OULUN AMMATTIKORKEAKOULU

Tero Hietala

Tietoturva terveys- ja hyvinvointialalla

Tietoturva terveys- ja hyvinvointialalla

Tero Hietala
Opinnäytetyö
Kevät 2024
Tietojenkäsittelyn tutkinto-ohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn tutkinto-ohjelma

Tekijä(t): Tero Hietala
Opinnäytetyön nimi: Tietoturva terveys- ja hyvinvointialalla
Työn ohjaaja(t): Minna Kamula
Työn valmistumislukukausi ja -vuosi: Kevät 2024 Sivumäärä: 33

Ajatus opinnäytetyön aiheesta ja sen kirjoittamisesta syntyi työharjoitteluni aikana, jolloin toimin terveydenhuollon, digitaalisten toimintaympäristöjen ja hyvinvoinnin turvaamisen ICMT-yrityksessä tietoturvaharjoittelijana. Tunsin, että oma kokemukseni ja tietämykseni aihealueesta edistäisi opinnäytetyön suunnittelua ja kirjoittamista. Osasin etsiä ja tutkia oikeanlaisia lähdemateriaaleja.

Tavoitteena oli syventää ymmärrystä terveys- ja hyvinvointialan tietoturvasta. Tutkimusongelmana on mitä haasteita terveys- ja hyvinvointialalla on tietoturvaan liittyen ja voidaanko keksiä ratkaisuja tietoturvan parantamiseksi.

Opinnäytetyön tietoperusta käsittelee yleisesti terveys- ja hyvinvointialan tietoturvaan liittyvää sanastoa, käsitteitä ja uutisia. Tätä varten hain artikkeleita ja kirjallisuutta mm. avoimista tietokannoista, mutta hyödynsin myös ajankohtaisia asiantuntijablogeja.

Opinnäytetyön lähdemateriaalien tutkimisen, analysoinnin ja raportoinnin aikana opin todella paljon Suomen potilastietolaista, standardeista ja uutisista koskien tietoturvaa terveys- ja hyvinvointialalla.

Asiasanat: Tietoturvallisuus, Kyberturvallisuus, Tietomurto, Terveys- ja Hyvinvointiala.

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Business Information Systems

Author(s): Tero Hietala
Title of thesis: Information security in the health and wellness sector
Supervisor(s): Minna Kamula
Term and year when the thesis was submitted: Spring 2024
Number of pages: 33

The idea for the thesis and its writing arose during my internship as an information security intern at ICMT, a company that secures healthcare, digital operating environments, and well-being. I felt that my own experience and knowledge of the subject area would contribute to the planning and writing of the thesis. I knew how to search for and research the right kind of source material.

The goal was to deepen the understanding of information security in the health and wellness sector. The research problem focused on identifying the challenges in the health and welfare sector related to information security and determining whether solutions could be found to improve it.

The thesis database covers vocabulary, concepts, and news related to information security in the health and wellness sector. For this, I searched for articles and literature from open databases and also utilized current expert blogs.

During the study, analysis, and reporting of the source materials for the thesis, I gained significant knowledge about the Finnish Patient Information Act, standards, and news regarding information security in the health and welfare sector.

Keywords: Information Security, Cyber Security, Data Breach, Health and wellness sector.

SISÄLLYS

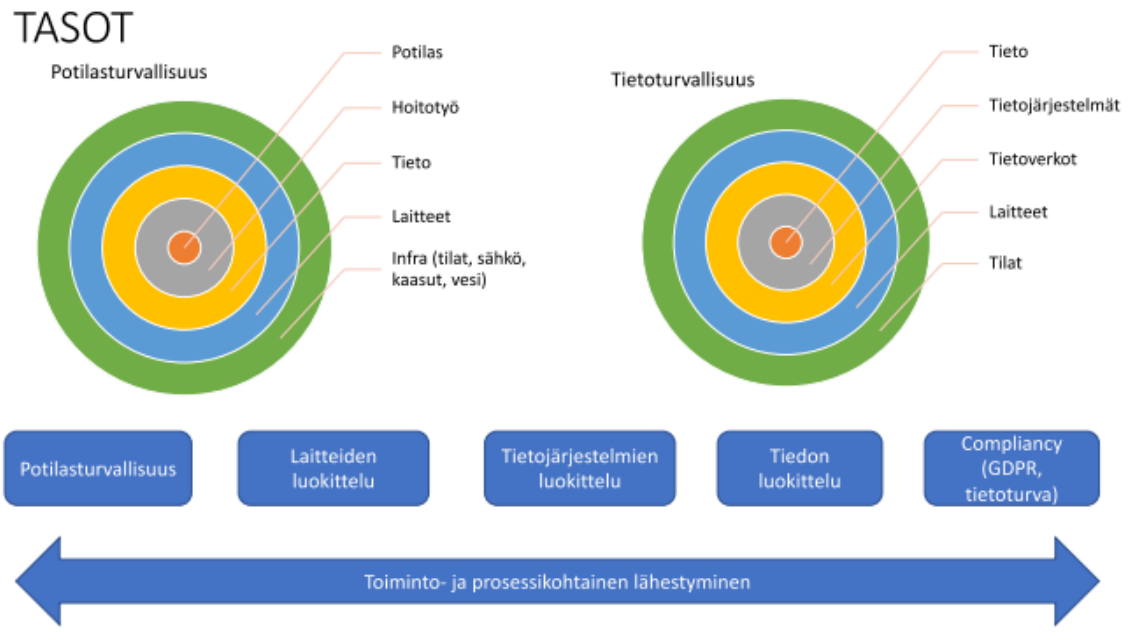
1 JOHDANTO

Tässä opinnäytetyössä käsitellään terveys- ja hyvinvointialan tietoturvaa, joka on noussut keskeiseksi ja ajankohtaiseksi aiheeksi Suomen terveydenhuollossa. Opinnäytetyön tavoitteena on syventää ymmärrystä terveys- ja hyvinvointialan tietoturvasta sekä tunnistaa keskeiset haasteet ja ratkaisut tietoturvan parantamiseksi. Yhteenvetona opinnäytetyön tulokset ja johtopäätökset tuovat esiin terveys- ja hyvinvointialan tietoturvan nykytilan sekä tarjoavat näkemyksiä ja suuntaviivoja tulevaisuuden kehitykseen ja toimintamalleihin. Idea opinnäytetyön aiheelle syntyi työharjoitteluni aikana, jossa toimin tietoturvaharjoittelijana. Tämän opinnäytetyön taustalla ei ollut toimeksiantajaa.

Opinnäytetyön tutkimusongelmana on mitä haasteita terveys- ja hyvinvointialalla on tietoturvaan liittyen ja voidaanko sen parantamiseksi keksiä ratkaisuja.

Tietoperustassa käsitellään yleisesti terveys- ja hyvinvointialan tietoturvaan liittyvää sanastoa, käsitteitä ja uutisia. Tätä varten haetaan artikkeleita ja kirjallisuutta mm. avoimista tietokannoista, mutta myös ajankohtaisia asiantuntijablogeja hyödynnetään. Tutkimusmenetelmänä käytetään kirjallisten lähteiden analysointia, havainnointia ja raportointia.

Tutkimuksessa ei huomioida tietojärjestelmän tai sen käytöstä johtuvia puutteita, jotka vaikuttavat hoitoon ja voivat esimerkiksi lääkkeiden yhteisvaikutuksesta aiheuttaa ongelmia potilaille. Kuvassa 1 esitetty kuvaus eri tasoista liittyen potilas- ja tietoturvallisuuteen. Opinnäytetyössä käsitellään pääsääntöisesti vain tietoturvallisuutta sekä potilasturvallisuuteen vahvasti liittyviä lääkinnällisiä laitteita, standardeja ja asetuksia.

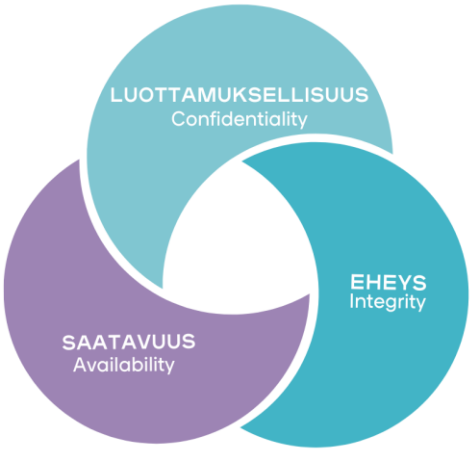


Kuva 1. Kuvaus eri tasoista sekä potilasturvallisuuden että tietoturvallisuuden näkökulmasta (Kyberturvallisuuskeskus 2022)

2 TIETOTURVA JA TIETOSUOJA

2.1 Tietoturva

Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus. Tieto voi olla digitaalisessa tai fyysisessä muodossa. Saatavuus takaa, että tieto on saatavilla tarvittaessa. Luottamuksellisuus varmistaa, että tietoa käsittelevät vain ne henkilöt, joilla on oikeus käsitellä sitä. Eheys varmistaa, että tieto säilyy luotettavana ja muuttumattomana esimerkiksi ennen tietoturvahyökkäystä ja sen jälkeen. Tietoturva on osa organisaation kokonaisturvallisuutta, johon kuuluu keskeisenä tekijänä riskien hallinta. Tietoturvallisuuden tulee olla osana organisaation prosesseja ja toiminnan jatkuvaa. (Visma 2019.) Kuvassa 2 on esitetty CIA-mallin kolme osa-aluetta.



Kuva 2. CIA-malli (Funidata 2023)

CIA-mallin kolme osa-aluetta

Luottamuksellisuus (Confidentiality) varmistaa, että herkkä tieto on saatavilla vain valtuutetuille yksilöille tai järjestelmille, suojaten sitä luvattomalta pääsyltä.
Eheys (Integrity) tarkoittaa tiedon tarkkuuden ja luotettavuuden ylläpitämistä estämällä luvattomat muutokset, muutokset tai väärentämiset.
Saatavuus (Availability) tarkoittaa, että tiedot ja järjestelmät ovat käytettävissä ja toiminnassa tarvittaessa, minimoimalla katkokset tai häiriöt. (Digiturvamalli 2024.)

2.1.1 Kyberturvallisuus

Kyberturvallisuus kattaa laajan kirjon toimia ja ohjelmistoja, joilla pyritään turvaamaan esimerkiksi laitteita ja tietoa kyberturvahyökkäyksiltä, häiriöiltä ja muilta vaaroilta. Kyberturvallisuus on myös hyvin keskeinen osa yksityishenkilöiden, yritysten sekä valtioiden puolustusta ja sodankäyntiä. Isot yritykset ja organisaatiot voivat olla usein houkuttelevia kohteita verkkorikollisille. Riittämättömät turvatoimet voivat johtaa monenlaisiin haittoihin, kuten rahan menetykseen, identiteettivarkauteen, tilien kaappaamiseen, datan häviämiseen, henkilökohtaisten tiedostojen lukitsemiseen ja yksityisyyden menetykseen. (F-Secure 2024.)

Mikä on tieto- ja kyberturvallisuuden ero?
Kyberturvallisuus koskee elektronisten laitteiden, yksityishenkilöiden ja organisaatioiden suojaamista tietoturvahyökkäyksiltä kyberavaruudessa. Tietoturva koskee pääsääntöisesti tiedon luottamuksellisuuden, eheyden ja saatavuuden suojaamista. Kyberturvallisuuteen lukeutuu muun muassa pilvitietoturva, sovellusten suojaus, kriittinen infrastruktuuri ja verkkoturvallisuus. Tietoturva käsittelee pääsyn ja vaatimuksenmukaisuuden hallintaa sekä teknisiä hallintalaitteita. (SecurityScorecard 2020.)

2.1.2 Yleisiä tietoturvauhkia

Kiristyshaittaohjelmat ovat haittaohjelmia, joita käytetään erityisesti kiristyshyökkäyksiin. Hyökkäyksissä organisaation tai henkilön tiedot salataan, jolloin he eivät voi käyttää tietojaan ennen kuin lunnassumma on maksettu.
Virukset ja madot ovat haitallisia ja usein huomaamattomia haittaohjelmia, jotka voivat levitä itsenäisesti käyttäjän verkossa tai järjestelmässä. Pahimmillaan ne voivat aiheuttavaa merkittävää vahinkoa järjestelmille ja tiedoille.
Tietojenkalasteluhyökkäyksessä hyökkääjä tekeytyy luotettavaksi organisaatioksi tai käyttäjäksi varastaakseen tietoja sähköpostin, tekstiviestin tai muun viestintätavan avulla. Edellä mainituilla hyökkäyksillä pyritään saamaan haltuun arkaluontoisia ja henkilökohtaisia tietoja.
Hajautetut palvelunestohyökkäykset (DDoS) käyttävät bottiverkkoja yrityksen sivuston tai sovellusten kaatamiseen, jolloin niiden oikeutetut käyttäjät eivät voi käyttää palvelua. Hyökkäykset voivat aiheuttaa merkittäviä toiminnan keskeytyksiä ja taloudellisia ongelmia organisaatioille. (Microsoft 2024.)

2.2 Tietosuoja

Jokaisella kansalaisella on oikeus henkilötietojensa suojaan. Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä. (Tietosuojavaltuutetun toimisto 2024.)

Henkilötiedoilla tarkoitetaan kaikkia mahdollisia tietoja, jotka koskevat tunnistettua tai tunnistettavissa olevaa henkilöä. Henkilötietoja ovat muun muassa nimi, osoite, IP-osoite, kulttuurinen profiili, tulot ja henkilökortin tai passin numero. (Europa 2022.)

GDPR (General Data Protection Regulation) on henkilötietojen käsittelyä sääntelevä laki, joka astui voimaan toukokuussa 2018. Se on tietosuojalaki, joka määrittelee yksityishenkilöiden henkilötietojen käsittelyä koskevat säännöt ja velvoitteet Euroopassa. Lainsäädäntöuudistuksen tavoitteena on parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa, edistää digitaalisten sisämarkkinoiden kehitystä sekä vastata uusiin digitalisaatioon ja globalisaation liittyviin tietosuojakysymyksiin. (Tietosuojavaltuutetun toimisto 2024.)

3 TIETOTURVA TERVEYS- JA HYVINVOINTIALALLA

3.1 Suomen lainsäädäntö

Suomessa potilastietolailla tarkoitetaan lakia 784/2021, 703/2023, joka säätelee sosiaali- ja terveydenhuollon asiakastietojen käsittelyä. Lailla turvataan potilaiden yksityisyyden suoja sekä varmistetaan, että terveydenhuollossa käsiteltävät tiedot ovat luotettavia ja asianmukaisesti säilytettyjä. (Finlex 2024.)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021)

1.11.2021 voimaan astunut lainsäädäntö (784/2021) sisältää säännökset sosiaali- ja terveydenhuollon asiakastietojen sähköisen käsittelyn yleisistä vaatimuksista mm. potilastiedon käyttöä säätelevien asiakkaan informoinnin, luovutusluvan, suostumuksen ja kieltojen suhteen. Lain pääasiallisena tarkoituksena on turvata tietojen käytettävyys, eheys ja säilyminen sekä asiakkaan yksityisyyden suoja. Asiakastietojen käsittelylle asetettavien yleisten vaatimusten avulla pyritään luomaan perusta asianmukaiselle sähköiselle tietojenkäsittelylle, jossa edellytetään yhtenäisen tietoturvatason toteutumista kaikissa asiakkaan tietojen käsittelyn vaiheissa. Laki myös velvoittaa sosiaalihuollon palvelunantajat liittymään Kanta-palveluihin, mikä mahdollistaa asiakastietojen luovuttamisen muille sosiaalihuollon palvelunantajille. Lisäksi lainsäädännössä täsmennetään yksityisten terveydenhuollon palvelunantajien liittymisvelvollisuutta. Tämä varmistaa, että myös yksityiset terveydenhuollon toimijat noudattavat tietoturva- ja tietosuojastandardeja asiakkaidensa tietojen käsittelyssä. (Kauvo & Virkkunen 2022.)

Alla lueteltuna lain tärkeimpiä lukuja ja niiden pykäliä.

1 Luku – Yleiset säännökset.

> Pykälä 1. Lain tarkoitus: ” Tämän lain tarkoituksena on edistää ja mahdollistaa sosiaali- ja terveydenhuollon tuottamien asiakastietojen ja asiakkaan itsensä tuottamien hyvinvointitietojen tietoturvallista käsittelyä terveydenhuollon ja sosiaalipalveluiden järjestämisen ja tuottamisen käyttötarkoituksissa. Lain tarkoituksena on myös edistää asiakkaan tiedonsaantimahdollisuuksia asiakastietojensa käsittelystä. ”

2 Luku – Valtakunnallisten tietojärjestelmäpalvelujen rekisterinpito.

Pykälä 4. Valtakunnallisten tietojärjestelmien rekisterinpitäjä: ” Kansaneläkelaitos on omatietovarannon, luovutuslokirekisterin lokitietojen säilytyspalvelun ja sen omaan toimintaansa liittyvien käyttölokien rekisterinpitäjä. Kansaneläkelaitoksella ei kuitenkaan ole oikeutta käsitellä omatietovarantoon tallennettuja tietoja laajemmin kuin mitä omatietovarannon ylläpitoon kuuluvat tehtävät välttämättä edellyttävät tai luovuttaa niitä muihin kuin 13 §:n 2 momentin mukaisiin käyttötarkoituksiin siten kuin mainitussa momentissa säädetään. Kukin sosiaali- ja terveydenhuollon palvelunantaja on toiminnassaan syntyneiden käyttölokien rekisterinpitäjä. Ammattilaisen käyttöliittymän käyttölokien yhteisrekisterinpitäjiä ovat terveydenhuollon ammattihenkilö ja Kansaneläkelaitos. Kansaneläkelaitos toimii käyttöliittymän käyttölokien yhteyspisteenä. Reseptikeskuksen rekisterinpitäjästä säädetään sähköisestä lääkemääräyksestä annetun lain (61/2007) 18 §:ssä.”

4 Luku – Asiakastietojen käsittely sosiaali- ja terveydenhuollossa.

Pykälä 15. Käyttöoikeus asiakastietoon: ” Käyttöoikeuksien on perustuttava sosiaali- tai terveydenhuollon ammattihenkilön ja muun asiakas- ja potilastietoja käsittelevän henkilön työtehtävään ja annettavaan palveluun siten, että henkilöllä on käyttöoikeus vain työtehtävissään tarvitsemiinsa välttämättömiin asiakastietoihin, joihin hänellä on tiedonsaantioikeus. Asiakastietojen käsittelyn perusteena on oltava tietoteknisesti varmistettu asiakas- tai hoitosuhde tai muu lakiin perustuva oikeus. Sosiaali- ja terveysministeriön asetuksella säädetään, mitä tietoja ammattihenkilöt ja muut asiakastietoja käsittelevät henkilöt työtehtävänsä ja annettavan palvelun perusteella saavat käyttää. Palvelunantajan on määriteltävä sosiaali- ja terveydenhuollon ammattihenkilön tai muun asiakastietoja käsittelevän henkilön oikeus käyttää asiakastietoja. Palvelunantajan on pidettävä rekisteriä asiakastietojärjestelmiensä ja asiakasrekisteriensä käyttäjistä sekä näiden käyttöoikeuksista.”

Pykälä 17. Asiakastietojen käsittelijöiden tunnistaminen: ” Asiakastietojen sähköisessä käsittelyssä asiakas, palvelunantaja, muu asiakastietojen käsittelyn osapuoli ja näiden edustajat sekä tietotekniset laitteet on tunnistettava luotettavasti. Asiakastietoja käsittelevät henkilöt, palvelunantajat, tietotekniset laitteet ja valtakunnalliset tietojärjestelmäpalvelut on tunnistettava todentamalla. Terveydenhuollon potilastietoja saa luovuttaa salassapitosäännösten estämättä sosiaalihuollon palvelunantajalle sosiaalihuollon järjestämiseksi, tuottamiseksi ja toteuttamiseksi potilaan antaman suostumuksen perusteella. Suostumuk-

sen edellytyksistä säädetään tietosuoja-asetuksen 7 artiklassa. Potilastiedot voidaan luovuttaa asiakkaalle hyvinvointisovelluksen tai kansalaisen käyttöliittymän kautta. Saadakseen tiedot hyvinvointisovellukseen potilaan tulee ottaa hyvinvointisovellus käyttöön ja hyväksyä tietojen luovutus."

Pykälä 20. Potilastietojen luovuttaminen valtakunnallisten tietojärjestelmäpalvelujen avulla: " Terveydenhuollon potilastietoja saa luovuttaa salassapitosäännösten estämättä 6 §:ssä tarkoitettujen valtakunnallisten tietojärjestelmäpalvelujen avulla toiselle terveydenhuollon palvelunantajalle tai toiseen saman palvelunantajan potilasrekisteriin potilaan terveydenhuollon järjestämiseksi, tuottamiseksi ja toteuttamiseksi. Potilastietoja ei kuitenkaan saa luovuttaa ilman potilaan antamaa luovutuslupaa tai potilaslain 13 §:n 3 momentin 3 kohdassa taikka muussa luovutuksen oikeuttavassa laissa säädettyä perustetta. "

5 Luku – Tietoturvallisuuden ja tietosuojan omavalvonta.

Pykälä 27. Tietoturvasuunnitelma: " Palvelunantajan, välittäjän ja Kansaneläkelaitoksen on laadittava tietoturvaan ja tietosuojaan sekä tietojärjestelmien käyttöön liittyvä tietoturvasuunnitelma Ennen liittymistään valtakunnallisten tietojärjestelmäpalvelujen käyttäjäksi on palvelunantajan tietoturvasuunnitelmassa selvitettävä, miten tietosuoja ja valtakunnallisten palvelujen tietoturvallisen käytön edellyttämät vaatimukset on varmistettu."

Pykälä 28. Tietoturvallisuuden omavalvonnan toteuttaminen ja vastuu. " Sosiaali- ja terveydenhuollon palvelunantajan vastaavan johtajan on huolehdittava, että 27 §:ssä tarkoitettu tietoturvasuunnitelma laaditaan ja sitä noudatetaan. Vastaavan johtajan on annettava kirjalliset ohjeet asiakastietojen käsittelystä ja noudatettavista menettelytavoista sekä huolehdittava henkilökunnan riittävästä asiantuntemuksesta ja osaamisesta asiakastietojen käsittelyssä. Tietosuojan ja tietoturvan seurannan ja valvonnan toteuttamiseksi palvelunantajalla on oikeus saada Kansaneläkelaitokselta omien asiakasrekisteriensä lokitiedot, tiedonhallintapalvelussa ja tahdonilmaisupalvelussa olevien tietojen käsittelyyn liittyvät lokitiedot ja omatietovarannon lokitiedot siltä osin kuin asianomaisen palvelujenantajan henkilökunta on katsellut ja käsitellyt asiakkaan tiedonhallintapalvelussa, tahdonilmaisupalvelussa ja omatietovarannossa olevia tietoja, jos se on tarpeen asiakkaan asiakastietojen käsittelyn lainmukaisuuden selvittämiseksi. Kansaneläkelaitoksen ja välittäjän on seurattava tietoturvasuunnitelmansa toteutumista."

7 Luku – Tietojärjestelmien ja hyvinvointisovellusten olennaiset vaatimukset.

Pykälä 37. Tietoturvallisuuden arviointi.” Luokkaan A kuuluvan tietojärjestelmän ja hyvinvointisovelluksen olennaisten tietoturvallisuusvaatimustenmukaisuuden arviointi suoritetaan tämän lain ja tietoturvallisuuden arviointilaitoksista annetun lain mukaisesti. Tietoturvallisuuden arviointilaitoksen on annettava suorittamastaan tietoturvallisuuden arvioinnista tietojärjestelmäpalvelun tuottajalle ja hyvinvointisovelluksen valmistajalle todistus sekä siihen liittyvä tarkastusraportti. Arviointi on suoritettava tietojärjestelmän ja hyvinvointisovelluksen käyttötarkoitusta koskevien olennaisten vaatimusten tai järjestelmään tehtyjen muutosten laajuuden mukaisesti.”

8 Luku – Ohjaus ja valvonta.

Pykälä 39. Ohjaus, valvonta ja seuranta: ” Sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn ja siihen liittyvän tiedonhallinnan yleinen suunnittelu, ohjaus ja valvonta sekä päätöksenteko merkittävien tiedonhallintahankkeiden kokonaisrahoituksesta kuuluvat sosiaali- ja terveysministeriölle. Digi- ja väestötietoviraston hoitaman varmennepalvelun yleinen ohjaus ja valvonta kuuluvat kuitenkin sosiaali- ja terveysministeriölle ja valtiovarainministeriölle yhteisesti. Terveyden ja hyvinvoinnin laitos vastaa sosiaali- ja terveydenhuollon asiakastiedon sähköisen käsittelyn ja siihen liittyvän tiedonhallinnan sekä 6 §:ssä tarkoitettujen valtakunnallisten tietojärjestelmäpalvelujen ja yhteisten hallinnonalakohtaisten tietovarantojen käytön ja toteuttamisen suunnittelusta, ohjauksesta ja seurannasta. Sosiaali- ja terveysalan lupa- ja valvontavirasto sekä aluehallintovirasto toimialueellaan ohjaavat ja valvovat niille säädetyn toimivallan mukaisesti osaltaan tämän lain noudattamista.”

Pykälä 41. Ilmoittaminen tietojärjestelmän olennaisten vaatimusten poikkeamista: ” Jos palvelunantaja havaitsee, että tietojärjestelmän olennaisten vaatimusten täyttymisessä on merkittäviä poikkeamia, sen on ilmoitettava asiasta tietojärjestelmäpalvelun tuottajalle. Jos poikkeama voi aiheuttaa merkittävän riskin asiakasturvallisuudelle tai tietoturvalle, on palvelunantajan, apteekin, tietojärjestelmäpalvelun tuottajan tai valmistajan, Kansaneläkelaitoksen tai Terveyden ja hyvinvoinnin laitoksen ilmoitettava siitä Sosiaali- ja terveysalan lupa- ja valvontavirastolle. Myös muu taho voi ilmoittaa Sosiaali- ja terveysalan lupa- ja valvontavirastolle havaitsemistaan riskeistä. Jos palvelunantaja tai muu taho havaitsee tietojärjestelmän olennaisten vaatimusten täyttymisessä tietosuojapoikkeamia, sen on ilmoitettava asiasta tietosuojavaltuutetulle.” (Finlex 2021.)

Sosiaali- ja terveydenhuollon asiakastietojen sähköisen käsittelyn lainsäädäntö on hyvin merkittävä tietojen käsittelyn, luotettavuuden ja yksityisyyden kannalta. Tässäkin lainsäädännössä nousee esiin tietoturvan tärkeimmät elementit, joita ovat eheys, saatavuus ja luottamuksellisuus. Lain käytännön toteutuminen organisaatioissa riippuu sen noudattamisesta. Lainsäädännön noudattaminen edistää ja turvaa jokaisen henkilön asiakastietoja. Laki myös erityisesti määrittelee tiedonvaihdon eri sosiaali- ja terveydenhuollon toimijoiden välillä. Tämä on erittäin tärkeää silloin kun potilas esimerkiksi saa hoitoa useammalta eri organisaatiolta.

3.2 Terveydenhuollon tietoturvallisuusstandardit

Terveydenhuollon aihealue sisältää standardeja, jotka liittyvät muun muassa terveyspalveluihin, lääkinnällisiin laitteisiin, apuvälineisiin, lääkintätiloihin, lääke- ja laboratoriolääketieteeseen sekä tietosuojaan ja tietoturvallisuuteen (kuva 3). Terveydenhuollon tietoturvallisuuden erityispiirteitä käsittelee erityisesti standardiin SFS-EN ISO 27799:2016 standardin ISO/IEC 27002 avulla. Tässä laajasti tunnetussa ja kansainvälisessä standardissa esitetään organisaation tietoturvastandardeja ja tietoturvallisuuden hallintakäytänteitä koskevaa ohjeistusta. Standardissa käsitellään hallintakeinojen valintaa, toteuttamista ja hallintaa, ottaen myös samalla huomioon organisaation monimuotoiset tietoturvallisuuden riskiympäristöt. (SFS 2024.)

Terveydenhuoltoalalla on lisäksi olemassa myös oma laatustandardi, joka on luotu maailman tunnetuimmasta laadunhallintajärjestelmästä, ISO 9001:stä. Tämä standardi on suunniteltu kaikkien terveyspalveluja tarjoavien organisaatioiden käyttöön riippumatta organisaation koosta, tyypistä tai sen tuottamista palveluista. (SFS 2024.) Kuvassa 3 on lueteltuna aihealueiden keskeisimmät standardit.

Kuva 3. Terveydenhuollon IT-standardit (SFS 2024)

Terveydenhuollon standardien kolme aihealuetta käsittelevät:
Yleisiä asioita kuten IT johtamista, hallintaa ja ohjausta.
Terveydenhuollon tietotekniikkaa mm. lääkinnälliset laitteet ja potilastietojärjestelmät.
Teknologiaa liittyen mm. ohjelmistotuotantoon ja järjestelmiin.

3.3 Lääkinnälliset laitteet

Lääkinnällisiä laitteita ovat hengityskoneiden tai defibrillaattorien lisäksi useat kotoa löytyvät tarvikkeet, esimerkiksi verenpainemittari, laastari, silmälasit ja kuulolaite. Lääkinnällisiä laitteita ovat myös esimerkiksi silmien kostutukseen tarkoitetut silmätipat tai lihaskipuihin käytettävä kylmägeelit. Lääkinnällisiin laitteisiin eivät taas lukeudu esimerkiksi sykemittarit, hengityssuojat tai käsien desinfiointiaineet. (Fimea 2024.)

Suomessa Fimea valvoo lääkinnällisten laitteiden vaatimustenmukaisuutta ja sen alan toimijoita. Valvonta kattaa lääkinnällisten laitteiden markkinoille saattamisen, ammattimaisen käytön ja ylläpidon. Fimean valvonta tapahtuu yhteistyössä EU:n viranomaisten kanssa. Tämän lisäksi Fimea vastaa lääkinnällisten laitteiden markkinoinnin valvonnasta ja käsittelee vaaratilanneilmoituksia sekä myöntää lääkinnällisille laitteille myynnin esteettömyystodistuksia, tutkimus- ja poikkeuslupia. (Fimea 2024.)

Lääkinnällisten laitteiden standardeissa asetetut vaatimukset kattavat turvallisuuden, laadun ja toiminnan instrumenteissa, laitteistoissa, ohjelmistoissa, materiaaleissa ja tarvikkeissa. Laitteet on valmistettava ja suunniteltava siten, että ne eivät suunnitelluissa olosuhteissa ja tarkoituksessa käytettyinä vaaranna potilaiden turvallisuutta ja terveydentilaa. Vuonna 2017 astuivat voimaan EU:n asetukset (2017/745) lääkinnällisistä laitteista (Medical Devices Regulation, MDR) ja (2017/746) in vitro -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista (In Vitro Diagnostic Regulation, IVDR). MDR astui kuitenkin vasta voimaan 26.5.2021. Sen siirtymäaikaa pidennettiin alkuperäisestä vuodella COVID-19-pandemian vuoksi. Asetus koskee sellaisenaan kaikkia EU-maita. MDR tiukentaa lääkinnällisten laitteiden valmistajien, maahantuojien ja jakelijoiden velvoitteita. Asetusta in vitro -diagnostiikkaan tarkoitetuista lääkinnällisistä laitteista sovelletaan pääsääntöisesti 26.5.2022 lähtien. IVD-asetus tuo tiukemmat vaatimukset kliiniselle tutkimusnäytölle ja vaatimustenmukaisuuden arvioinnille. (SFS 2024.) Kuvassa 4 kuvataan Suomessa lääkinnällisen laitteen ideasta tuotteeksi -kaavio.

Kuva 4. Ideasta tuotteeksi (SFS 2020)

3.4 Tietoturvakoulutus

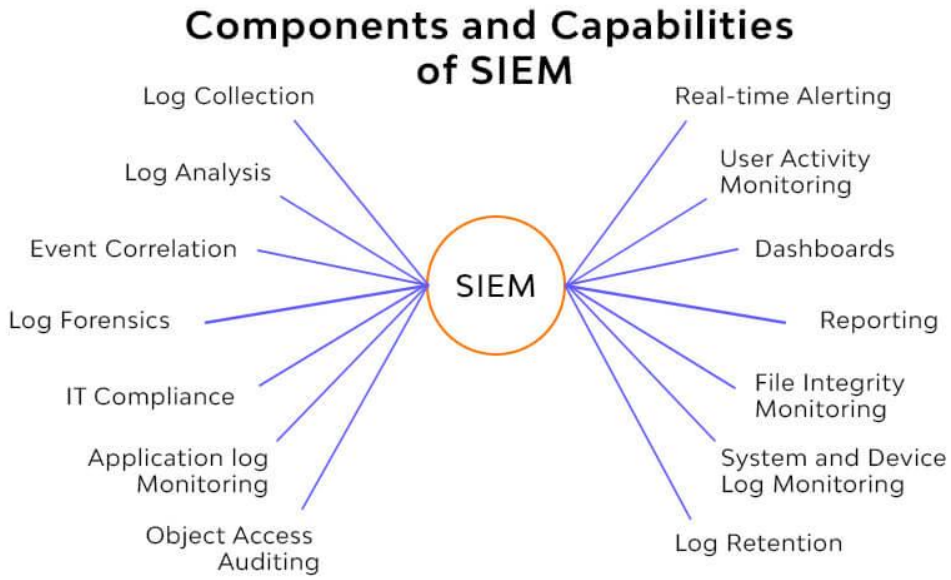
Tietoturvakoulutus on hyvin keskeinen osa organisaation tietoturvastrategiaa, sillä se tähtää organisaation henkilöstön tietoturvatietoisuuden ja -taitojen parantamiseen. Riittävästi koulutettu henkilöstö pystyy tehokkaammin tunnistamaan ja torjumaan tietoturvariskejä työelämässä, kotona ja

matkoilla. Erilaisia koulutusmenetelmiä voivat olla esimerkiksi pelit, videot, kyselyt, verkkokoulutukset ja webinaarit. Organisaation turvallisuusstrategian tehokkuus riippuu osin siitä, kuinka hyvin henkilöstö on valmistautunut toimimaan tietoturvariskitilanteissa niiden sattuessa. (2ns 2024.) Kuvassa 5 terveydenalan kyberturvaan erikoistuneen Fortified organisaation kaavio siitä, kuinka tehdä kyberturvallisuuskoulutuksesta osa terveydenhuoltokulttuuria.

Kuva 5. Kuinka tehdä kyberturvallisuuskoulutuksesta osa terveydenhuoltokulttuuria (Fortified 2023)

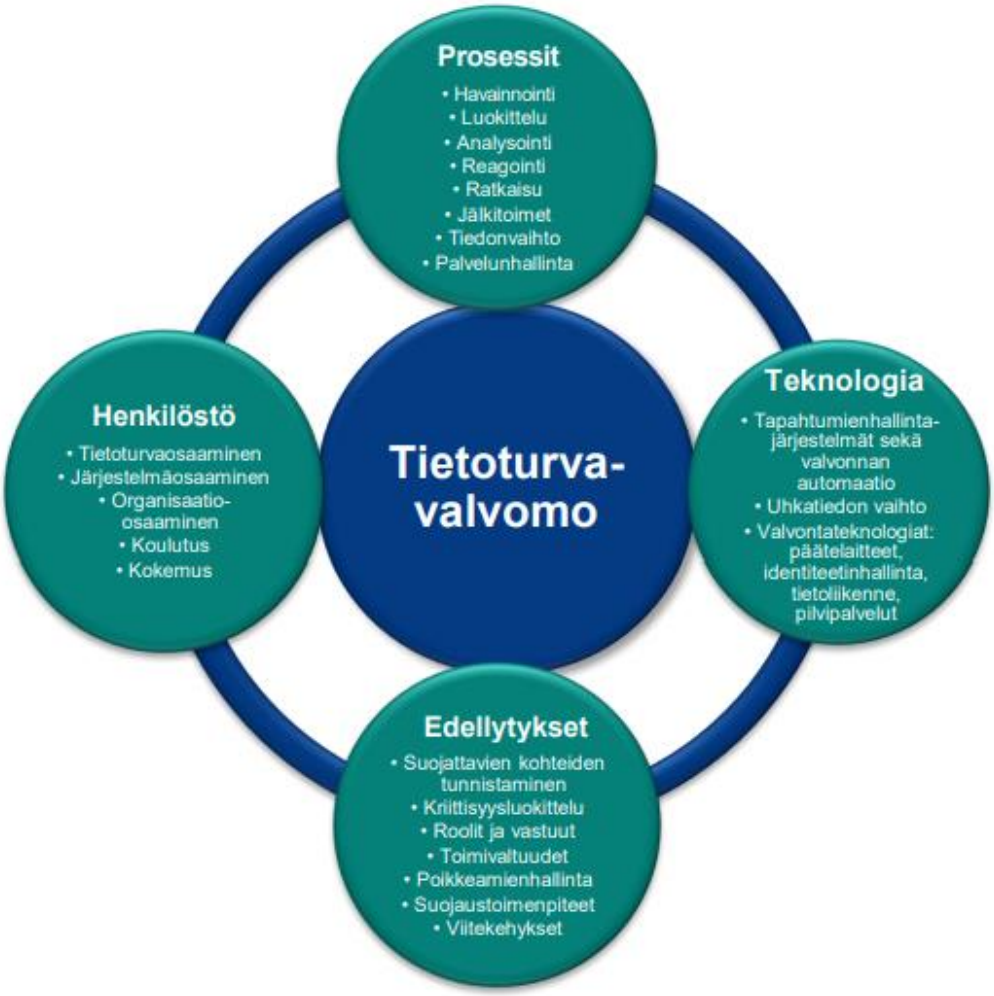
3.5 Tietoturvapoikkeamien hallinta

SIEM (Security Information and Event Management) on tapahtumien ja tietoturvatietojen seurantatyökalu, joka tallentaa lokitietoa kaikesta yrityksen kyberturvallisuuteen liittyvästä. Se ilmoittaa havaitsemistaan uhkista ja mahdollistaa siten nopean reagoinnin mahdollisiin tietoturvauhkiin. (Advania 2024.) Kuvassa 6 on esitetty SIEM-työkalun keskeiset komponentit ja ominaisuudet, joita ovat muun muassa lokien kerääminen, lokien analyysi, raportointi ja reaaliaikainen hälytys.



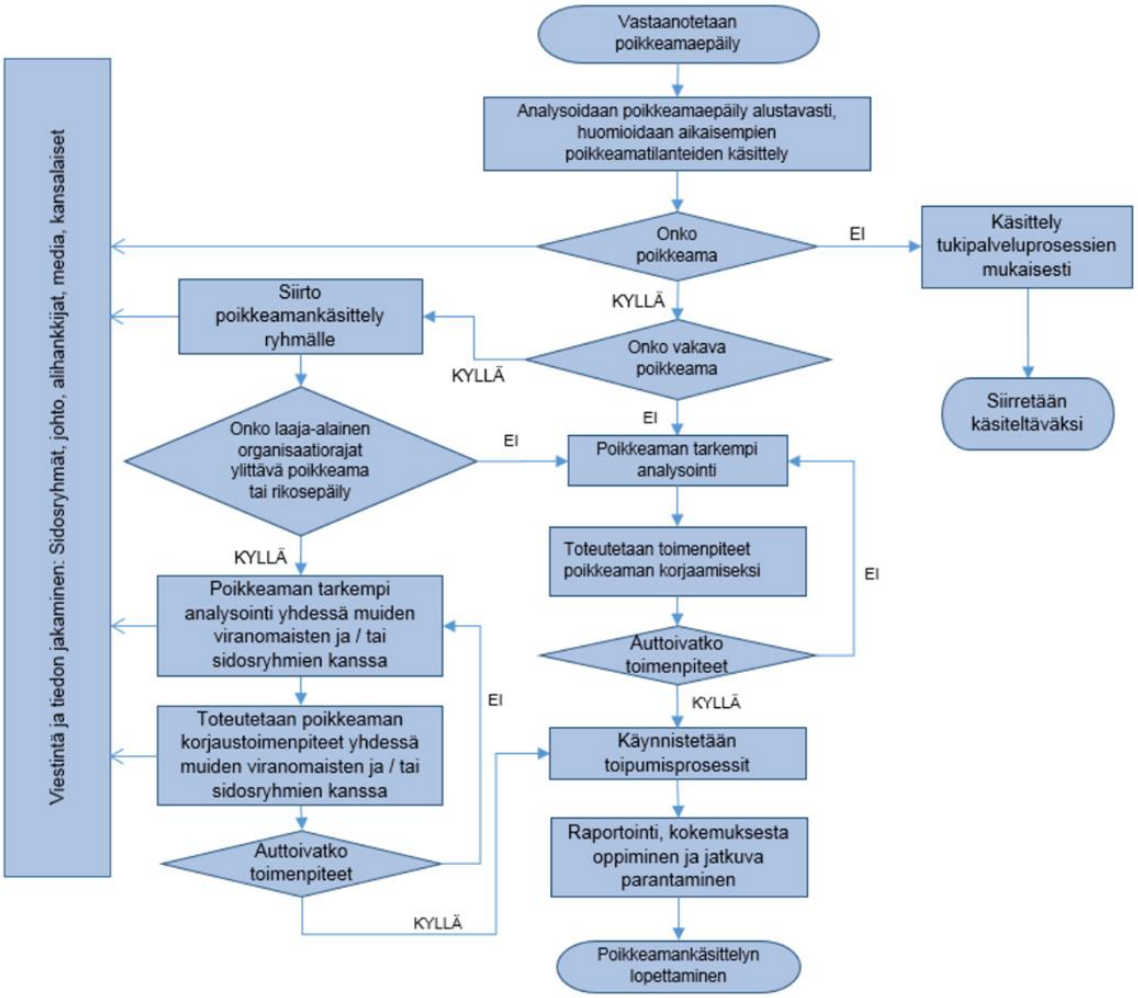
Kuva 6. SIEM-työkalun komponentit ja ominaisuudet (Nordcloud 2024)

Tietoturvavalvomo eli Security Operations Centre (SOC) muodostaa keskeisen komponentin organisaation kyvyssä valvoa digitaalista turvallisuutta ja reagoida siinä tapahtuviin poikkeamiin, aiheutuivatpa poikkeamat sitten organisaation ulkopuolisesta tai sen sisäpuolisesta syystä (kuva 7). Tietoturvavalvomo kerää ja käsittelee tauotta tietoa valvottavista järjestelmistä. Tietoa toimittaviin järjestelmiin lukeutuvat esimerkiksi palomuurit, haavoittuvuuksien seurantajärjestelmät, tunkeutumisen havainnointijärjestelmät sekä verkkotasolla että yksittäisissä päätelaitteissa, automatisoidut tunkeutumisen estojärjestelmät, lokijärjestelmät ja haittaohjelmasuojaukset. Tietoturvavalvomotoiminnan tavoitteena on havaita todennäköiset tietoturvapoikkeamat, analysoida havainnot, poistaa havaitut haittaohjelmat tai hyökkääjät ja palauttaa valvottavat järjestelmät tietoturvalliseen tilaan. (Digi- ja väestötietovirasto 2023.)



Kuva 7. Tietoturvavalvomon eri osa-alueet (Digi- ja väestötietovirasto 2023)

Tietoturvapoikkeamien hallintaprosessi koostuu monista eri osista (kuva 8). Sen keskeisenä tarkoituksena on varautua häiriötilanteisiin ja turvata toiminnan jatkuvuus minimoimalla häiriötilanteiden aiheuttamat vahingot. Lisäksi hallintaprosessin tavoitteena on estää vastaavien häiriötilanteiden syntymistä tulevaisuudessa. Tietoturvapoikkeamien käsittelyprosessiin vaikuttavat useat tekijät, kuten organisaation koko, poikkeaman tyyppi ja toimintojen ulkoistaminen. Tehokas ja järjestelmällinen tietoturvapoikkeamien hallinta on olennainen osa organisaation tietoturvaa ja riskienhallintaa. (Valtionvarainministeriö 2017.)



Kuva 8. Tietoturvapoikkeamien käsittelyprosessi (Valtionvarainministeriö 2017)

3.6 Tietoturva-auditointi

Tietoturva-auditointi on tehokas työkalu, joka antaa kolmannen osapuolen objektiivisen näkemyksen yrityksen tietoturvan nykytilasta. Se on systemaattinen prosessi, jossa käydään läpi organisaation määrittelemän osa-alueen toiminta tietoturvan näkökulmasta. Auditoinnin kohteeksi voidaan valita esimerkiksi tietty liiketoimintayksikkö, järjestelmä, toimintaympäristö tai työvälineet. (Nixu 2023.)

Tietoturva-auditoinnit soveltuvat organisaatioille, joissa kiinnitetään huomiota tietoturvallisen toiminnan kehittämiseen tai organisaatioille, jotka haluavat varmistua tämänhetkisestä tietoturvatilanteesta ja mahdollisista kehityskohteista. (Opsec 2024.)

3.6.1 Kybermittari

Kyberturvallisuuskeskuksen kehittämä Kybermittari on ilmainen kyberturvallisuuden arviointi- ja kehittämispalvelu, joka on tarkoitettu tietoturva-ammattilaisille ja organisaatioiden johdolle. Kybermittari on räätälöity Suomessa toimivien yritysten ja organisaatioiden tarpeisiin ja se pohjautuu kansainvälisiin kyberkyvykkyyksien mittausmalleihin. Kybermittarin avulla johto saa näkymän toiminnalle tärkeiden kyberkyvykkyyksien kypsyystasoon osa-alueittain ja tavoitteittain. Kybermittari näyttää, millä tasolla kyberriskien tunnistaminen, suojautuminen, havainnointi, reagointi ja palautuminen ovat organisaatiossa. Mittaustulosten avulla organisaatio voi seurata ja raportoida kyberturvallisuuden kehitystä eri mittauskertojen välillä. Organisaatio mittaa itsearviointina tai tuettuna kypsyystasonsa kyberturvallisuuden hallinnan eri osa-alueilla. Kybermittari kertoo saavutetun kypsyystason ja esittää seuraavalle tasolle vaadittavat kehitysalueet. (Kyberturvallisuuskeskus 2024.)

Kybermittari koostuu yhdestätoista eri kyberturvallisuuden osiosta. Lisäksi siihen sisältyvät eri osioille asetetut tavoitteet sekä näiden täyttymistä mittaavat käytännöt. Osiot on esitetty kuvassa 9, jossa näkyvät myös NIST-viitekehyksen viisi eri vaihetta. (Kyberturvallisuuskeskus 2022.)

Kuva 9. Kybermittarin osiot (Kybertuvallisuuskeskus 2022)

3.6.2 NIST SP 800-53

NIST SP 800-53 on tietoturvastandardi, jota käytetään muun muassa sovelluksien tietoturva-arviointien viitekehyksenä. Standardin on kehittänyt National Institute of Standards in Technology (NIST). Standardi tarjoaa laajan valikoiman tietoturvatoimenpiteitä ja ohjeita, jotka käsittelevät eri alueita, kuten riskienhallintaa, pääsynhallintaa ja haavoittavuuksien hallintaa. (Varonis 2023.) Standardin viisi ydinkomponenttia ovat tunnistaminen, suojaaminen, havainnointi, vastaaminen ja palautuminen (kuva 10).

Kuva 10. NIST 800-53 viisi ydinkomponenttia (Sprinto 2024)

3.6.3 ISO/IEC 27001:2022

ISO/ICE 27001 on maailman tunnetuin tietoturvan hallintajärjestelmien standardi. Standardi antaa kaikenkokoisille ja kaikilta toimialoilta toimiville yrityksille ohjeita tietoturvan hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen. ISO/IEC 27001- sertifikaatti on yksi tapa osoittaa sidosryhmille ja asiakkaille, että yritys tai organisaatio on sitoutunut ja pystyy hallitsemaan tietoja turvallisesti ja varmasti. Sertifikaatti on laajalti käytössä ympäri maailmaa. ISO Survey 2022:n mukaan yli 70 000 sertifikaattia ilmoitettiin 150 maasta kaikilta talouden aloilta maataloudesta sosiaalipalveluihin. (ISO 2022.) Kuvassa 11 esitetään organisaatioiden tietoturvamatkaa eli tietoturvan kehittämistä ISO 27001- standardin rakennetta mukaillen.

Kuva 11. Tietoturvamatka ISO 27001 -standardin rakennetta mukaillen (Arter 2022)

3.7 Vastaamon tietomurto

Ensimmäinen psykoterapiakeskus Vastaamon tietomurto tapahtui marraskuussa 2018. Toinen tietomurto ajoittui maaliskuulle 2019. Kyseiset tietomurrot koskivat jopa kymmeniätuhansia asiakkaita. Varastettuihin tietoihin kuuluivat henkilötietoja, kuten osoitteet, koko nimi, sosiaaliturvatunnus ja psykoterapiatuntien sisältö. Lokakuussa 2020 hakkerit vaativat Vastaamolta noin puolen miljoonan euron lunnaita kryptovaluutta bitcoineina. Pian lunnasvaatimuksen jälkeen psykoterapiakeskuksen asiakkaat alkoivat myös saada uhkauksia sähköpostitse, joissa näkyivät heidän henkilötunnuksensa ja heiltä pyydettiin muutaman sadan euron lunnaita. (Theelephantmum 2020.)

Tietoturvaloukkaus tapauksen tultua julkisuuteen aloittivat viranomaiset heti tiiviin yhteystyön uhrien tukemiseksi sekä syyllisten kiinni saamiseksi. Psykoterapiakeskus Vastaamon tietomurto oli historiallinen ja poikkeuksellinen tietoturvaloukkaustapaus Suomessa ja maailmalla. Suuri määrä tiedoista päätyi lopulta pimeään verkkoon kaikkien saataville. Tämänkaltaista kiristyshyökkäystä ei ollut aikaisemmin nähty, eikä vastaavaa ole ilmennyt tapauksen jälkeen Suomessa tai muualla maailmassa. (Kyberturvallisuuskeskus 2022.)

Myräkkä Vastaamon tapahtumista herätti laajaa keskustelua potilastietojen tietoturvasta sekä kotimaassa että kansainvälisesti. Selvää oli, että tietoja on suojeltava niin, ettei niistä tule rikollisille

kauppatavaraa tai kiristyskeinoa. Syksyllä 2021 terveyden ja hyvinvoinnin laitos (THL) reagoi tapahtuneeseen päivittämällä asiakastietojärjestelmien luokittelua ja niiden tietoturvallisuuden arviointia koskevat ohjeensa. (Kyberturvallisuuskeskus 2022.)

Julius Kivimäkeä alias Aleksanteri Kivimäkeä syytetään Vastaamoon kohdistuneesta törkeästä tietomurrosta, liki 9600 törkeästä yksityiselämää loukkaavasta tiedon levittämisestä, yli 21300:sta törkeän kiristyksen yrityksestä sekä 20 törkeästä kiristyksestä. Oikeudenkäynti Psykoterapiakeskus Vastaamoon kohdistuneesta tietomurrosta ja potilaiden kiristyksestä päättyi 8.3.2024. (IS 2024.)

Käräjäoikeus antoi tuomionsa Vastaamoa koskevassa jutussa tiistaina 30.4.2024. Länsi-Uudenmaan käräjäoikeus on tuominnut Aleksanteri Kivimäen 6 vuoden ja 3 kuukauden vankeusrangaistukseen tietomurtoon liittyvistä rikoksista. (Yle 2024.)

3.8 Näin tunnistat digihuijauksen

Digihuijaukset ovat rikollisten tekemiä erityyppisiä petoksia, joissa hyödynnetään digitaalisia laitteita kuten, tablettia, tietokonetta tai kännykkää. Näissä huijauksissa menetetään rahaa, henkilötietoja tai käyttäjätunnuksia ja salasanoja. Yleisimpiä digihuijauksia ovat verkkokauppahuijaukset, tietojenkalastelu, romanssihuijaukset, sijoitushuijaukset sekä toimitusjohtajahuijaukset. (Kuluttajaliitto 2021.)

Kyberturvallisuuskeskus (Kyberturvallisuuskeskus 2023) antaa seuraavanlaiset ohjeet digihuijaukselta suojautumiseen.

Älä luota aina sokeasti sähköpostin lähettäjätietoihin. Osoite voi olla väärennetty, sähköpostin lähettäjän tietokoneeseen on voitu murtautua tai hänen sähköpostisalasanansa on voitu arvata. Älä klikkaa epäilyttävältä vaikuttavan viestin sisältämää linkkiä, vaan mene selaimella suoraan haluamasi palvelu sivuille.

Älä luota kaikkiin verkkosivustoihin. Älä syötä luottokorttitietojasi tai verkkopankkitunnuksiasi epäilyttävän oloiselle sivustolle harkitsematta.

Tarkasta selaimen kohdeosoite. Nettihuijarit rekisteröivät tietojenkalastelusivuiksi verkkotunnuksia, jotka ovat lähes saman muotoisia ja nimisiä kuin alkuperäisetkin verkkotunnukset (esimerkiksi nordea.fi vs. noreda.fi).

Onhan selaimen tietoliikenteen salaus päällä? Verkkopankkien salauksen voi tarkistaa selaimen osoiterivin lukkoikonista ja https://-alkuisesta verkko-osoitteesta. Jos osoiterivillä ei ole näkyvillä lukkoikonia niin hyvin suurella todennäköisyydellä kyseessä ei ole oikea verkkopankki. https://-alku tai lukkoikoni eivät tänä päivänä ole tae verkkosivun aitoudesta tai luotettavuudesta. Nykyään on mahdollista huijata myös tietoliikenteen salauksella.

Jos salasanasi on murrettu, kannattaa se vaihtaa välittömästi. Jos olet käyttänyt samaa salasanaa myös muissa palveluissa, vaihda myös niiden salasana pikimmiten. Luo myös jokaiseen käyttämääsi palveluun oma salasana. (Kyberturvallisuuskeskus 2023.)

Kuvassa 12 esitellään yksi mahdollinen skenaario, miten hyökkääjät voivat toteuttaa kiristyshaittaohjelmahyökkäyksen. Hyökkäystapoja ja toteuttamiskeinoja on tämän lisäksi myös useita muita.

Kuva 12. Esimerkki organisaatioon kohdistuvasta kiristyshaittaohjelmahyökkäyksestä (Kyberturvallisuuskeskus 2022)

4 TULOKSET JA JOHTOPÄÄTÖKSET

Opinnäytetyön tavoitteena oli kartoittaa tietoturvan nykytila ja sen haasteet terveys- ja hyvinvointialalla. Tutkimusongelmana oli mitä haasteita terveys- ja hyvinvointialalla on tietoturvaan liittyen ja voidaanko sen parantamiseksi keksiä ratkaisuja. Tein ajatuskartan terveys- ja hyvinvointialan tietoturvaan vaikuttavista asioista (kuva 13). Vaaleansinisillä olevat taustat ovat positiivisia asioista ja punaisella värjätyt negatiivisesti vaikuttavia tietoturvauhkia.

Kuva 13. Terveys- ja hyvinvointialan tietoturvan ajatuskartta (Omakuva 2024)

Tietoperustaa kirjoittaessa, lähdemateriaaleja ja uutisia tutkiessa nousi esiin myös muutamia kysymyksiä liittyen henkilöstön tietoturvakouluttamiseen sekä tietomurtoihin. Psykoterapiakeskus Vastaamon tietomurto herätti monessa kansalaisessa huolia liittyen tämänhetkiseen potilasturvallisuuteen. Suuri tietomurto mahdollistui, koska Vastaamon asiakastietojärjestelmää valvottiin vähemmän kuin monien muiden terveysalan toimijoiden. Tietojärjestelmällä ei ollut yksityiskohtaisia tietoturvavaatimuksia tai sille ei ollut tehty ulkopuolista arviointia. Ennen psykoterapiakeskus Vastaamon tietomurtoa yksityisillä terveydenhuollon palveluntarjoajilla ei ollut vaatimuksia liittyä Kanta-palveluun. Kanta tuottaa sosiaali- ja terveydenhuollon digitaalisia palveluja, jotka hyödyttävät kansalaisia sekä sosiaali- ja terveydenhuollon toimijoita (Kanta 2024.) Uusi laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (784/2021) tuli voimaan 1.11.2021. Laki velvoittaa

sosiaalihuollon palvelunantajat liittymään Kanta-palveluun. Tämä toivon mukaan poistaa mahdollisuuden vastaavanlaisesta tietomurrosta kuin Vastaamon tapauksessa oli kyse.

Digihuijauksen uhriksi päätyminen myös mahdollistaa henkilötietojen joutumista vääriin käsiin. Kappaleessa 2.9 ”Näin tunnistat digihuijauksen” kyberturvallisuuskeskus on laatinut ohjeet, kuinka voidaan minimoida mahdollisuus joutua huijauksen uhriksi. Viimeisen 5 vuoden aikana olen lukenut paljon uutisia ja artikkeleita henkilöistä, jotka ovat joutuneet digihuijauksen uhriksi ja menettäneet jopa satoja tuhansia euroja. Poliisi on laatinut hyvin informoivat kampanjan digihuijauksien välttämiseen videoiden avulla. Videot löytyvät osoitteesta https://poliisi.fi/ennakoija. Kampanja tavoitteena on ensisijaisesti lisätä ikäihmisten kykyä tunnistaa ja välttää digihuijauksia, mutta mielestäni kampanjan sopii kaiken ikäisille henkilöille.

Tietoturvakouluttamiseen liittyen mielestäni selkeillä ja helposti ymmärrettävillä tietoturvakäytännöillä ja -ohjeilla sekä henkilökunnan säännöllisillä koulutuksilla parannettaisiin tietoturvasääntöjen noudattamista ja toteutumista merkittävästi. Lisäksi olisi tärkeää varmistaa, että kaikki työntekijät ymmärtävät tietoturvan merkityksen osana organisaation toimintaa ja sitoutuvat sen edistämiseen päivittäisessä työssä.

5 POHDINTA

Opinnäytetyön lähdemateriaalien tutkimisen, analysoinnin ja raportoinnin aikana opin todella paljon Suomen potilastietolaista, standardeista ja uutisista koskien tietoturvaa terveys- ja hyvinvointialalla. Tämänhetkinen tilanne ja tulevaisuuden näkymät tietoturvan osalta ovat positiiviset. Yhä enemmän puhutaan tietomurroista ja digihuijauksista ja niistä uutisoiminen edistää näiden tiedottamista Suomen kansalaisille. Terveydenhuollon tietojärjestelmien suunnittelu ja rakentaminen on erittäin vaativaa, koska ala on niin tiukasti säänneltyä lukuisten eri lakien, standardien ja sääntelyiden vuoksi. Tarvitaan paljon enemmän kuin idea siitä, millainen olisi hyvä ja tarpeellinen järjestelmä terveydenhoitoalan tarpeisiin.

Tiukka aikataulu edellytti suunniteltua ja tiivistä työskentelytahtia. Käytin paljon aikaa ajankohtaisten ja relevanttien lähteiden tutkimiseen ja niiden läpikäymiseen. Opinnäytetyön aikana saadut neuvot ja vinkit ohjaajaltani olivat suuressa roolissa työn etenemisessä. Opinnäytetyön aihe ja tavoitteet olivat alusta alkaen selkeät. Loppujen lopulta eri lähteiden ja artikkeleiden tutkiminen osoitti, että tietoturva aihealueena on todella laaja.

Näin jälkeenpäin ajateltuna opinnäytetyön tutkimuskysymyksien kannalta olisi ollut suositeltavaa haastatella terveys- ja hyvinvointialalla työskenteleviä henkilöitä koskien heidän kokemukseensa tietoturvakouluttamisesta työssään. Näin olisin saanut hyvinkin ajankohtaista tietoa ja materiaalia tutkimuskysymyksiin.

LÄHTEET

Arter 2022. kuva 11. Näin pääset alkuun tietoturvatyössä ja vältyt turhalta tekemiseltä. Hakupäivä 13.5.2024. https://www.arter.fi/matka-kohti-iso-27001-27701-tietoturvasertifiointia/.

Advania 2024. Tietoturvan valvonta (SIEM ja SOC). Hakupäivä 7.5.2024. https://www.advania.fi/palvelumme/tietoturva/tietoturvan-valvonta.

Digi- ja väestötietovirasto 2023. Kuva 7. Kuntien tietoturvavalvomoiden toimintamalli, s.7. Hakupäivä 15.5.2024. https://dvv.fi/documents/16079645/110183105/Selvitys+-+Kuntien+tietoturvavalvomoiden+toimintamalli.pdf/a7f70592-f6eb-218f-eefe-a4821fbf7ce5/Selvitys+-+Kuntien+tietoturvavalvomoiden+toimintamalli.pdf?t=1700818145439.

Digiturvamalli 2024. CIA-arvojen mukaisen luokittelun käyttöönotto digiturvamallissa. Hakupäivä 20.5.2024. https://www.digiturvamalli.fi/ohjeartikkelit/cia-arvojen-mukaisen-luokittelun-kayttoonotto-digiturvamallissa#cia-luokittelulla-tarkoitetaan-.

Europa 2022. Yleinen tietosuoja-asetus. Hakupäivä 20.5.2024. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm.

Fimea 2024. Mitä ovat lääkinnälliset laitteet? Hakupäivä 3.5.2024. https://fimea.fi/laakinnalliset_laitteet/mita-ovat-laakinnalliset-laitteet-.

Fimea 2024. Lääkinnälliset laitteet. Hakupäivä 3.5.2024. https://fimea.fi/laakinnalliset_laitteet.

Finlex 2021. Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Hakupäivä 2.5.2024. https://www.finlex.fi/fi/laki/alkup/2021/20210784.

Finlex 2023. Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä. Hakupäivä 2.5.2024. https://www.finlex.fi/fi/laki/alkup/2023/20230703.

Fortified 2023. Kuva 5. How to Make Cybersecurity Training Part of your Healthcare Culture. Hakupäivä 11.5.2024. https://fortifiedhealthsecurity.com/blog/cybersecurity-employee-training/.

Funidata 2023. Kuva 2. Tietoturva SaaS palvelukehityksessä – miten huolehdimme tietoturvan eri osa-alueista. Hakupäivä 1.5.2024. https://www.funidata.fi/blogi/tietoturva-saas-palvelukehityksessa.

F-Secure 2024. Mitä on kyberturvallisuus? Hakupäivä 21.5.2023. https://www.f-secure.com/fi/articles/what-is-cyber-security.

Ilta-Sanomat 2024. Vastaamo-oikeudenkäynti päättyy tänään. Hakupäivä 7.5.2024. https://www.is.fi/digitoday/art-2000010279759.html.

ISO 2022. ISO/IEC 27001:2022. Hakupäivä 7.5.2024. https://www.iso.org/standard/27001.

Kauvo Taina ja Virkkunen Heikki (toim.) 2022. Kirjaamisopas: potilastiedon kirjaamisen yleisopas versio 5.0. Terveyden ja hyvinvoinnin laitos, s.19–21. Hakupäivä 24.5.2024. https://www.julkari.fi/bitstream/handle/10024/144139/Potilastiedon%20kirjaamisen%20yleisopas_PRINT-3-2022.pdf?sequence=1&isAllowed=y.

Kanta 2024. Mitä kantapalvelut ovat? Hakupäivä 15.5.2024. https://www.kanta.fi/mita-kanta-palvelut-ovat.

Kuluttajaliitto 2021. Näin tunnistat digihuijauksen. Hakupäivä 10.5.2024. https://www.kuluttajaliitto.fi/wp-content/uploads/2023/12/5b621e5b-naintunnistatdigihuijauksen_fin_saavutettava-1.pdf.

Kybertuvallisuuskeskus 2022. Kuva 1. Toimintojen ja tietojärjestelmien kriittisyyden luokittelu, s.13. Hakupäivä 22.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Sote_toimintojen_ja_tietoj%C3%A4rjestelmien_kriittisyyden_luokittelu_v1.0.pdf.

Kybertuvallisuuskeskus 2022. Kuva 9. Toimintojen ja tietojärjestelmien kriittisyyden luokittelu, s.10. Hakupäivä 22.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Sote_toimintojen_ja_tietoj%C3%A4rjestelmien_kriittisyyden_luokittelu_v1.0.pdf.

Kyberturvallisuuskeskus 2022. Kyberturvallisuuskeskuksen viikkokatsaus - 44/2022. Hakupäivä 7.5.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-442022'.

Kyberturvallisuuskeskus 2024. Kybermittari. Hakupäivä 6.5.2024. https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari.

Kyberturvallisuuskeskus. Kuva 12. Toiminta kiristyshaittaohjelmatilanteessa – johdon ohje. Sivu 3. Hakupäivä 12.5.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toiminta%20kiristyshaittaohjelmatilanteessa%20-%20johdon%20ohje.pdf.

Kyberturvallisuuskeskus 2022. Tietoturvailmiöt, jotka muuttivat maailmaa. Hakupäivä 7.5.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietoturvailmiot-jotka-muuttivat-maailmaa.

Kyberturvallisuuskeskus 2023. Hakupäivä 12.5.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-nettihuijaukselta.

Microsoft 2024. What is information security infosec? Hakupäivä 21.5.2024. https://www.microsoft.com/fi-fi/security/business/security-101/what-is-information-security-infosec.

Nixu 2023. Ovatko asiakkaidesi tiedot turvassa? Se selviää auditoimalla. Hakupäivä 8.5.2024. https://www.nixu.com/fi/blog/ovatko-asiakkaidesi-tiedot-turvassa-se-selviaa-auditoimalla.

Nordcloud 2024. Kuva 6. What are the advantages of SIEM? Hakupäivä 15.5.2024. https://nordcloud.com/tech-community/advantages-of-siem/.

Opsec 2024. Opsec Oy:n tietoturvapalvelut. Hakupäivä 8.5.2024. https://www.opsec.fi/fi/palvelut/tietoturva/.

Second Nature Security 2024. Miksi henkilöstön tietoturvakoulutus on tärkeää? Hakupäivä 8.5.2024. https://www.2ns.fi/miksi-henkiloston-tietoturvakoulutus-on-tarkeaa/.

SecurityScorecard 2020. What is the Difference Between Information Security and Cybersecurity? Hakupäivä 24.5.2024. https://securityscorecard.com/blog/information-security-versus-cybersecurity/.

SFS 2024. Sosiaali- ja terveydenhuoltoala. Hakupäivä 3.5.2024. https://sfs.fi/osallistu-ja-vaikuta/aihealueet/sosiaali-ja-terveydenhuoltoala/.

SFS 2024. Kuva 3. Terveydenhuollon IT-standardit. Hakupäivä 6.5.2024. https://sales.sfs.fi/fi/index/tietoastandardeista/terveydenhuollonit-standardit.html.stx.

SFS 2020. Kuva 4. Sosiaali- ja terveydenhuoltoala. Hakupäivä 3.5.2024. https://sfs.fi/osallistu-ja-vaikuta/aihealueet/sosiaali-ja-terveydenhuoltoala/.

Sprinto. Kuva 10. NIST 800-53: The Ultimate Guide. Hakupäivä 13.5.2024. https://sprinto.com/blog/nist-800-53-guide/.

Tietosuojavaltuutetun toimisto 2024. Mitä tietosuoja on? Hakupäivä 20.5.2024. https://tietosuoja.fi/tietosuoja.

Tietosuojavaltuutetun toimisto 2024. Usein kysyttyä EU:n tietosuoja-asetuksesta. Hakupäivä 5.5.2024. https://tietosuoja.fi/usein-kysyttya-gdpr.

Theelephantmum 2020. Vastaamo Data Breach: Information and Actions for Victims. Hakupäivä 7.5.2024. https://www.theelephantmum.com/vastaamo-data-breach/.

Valtionvarainministeriö, vahti 2017. Kuva 8. Tietoturvapoikkeamatilanteiden hallinta, s.15. Hakupäivä 7.5.2024. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf?sequence=6&isAllowed=y.

Varonis 2023. NIST 800-53: Definition and Tips for Compliance. Hakupäivä 7.5.2024. https://www.varonis.com/blog/nist-800-53.

Visma 2019. Tietosuoja vai tietoturva? Hakupäivä 20.5.2024. https://www.visma.fi/blog/tietosuoja-tietoturva/.

Yle 2024. Aleksanteri Kivimäelle yli kuusi vuotta vankeutta Vastaamon tietomurrosta – Kivimäki pettynyt. Hakupäivä 7.5.2024. https://yle.fi/a/74-20084812.