaus sekä se, ettei niiden lukemiseen ole velvoitettu.

Vastaajista yhdeksän prosenttia antaisi salasanansa puhelimitse tietohallinnolle ja 14 prosenttia luovuttaisi sen puhelimitse viranomaiselle. Vastaajista 16 % piti potilaan tietojen siirtämistä sähköpostitse jatkohoitopaikkaan mahdollisena. Erityisesti ammatillisen koulutuksen saaneet vastaajat pitivät tätä toimintatapaa mahdollisena ($p<0.01$). Kahdeksan prosenttia oli sitä mieltä, että opiskelija voi käyttää ohjaajansa käyttäjätunnuksia ja yhdeksän prosenttia vastaajista kertoi käyttäneensä työkaverin käyttäjätunnusta. Toimintatapaa perusteltiin avoimissa vastauksissa muun muassa seuraavasti:

> *”Uloskirjautuminen joka välissä on yhteiskäyttökoneissa erittäin epäkäytännöllinen tapa työskennellä. Koneen lukitseminen on työyhteisön mielestä epätoivottava tapa toimia, koska silloin omit koneen itsellesi. Juuri ketään ei haittaa käyttää silloin tällöin hiukan toisen tunnuksia = tietoturvan kannalta väärin, mutta käytännössä hiljaiesti hyväksytty tapa toimia.”*

Kaikkien hoitotyön arjen tietoturvaa ja -suojaa kuvaavien väittämien tulokset on koottu taulukkoon 1.

Taulukko 1. Hoitotyön arjen tietoturvaosaaminen (n=193).

	Täysin samaa mieltä	Jokseenkin samaa mieltä	Jokseenkin eri mieltä	Täysin eri mieltä	En osaa sanoa
Jos tietohallinto pyytää puhelimitse salasanaani, niin en voi antaa sitä heille.	83 %	7 %	2 %	7 %	1 %
Jos viranomainen pyytää puhelimitse salasanaani, niin voin antaa sen heille.	12 %	2 %	2 %	83 %	1 %
Taukohuoneen pöydältä tai tulostimesta löytyvistä potilaspapereista vastaa niiden löytäjä.	16 %	20 %	18 %	42 %	4 %
Ohjauksessani oleva opiskelija voi käyttää käyttäjätunnustani.	2 %	6 %	15 %	75 %	2 %
Samoja potilaita / asiakkaita hoitavat henkilöt voivat käyttää samaa käyttäjätunnusta / varmenne- tai vastaavaa korttia.	3 %	0 %	0 %	95 %	2 %
Voin käyttää omaa muistitikkua työkoneessani.	2 %	5 %	9 %	81 %	3 %
Puhelimen akun lataaminen työkoneen kautta on turvallista.	1 %	4 %	15 %	67 %	13 %
Sähköpostilla ei voi siirtää potilaan henkilötietoja jatkohoitoyksikköön.	80 %	2 %	5 %	11 %	2 %
Työssä käyttämääni muistitikkua ei voi käyttää omalla kotikoneella.	77 %	8 %	8 %	5 %	2 %
Olen käyttänyt työkaverini käyttäjätunnusta työhöni liittyvissä tietojärjestelmissä.	3 %	6 %	8 %	82 %	1 %
Tiedän, kuinka toimin, jos oma henkilö-/ varmennekorttini ei toimi	64 %	21 %	6 %	3 %	6 %
Tuntematon henkilö yrittää avata omalla kulkuavaimellaan / -kortillaan oven. Voin auttaa häntä ja avata hänelle oven.	0 %	5 %	18 %	76 %	1 %

Hoitohenkilöstön tieto- ja kyberturvallisuus-osaaminen

Kaikki vastaajat (99,5 %) arvioivat tietävänsä mitä tietoturvalla ja tietosuojalla tarkoitetaan. Kyberturvallisuuden käsite oli tuttu 80 %:lle vastaajista. Suurin osa vastaajista (74 %) arvioi, että heillä on riittävät tieto- ja kyberturvallisuustaidot tehtäviensä hoitamiseen. Ikäryhmään 50-64 vuotta kuuluvat vastaajat arvioivat taitonsa muita ikäryhmiä useammin riittämättömiksi ($p<0.01$). Oman arvionsa mukaan, 83 % vastaajista, tietää, miten toimia tietojärjestelmähäiriön sattuessa (esimerkiksi jos potilastietojärjestelmä ei toimi). Eniten tiedon puutteita esiintyi alle 30-vuotiailla vastaajilla ($p<0.01$).

Kyberturvallisuustietoisuutta selvitettiin yleisimpiä kyberuhkia koskevilla kysymyksillä. Yli puolet vastaajista arvioi tietävänsä hyvin tai melko hyvin, mitä kiristyshaittaohjelmat ovat (63 %) ja miten ne leviävät (62 %). Lähes kaikki vastaajat arvioivat tietävänsä hyvin tai melko hyvin, mitä huijausviestit (94 %) ja tietojenkalastelu (92 %) tarkoittavat. Sosiaalisen median riskit tunnettiin hyvin (41 %) tai melko hyvin (48 %).

Puolet vastaajista (50 %) ei tiennyt tai ei osannut sanoa, mitä informaatiovaikuttaminen tarkoittaa. Tietosuoja-asetus GDPR ja sen vaikutukset omaan työhön tunnettiin melko huonosti (43 %) tai ei ollenkaan (18 %). Palvelujen ulkoistamisen sekä laite- ja ohjelmistohankintojen riskit ja vastuut tunnettiin melko huonosti (44 %) tai huonosti (13 %). Noin kolmannes vastaajista (31 %) arvioi tietävänsä melko huonosti, mitä palvelunestohyökkäys tarkoittaa. Kaikkien tieto- ja kyberturvallisuusosaamista kuvaavien väittämien tulokset on koottu taulukkoon 2.

Taulukko 2. Hoitohenkilöstön tieto- ja kyberturvallisuusosaaminen (n=194).

	Tiedän hyvin	Tiedän melko hyvin	Tiedän melko huonosti	En tiedä lainkaan	En osaa sanoa
Mikä on päivitysten merkitys tietoturvallisuudelle?	44 %	45 %	8 %	0 %	3 %
Mikä on päivitysten merkitys kyberturvallisuudelle?	37 %	37 %	17 %	4 %	5 %
Mitä ovat kiristyshaittaohjelmat?	24 %	39 %	24 %	7 %	6 %
Miten kiristyshaittaohjelmat leviävät?	17 %	45 %	24 %	9 %	5 %
Mitä ovat huijausviestit?	46 %	48 %	6 %	0 %	0 %
Mitä on tietojenkalastelu?	43 %	49 %	7 %	0 %	1 %
Mikä on palvelunestohyökkäys?	24 %	35 %	31 %	7 %	3 %
Mitä ovat varmuuskopiot?	50 %	40 %	9 %	0 %	1 %
Mitä varmuuskopioilla tehdään?	38 %	41 %	18 %	1 %	2 %
Mitä tietoturvariskejä on sosiaalisessa mediassa?	41 %	48 %	10 %	0 %	1 %
Mikä on tietoturvarajoitusten ja -ohjeistusten merkitys?	44 %	44 %	9 %	0 %	3 %
Kuinka luottamuksellista tietoa tulee käsitellä?	65 %	32 %	2 %	0 %	1 %
Mikä on EU:n uusi tietosuoja-asetus (GDPR) ja	7 %	25 %	43 %	18 %	7 %

kuinka se vaikuttaa minuun?					
Mitä tietoturvariskejä ja -vastuita liittyy ulkoistamiseen sekä laite- ja ohjelmistohankintoihin?	11 %	25 %	44 %	13 %	7 %
Mitä on informaatiovaikuttaminen?	14 %	36 %	32 %	12 %	6 %

Pohdinta

Digitaalinen turvallisuus on osa potilasturvallisuuden varmistamista. Tässä tutkimuksessa noin viidesosa (19 %, n=37) vastaajista koki, että heillä on riittävät (vastausvaihtoehto ”täysin samaa mieltä”) tieto- ja kyberturvallisuustaidot työtehtäviensä hoitamiseen. Tulos kertoo hoitohenkilöstön akuutista osaamisen kehittämistarpeesta. Terveydenhuollon organisaatioihin kohdistuvat kyberhyökkäykset jatkavat kasvuaan [21], samalla kun terveysalan henkilöstön kuormittuneisuus [22] ja vaihtuvuus [23] näyttävät jatkavan negatiivista kehitystään. Lisäksi etäteknologian käyttöönoton lisääntyminen ja sote-uudistukseen liittyvä digitalisaatiokehitys haastaa alalla toimivan henkilöstön osaamista.

Tutkimuksen kohderyhmänä oli henkilöstö, jonka keskeisimpänä tehtävänä on potilaan hoitaminen, tutkiminen tai hyvinvoinnista huolehtiminen. Tutkimukseen osallistuneet kertoivat tietoturvaohjeiden noudattamisen vaikeuttavan tai hidastavan päivittäistä työtä. Tämä on johtanut toimintapoihin, jotka sujuvoittavat työskentelyä, mutta eivät ole tietoturvaohjeistusten mukaisia. Tulos tukee aiemmin tehtyä tutkimusta [7,24]. Coventry ja muut (2020) toteavat artikkelissaan, että tietoturvaohjeistusten tulisi terveydenhuollon toiminnan kannalta olla realistisia, käyttäjäystävällisiä ja aikatehokkaita. Nykyisiä tietoturvakäytänteitä pidetään usein raskaina, esimerkiksi järjestelmiin kirjautumiset voivat olla toistuvia, turhauttavia ja aikaa vieviä [7].

Terveydenhuollon henkilöstöön kohdistuvaa tietojenkalastelua tapahtuu esimerkiksi puhelimitse [25] ja sähköpostin [26] avulla. Tämän tutkimuksen mukaan, 14 % vastaajista luovuttaisi salasanansa puhelimitse viranomaiselle ja yhdeksän prosenttia tietohallinnolle. Toisaalta 92 % vastaajista kertoi tietävänsä, mitä tietojenkalastelu tarkoittaa. Tutkimustulos herättää pohtimaan, vastaajien arvioiman osaamisen ja käytännön toiminnan välistä ristiriitaa. Tutkimusta olisi näiltä osin tarpeellista syventää. Aiemmassa tutkimuksessa on tarkasteltu terveydenhuollon henkilöstöön sähköpostitse kohdistuvaa tietojenkalastelua. Tutkimuksessa lähetettiin noin kolme miljoonaa simuloitua tietojenkalasteluviestiä, kuuden eri sairaalan työntekijöille. Sähköpostin vastaanottaneista 14 % avasi viestissä olleen huijauslinkin [27]. Tutkimustulos on huolestuttava, sillä jo yksi varomaton linkin avaaminen voi avata väylän organisaation tietoverkkoihin. Samalla tavoin, yksikin puhelimessa luovutettu käyttäjätunnus ja salasana voi vaarantaa tuhansia potilastietoja tai altistaa tietoverkot kyberhyökkäykselle.

Tutkimukseen osallistuneista 37 % arvioi tietävänsä hyvin, kuinka toimia tietoteknisen häiriön (jos esimerkiksi potilastietojärjestelmä ei toimi) aikana. Hoitajien toimintaa kyberhäiriötilanteessa on aiemmin tutkittu laadullisen simulaatiotutkimuksen avulla. Tutkimukseen osallistuneista henkilöistä 40 % (n=20) ei havainnut järjestelmään kohdistunutta kyberhyökkäystä. Häiriötä tunnistamattomat hoitajat joko keskeyttivät hoitotoiminnot epävarmoina ja turhautuneena tai jatkoivat potilaalle haitallista hoitoa seurantalaittees-

sa näkyvän väärän informaation perusteella. [18] Lääkintälaitteisiin kohdistuneita ja niiden kautta tapahtuneita hyökkäyksiä on tapahtunut muun muassa verikaasuanalysaattoreiden, röntgen ja MRI-laitteiden kautta [28]. Tätä lääkintälaitteisiin kohdistuvaa uhkaa on kuvattu tulevaisuuden painajaiseksi [29]. Lääkintä- tai etäseurantalaitteeseen kohdistuvien kyberuhkien mahdollisuus tulisi tuoda terveysalan opiskelijoille selkeästi esiin jo tutkintokoulutuksen aikana. Myös työssä olevan henkilöstön tietoisuutta tulisi lisätä täydennys- tai työpaikkakoulutuksen avulla.

Tietojärjestelmään tai lääkintälaitteeseen kohdistuvan kyberhyökkäyksen aikaista toimintaa ja hyökkäyksestä toipumista on Suomessa mahdollista turvallisesti harjoitella Jyväskylän ammattikorkeakoulun, JYVSECTEC, kyberharjoitusympäristössä. Terveydenhuollon kyberharjoituspilotti toteutettiin syksyllä 2021. Harjoituksessa oli mukana useita terveysalan kansallisia toimijoita sekä palveluita tuottavia organisaatioita. Harjoituksen aikana toteutettiin tehohoitotilanteeseen liittyvä simuloitu kyberhyökkäys. Harjoitukseen osallistuminen koettiin hyödylliseksi sekä toiminnan kehittämisen että tietoisuuden lisäämisen näkökulmasta [30]. JYVSECTEC järjestää terveydenhuollon kansallisen kyberturvallisuusharjoituksen vuosittain.

Eettisyys ja luotettavuus

Tutkimuksen toteutuksessa noudatettiin hyvää tieteellistä käytäntöä ja Tutkimuseettisen neuvottelukunnan sekä Jyväskylän ammattikorkeakoulun tutkimuseettisen toimikunnan ohjeistuksia. Tutkimukseen osallistuneilta organisaatioilta haettiin tutkimusluvat. Aineisto kerättiin nimettömänä, eikä tutkijoilla ollut mahdollisuutta tunnistaa tutkimukseen osallistuneita.

Tutkimukseen osallistuminen oli vapaaehtoista. Vastaajan tietoinen suostumus perustui kyselytutkimuksen saatekirjeessä kerrottuun tietoon tutkimuksen tarkoituksesta, vastaajien anonymiteetin säilyttämisestä ja tulosten raportoinnista. Tutkittavien tietosuojaan liittyvät asiat kuvattiin rekisteriselosteessa.

Mittarin esitestauksen perusteella lomakkeeseen ei tarvinnut tehdä muutoksia. Palautuneet lomakkeet olivat huolellisesti täytettyjä eikä vastauksia tarvinnut poistaa. Tutkimustuloksia analysoitaessa nousi esille väittämien täsmennystarpeita. Esimerkiksi väittämään ”Sähköpostilla ei voi siirtää potilaan henkilötietoja jatkohoitoyksikköön.” vastatessaan, vastaaja ei tiennyt, puhutaanko suojatusta vai suojaamattomasta sähköpostista. Tällä voi olla vaikutusta sähköpostin käyttöä koskeviin tuloksiin.

Tutkimukseen vastasi 194 hoitotyön tehtävissä työskentelevää henkilöä. Tutkimuksen tuloksia voidaan pitää suuntaa antavina. Vastaajamäärään voi vaikuttaa tutkimuksen toteuttamisen ajankohta, joka sijoittui juuri Covid -19 pandemian aikaan. Terveydenhuollon kuormittuneisuus näkyi todennäköisesti siinä, ettei aikaa haluttu käyttää tutkimukseen vastaamiseen. Toisaalta tietoturva ja -suoja sekä kyberturvallisuus voivat aihepiireinä olla terveydenhuollon henkilöstöä vähemmän kiinnostavia.

Johtopäätökset

Sekä ammattiin valmistuva että työssä oleva hoitohenkilöstö tarvitsee tieto- ja kyberturvallisuusosaamisen kehittämistä. Osaamisen kehittämisen ja ylläpitämisen tulisi olla jatkuvaa ja perustua määriteltyihin osaamisvaatimuksiin. Terveysalan opetussuunnitelmien uudistaminen tieto- ja kyberturvallisuusosaamisen näkökulmasta on tarpeen. Organisaation tieto- kyberturvallisuudesta vastaavan teknisen henkilöstön ja hoitohenki-

löstön välistä vuoropuhelua tulee tiivistää ja kehittää, jotta käyttöön otettavat (tietoturva)ohjeet ja toimintamallit mahdollisimman hyvin tukisivat arjen hoitotyötä ja olisivat selkeästi perusteltuja.

Tutkimusta rahoittanut taho

Tutkimus toteutettiin osana HealthCare Cyber Range (HCCR) -hanketta. Hanke toteutui vuosina 2019–2021. Tutkimuksen toteuttaminen rahoitettiin HCCR-hankkeelle myönnetyllä Euroopan aluekehitysrahaston (EAKR) tuella.

Sidonnaisuudet

Kirjoittajilla ei ole sidonnaisuuksia.

Lähteet

[1] Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity Risks in a Pandemic. J Med Internet Res. 2020 Sep 17;22(9):e23692. https://doi.org/10.2196/23692

[2] Martin G, Martin P, Hankin C, Darzi A, Kinross J. Cybersecurity, and healthcare: how safe are we? BMJ. 2017 Jul 6;358:j3179. https://doi.org/10.1136/bmj.j3179

[3] Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak. 2019 Jan 11;19(1):10. https://doi.org/10.1186/s12911-018-0724-5

[4] Swivel Secure. 9 reasons why healthcare is the biggest target for cyberattacks [internet]. Swivel Secure; 2009-2021 [viitattu 8.9.2021]. Saatavilla: https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

[5] Vuorinen S (toim). Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019: 14. Helsinki: Sosiaali- ja terveysministeriö; 2019. http://urn.fi/URN:ISBN:978-952-00-4085-7

[6] Bhuyan SS, Kabir UY, Escareno JM, Ector K, Palakodeti S, Wyant D, ym. Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. J Med Syst. 2020 Apr 2;44(5):98. https://doi.org/10.1007/s10916-019-1507-y

[7] Coventry L, Branley-Bell D, Sillence E, Magalini S, Pasquale M, Magkanaraki A, ym. Cyber-risk in Healthcare: Exploring Facilitators and Barriers to Secure Behaviour. Teoksessa: HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020. Copenhagen: Springer; 2020. https://doi.org/10.1007/978-3-030-50309-3_8

[8] Blythe J. Cyber security in the workplace: Understanding and promoting behaviour change. Teoksessa: Bottoni P, Matera M (eds). Proceedings of CHItaly 2013 Doctoral Consortium, Trento, Italy, September 16th 2013. p. 92–101.

[9] Hedström K, Karlsson F, Kolkowska E. Social action theory for understanding information security non-compliance in hospitals. Information Management & Computer Security 2013;21(4):266–287. https://doi.org/10.1108/IMCS-08-2012-0043

[10] Pullin DW. Cybersecurity: Positive Changes Through Processes and Team Culture. Front Health Serv Manage. 2018 Fall;35(1):3-12. https://doi.org/10.1097/HAP.0000000000000038

[11] Taanila A, Jylhä V. Vankiterveydenhuollon ammattilaisten tietosuoja- ja turvaosaaminen: kansallinen kyselytutkimus. FinJeHeW. 2022;14(2):179-190. https://doi.org/10.23996/fjhw.109920

[12] Silen-Lipponen M, Kinnunen P, Seppänen S. Sairaanhoitajien osaaminen varmistetaan valtakunnallisella kokeella. Tutkiva Hoitotyö 2018;16(2):38–40.

[13] Saranto K, Kinnunen UM, Koponen S, Kyytsönen M, Hyppönen H, Vehko T. Sairaanhoitajien valmiudet tiedonhallintaan sekä kokemukset potilas- ja asiakastietojärjestelmien tuesta työtehtäviin. FinJeHeW. 2020;12(3):212–228. https://doi.org/10.23996/fjhw.95711

[14] Kinnunen UM, Heponiemi T, Rajalahti E, Ahonen O, Korhonen T, Hyppönen H. Factors Related to Health Informatics Competencies for Nurses—Results of a National Electronic Health Record Survey. Comput Inform Nurs. 2019 Aug;37(8):420-429. https://doi.org/10.1097/CIN.0000000000000511

[15] Dill MW, Lucci S, Walsh T. Understanding Cybersecurity: A Primer for HIM Professionals. J AHIMA. 2016 Apr;87(4):46-51.

[16] Kamerer JL, McDermott D. Cybersecurity: Nurses on the Front Line of Prevention and Education. J Nurs Regul 2020;10(4):48-53. https://doi.org/10.1016/S2155-8256(20)30014-4

[17] Billingsley L, McKee SA. Cybersecurity in the Clinical Setting: Nurses' Role in the Expanding "Internet of Things." J Contin Educ Nurs. 2016 Aug 1;47(8):347-9. https://doi.org/10.3928/00220124-20160715-03

[18] Willing M, Dresen C, Gerlitz E, Haering M, Smith M, Binnewies C, ym. Behavioral responses to a cyber-attack in a hospital environment. Sci Rep. 2021 Sep 29;11(1):19352. https://doi.org/10.1038/s41598-021-98576-7

[19] Conaty-Buck S. Cybersecurity and healthcare records. Am Nurse Today 2017;12(9):62-65.

[20] Haukilahti T. Improving Cyber Security awareness: Health, social services and regional government reform in South Ostrobothnia [opinnäytetyö]. Jyväskylä: JAMK University of Applied Sciences; 2019. https://urn.fi/URN:NBN:fi:amk-201904185558

[21] Morgan S. The 2020-2021 Healthcare Cybersecurity Report. Cybersecurity Ventures; 2021 [viitattu 16.12.2022]. Saatavilla: https://www.herjavecgroup.com/healthcare-cybersecurity-report-2021/

[22] Selander K, Nikunlaakso R, Sipponen J, Niemi M, Olin N, ym. Sosiaali- ja terveysalan ammattilaisten kasautuva koronakuorma: kyselytutkimus Suomen tilanteesta syksyllä 2020. Tutkiva Hoitotyö 2021;19(2):30–37.

[23] Tevameri T. Katsaus sote-alan työvoimaan Toimintaympäristön ajankohtaisten muutosten ja pidemmän aikavälin tarkastelua. TEM toimialaraportit 2021: 2. Helsinki: Työ- ja elinkeinoministeriö; 2021. http://urn.fi/URN:ISBN:978-952-327-812-7

[24] Pollini A, Callari TC, Tedeschi A, Ruscio D, Save L, Chiarugi F, ym. Leveraging human factors in cybersecurity: an integrated methodological approach. Cogn Technol Work. 2022;24(2):371-390. https://doi.org/10.1007/s10111-021-00683-y

[25] Health Sector Cybersecurity Coordination Center. Vishing Attacks on the Rise. Health Sector Cybersecurity Coordination Center, U.S. Department of Health and Human Services; 2022 [viitattu 16.12.2022]. Saatavilla: https://www.hhs.gov/sites/default/files/vishing-attacks-on-the-hph-sector-analyst-note.pdf

[26] Jalali MS, Bruckes M, Westmattelmann D, Schewe G. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. J Med Internet Res. 2020 Jan 23;22(1):e16775. https://doi.org/10.2196/16775

[27] Gordon WJ, Wright A, Aiyagari R, Corbo L, Glynn RJ, Kadakia J, ym. Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. JAMA Netw Open. 2019 Mar 1;2(3):e190393. https://doi.org/10.1001/jamanetworkopen.2019.0393

[28] Storm D. MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks [internet]. Computerworld 2015 [viitattu 14.12.2022]. Saatavilla: https://www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

[29] Newman LH. Medical Devices Are the Next Security Nightmare [internet]. Wired March 2, 2017 [viitattu 14.12.2022]. Saatavilla: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/.

[30] JYVSECTEC. Terveydenhuollon harjoitukset. JYVSECTEC - JYVÄSKYLÄ SECURITY TECHNOLOGY [internet]. Jyväskylä: JAMK University of Applied Sciences, Institute of Information Technology [viitattu 14.12.2022]. Saatavilla: https://jyvsectec.fi/fin/terveydenhuolto/terveydenhuollon-harjoitukset/