



**UNIVERSITY
OF TURKU**

**Kyberturvallisuuden koulutusohjelman
toteuttaminen hoivakotiorganisaatiossa:
Tietoturvakulttuurin kehittäminen NIS2-direktiivin
näkökulmasta**

Tietotekniikan laitos
Diplomityö
Kyberturvallisuusteknologia

Kirjoittaja:
Eetu Laakso

Ohjaajat:
TkT Antti Hakkala
Prof. Jouni Isoaho

19.6.2025
Turku

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu
Turnitin OriginalityCheck -järjestelmällä.

Diplomityö

Tutkinto-ohjelma, oppiaine: Tietotekniikan tutkinto-ohjelma, Kyberturvallisuusteknologia

Tekijä(t): Eetu Laakso

Otsikko: Kyberturvallisuuden koulutusohjelman toteuttaminen hoivakotiorganisaatiossa:

Tietoturvakulttuurin kehittäminen NIS2-direktiivin näkökulmasta

Ohjaaja(t): TkT Antti Hakkala, Prof. Jouni Isoaho

Sivumäärä: 56 sivua

Päivämäärä: 19.6.2025

Työn aiheena on uuden koulutusohjelman käyttöönotto ja vaikutukset NIS2-direktiivin näkökulmasta. Työssä tarkastellaan mahdollisimman hyvää tapaa ottaa käyttöön uusi tietoturvaan ja -suojaan liittyvä koulutus. Lisäksi selvitetään millä tavoin tämä koulutus vaikuttaa organisaation tietoturvakulttuuriin. Tämän lisäksi työssä käydään organisaation NIS2-direktiiviin liittyvä valmius läpi. Näistä muodostuu työn tutkimuskysymykset.

Tutkimuksessa haastateltiin organisaation tietohallintojohtajaa ja toteutettiin kahdelle henkilökunnan tasolle kyselyt. Yhdessä kyselyssä keskityttiin rivihenkilökuntaan ja toisessa keskityttiin yksiköiden johtajiin. Kyselyiden avoimet kysymykset ja haastatteluiden tulokset analysoitiin teema-analyysillä, muu osa kyselyistä analysoitiin yksinkertaisilla tilastollisilla menetelmillä. Tuloksien analyysin ja kevyen kirjallisuuskatsauksen perusteella vastattiin tutkimuskysymyksiin.

Tulokset osoittavat, että uusi koulutus on saatu hyvälle alulle organisaatiossa ja onnistuneesti usean yksilön käyttöön. Kyselytuloksista ilmenee, että uusi koulutus on saanut hyvän vastaanoton henkilökunnalta ja yksiköiden johtajilta. Pilotoinnin perusteella koulutuksen käyttöönotossa havaittiin parannettavaa.

NIS2-haastattelun avulla pyrittiin hahmottamaan organisaation valmiutta täyttää direktiivin vaatimukset. Haastattelun perusteella voidaan todeta, että organisaatiossa on aloitettu valmistautuminen NIS2-direktiivin edellytyksiin. Direktiivin vaatimuksista suurin osa on täytetty, mutta joillakin osa-alueilla, kuten riskienhallinnassa sekä ylimmän johdon vastuun ja roolin määrittelyssä, on vielä kehitettävää.

Avainsanat: Kyberturvallisuus, Kyberturvakulttuuri, NIS2-direktiivi, Tietoturvakoulutus
Terveydenhuolto

Sisällysluettelo

1	Johdanto	1
1.1	Opinnäytetyöprosessiin osallistuvat yritykset	1
1.2	Tausta	1
1.3	Ongelman kuvaus	2
1.4	Tutkimuskysymykset	2
1.5	Tutkimusasetelma	2
1.5.1	Strateginen vaihe	3
1.5.2	Taktinen vaihe	3
1.5.3	Operatiivinen vaihe	4
1.6	Opinnäytetyön rakenne	4
1.7	Tekoälyn käyttö opinnäytetyössä	5
2	Teoreettinen tausta kyberturvallisuudesta terveydenhuollossa	6
2.1	Tietosuoja ja tietoturva	6
2.1.1	Tietosuoja	6
2.1.2	Tietoturva	6
2.2	Terveydenhuollon tietoturvaan ja tietosuojaan liittyvät tärkeimmät voimassa olevat lait ja asetukset	7
2.2.1	Yleinen Euroopan tietosuoja-asetus (GDPR)	7
2.2.2	Verkko- ja tietojärjestelmien turvallisuusdirektiivi 2 (NIS2)	8
2.2.3	Asiakastietolaki (703/2023)	11
2.2.4	Tietosuojalaki (1050/2018)	12
2.2.5	Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) ja Aluevalvontavirasto (AVI) ja Terveyden ja hyvinvoinnin laitos (THL)	12
2.3	Tyypillisiä tietoturva- ja tietosuojariskejä terveydenhuollossa	13
2.3.1	Yleiset tietoturva- ja -suojarikkeet ja niiden jaottelu	14
2.3.2	Tietoturvan ja tietosuojan resurssit terveydenhuollossa	15
2.3.3	WannaCry	16
2.3.4	Vastaamo	17
2.4	Riskienhallinta ja kyberturvallisuuskulttuurin rakentaminen teoriassa	18
2.4.1	Riskienhallinta ja riskienhallinnan mallit ja menetelmät	18
2.4.2	Kyberturvallisuuskulttuurin kehittäminen terveydenhuollon organisaatiossa	20
3	Tietoturva ja -suoja koulutusohjelman toimeenpano ja vaikutukset organisaatiossa	24

3.1	Vanhan tietosuojakoulutuksen kuvaus	24
3.2	Uuden tietoturva ja -suoja koulutuksen toteuttaminen	24
3.3	Johdon rooli koulutusohjelman toteuttamisessa	26
3.4	Palveluyksikön pilotointi ja palautekysely koko henkilökunnalle	28
4	Terveydenhuollon yrityksen NIS2-valmiuden mittaaminen	30
4.1	NIS2 valmiuden mittaamisen viitekehys	30
4.2	Viitekehyksestä luotu haastattelu	31
5	Työn tulokset	32
5.1	Pilotointi ja henkilökunnan kyselyn tulokset	32
5.2	Johtajien kyselyn tulokset	36
5.3	NIS2-haastattelun tulokset	40
5.3.1	Organisaatorakenne ja vastuut	40
5.3.2	Resurssit ja osaaminen	40
5.3.3	Kulttuuri ja tietoturvatietoisuus	41
5.3.4	Kokonaisarvio ja kehitysnäkymät	41
5.4	Tulosten analyysi ja pohdintaa	42
5.4.1	Henkilökunnan kysely	42
5.4.2	Johtajien kysely	43
5.4.3	NIS2-haastattelu	45
5.5	Onnistumisia, parannettavaa ja kehitysehdotuksia	47
5.5.1	Onnistumiset	47
5.5.2	Parannettavaa ja kehitysehdotuksia	48
6	Yhteenveto	50
6.1	Vastaukset tutkimuskysymyksiin	51
6.2	Työn rajoitukset ja tulevaisuuden kehityskohteet	52
	Lähdeluettelo	53
	Liitteet	57
	Liite 1: Palautekysely johtajille uudesta tietosuoja- ja tietoturvakoulutuksesta.	57
	Liite 2: Palautekysely henkilökunnalle uuteen tietoturva- ja tietosuojakoulutukseen	61
	Liite 3: NIS2 valmiuden haastattelukysymykset	65

Liite 4: Henkilöstölle lähetetty kalasteluviesti	68
Liite 5: Tekoälyn käyttö työssä	69

1 Johdanto

Kyberturvallisuuden tilanne maailmalla on vakava ja ENISA:n mukaan Euroopassa on yksinään jo valtava kyberturvallisuuden osaajien vaje [1]. Uudet teknologiat, kuten tekoäly, uhkaavat kyberturvallisuutta täysin uusilla tavoilla kerrotaan ENISA:n vuoden 2024 kyberturvan raportissa [2]. Raportti nostaa Euroopan sisällä tehtyjä toimia kyberturvan parantamiseksi Euroopan tasolla. Yksi tärkeimpinä toimia on sääntelyn lisääminen. Uusina säädöksinä mainitaan koko Eurooppaa koskeva NIS2-direktiivi [3] sekä tekoälyä koskevan säädökset. Nämä vaikuttavat suoraan kyberturvan raportissa nostettuihin moniin uhkiin.

Terveydenhuoltoala on pitkään ollut tilastojen kärjessä tapahtuneiden hyökkäysten ja hyökkäysten yrityksiin suhteen. Hyökkäysten yleisyyteen vaikuttavat useat tekijät, joihin esimerkiksi NIS2-direktiivillä pyritään puuttumaan ja sitä kautta suojaamaan valmiiksi jo heikossa asemassa olevien henkilöiden tietoja.

1.1 Opinnäytetyöprosessiin osallistuvat yritykset

Työ tehtiin yhteistyössä Yrjö ja Hanna säätiön kanssa. Yrjö ja Hanna kodit tarjoavat asumis- ja hyvinvointi palveluita ikäihmisille. Tässä työssä keskitytään Yrjö ja Hanna kotien hyvinvointipalveluiden organisaatioon ja Yrjö ja Hanna säätiöstä jatkossa puhuttaessa tarkoitetaan hyvinvointipalveluiden organisaatiota.

Yrjö ja Hanna säätiön hyvinvointipalvelut koostuvat useista palveluyksiköistä, jotka on suunnattu eri asiakasryhmille, kuten ikääntyneille ja muille erityisryhmille [4]. Hyvinvointipalveluilla on yhteensä 26 yksikköä [4]. Yrjö ja Hanna kotien yksi keskeisimmistä arvoista on kohtaaminen, jota on korostettu erityisesti asumispalveluiden suunnittelussa [5]. Kodit on rakennettu tukemaan yhteisöllisyyttä asukkaiden ja henkilökunnan välille. Tämän vuoksi palveluyksiköissä järjestetään viriketoimintaa, johon osallistuu asukkaiden lisäksi myös henkilökuntaa.

1.2 Tausta

NIS2-direktiivi on jatkoa vuonna 2016 voimaan tulleelle NIS-direktiiville [6]. Sen tavoitteena on ollut taata hyvä kyberturvallisuuden taso sen piiriin kuuluvilla toimialoilla. Alkuperäisen direktiivin ongelmaksi muodostui se, ettei sen täytäntöönpanoa määritelty riittävän tarkasti. Tämän seurauksena NIS-direktiiviä on EU:n jäsenvaltioissa sovellettu eri tavoin, mikä on heikentänyt sen kykyä taata tasavertainen kyberturvallisuuden taso koko Euroopassa [7].

1.3 Ongelman kuvaus

Tulevaisuudessa kyberturvallisuuden merkitys kasvaa entisestään, sillä digitalisaatio ja uudet teknologiat, kuten tekoäly, kiihdyttävät yhteiskunnan digitalisaatiota, eikä terveydenhuolto tee tässä poikkeusta. Turvallinen ja vastuullinen toiminta korostuu yhä entisestään terveydenhuollossa digitalisaation tuoman muutoksen myötä.

Kyberturvallisuuden merkityksen lisääntyessä, myös kyberturvallisuuskoulutuksen vaikutus kasvaa. Uuden NIS2-direktiivin myötä siirrytään kohti tiukkenevaa lainsäädäntöä, joka edellyttää muun muassa kyberturvakoulutuksen järjestämistä. Henkilökunta terveydenhuollossa käsittelee kriittisiä tietoja. On erityisen tärkeää, että heidän tietonsa ja ymmärryksensä kyberturvallisuutta kohtaan ovat käsittelyn vaatimalla tasolla.

Terveydenhuollon ensisijainen tavoite on tuottaa terveyttä, jolloin muut kuin hoitotyön tehtävät saattavat jäädä vähemmälle. Suomessa on ollut pitkään keskusteltu sote-uudistuksesta, sen resursseista ja erityisesti hoitajamitoituksista. Käyty keskustelu osoittaa, että jo valmiiksi niukoilla resursseilla on vaikea vastata työympäristön digitalisoinnin tuomiin uusiin vaatimuksiin.

1.4 Tutkimuskysymykset

Tutkimuskysymyksiä työssä on yhteensä kolme.

TK1: Millä tavoin voidaan mahdollisimman hyvin ottaa käyttöön uusi koulutusohjelma?

TK2: Onko uudella koulutuksella havaittavissa vaikutuksia kyberturvallisuuskulttuurin edistymiseen hoivakotiyrityksessä?

TK3: Kuinka hyvin hoivakotiorganisaatio on valmistautunut NIS2:een?

1.5 Tutkimusasetelma

Wohlin ja Aurum [8] ovat tutkineet artikkelissaan hyviä käytänteitä, joilla suorittaa tutkimus. He esittelevät useita tärkeitä päätöskohtia, jotka pitää ottaa huomioon tehdessään tutkimusta tietystä aiheesta. Niiden tarkoituksena on tukea sopivimpien menetelmien ja lähestymistapojen, päättelylogiikan ja aineistonanalyysin valintaa. Päätöskohtia on yhteensä kahdeksan. Tässä luvussa käydään läpi kyseiset kohdat, ja perustellaan niiden avulla valitut tutkimusmenetelmät.

Wohlin ja Aurum jakavat päätöskohdat kolmeen eri vaiheeseen [8]. Vaiheet ovat tutkimuksen strateginen vaihe, joka käsittää päätöskohdat 1–4, taktinen vaihe, joka käsittää kohdat 5 ja 6 ja lopuksi tulee vielä tutkimuksen operatiivinen vaihe.

1.5.1 Strateginen vaihe

Tutkimuksen strateginen vaihe koostuu päätöskohdista 1–4 ja sen tavoitteena on päättää mitä tutkitaan ja miksi. Tässä vaiheessa käsiteltäviä päätöskehtia ovat tutkimuksen tavoite, eli onko kyseessä uuden tiedon etsiminen vai käytetäänkö jo olemassa olevaa tietoa ratkaisemaan jokin käytännön ongelma, huomioidaan tutkimuksen tarkoitus, valitaan päättelytapa ja tutkimusfilosofia.

Tämä diplomityö perustuu kirjallisuuteen ja käyttää siinä esitettyä NIS2-direktiivin viitekehystä. Työ on siten käytännönläheistä, eikä uuden tiedon etsimistä. Tutkimuksen tarkoituksena on kartoittaa hoivakodin palveluyksiköiden nykytilaa tietoturvan ja NIS2-direktiivin valmiuden osalta, sekä soveltaa havaintoja teoriaan, eli toteuttaa tutkimusta induktiivisesti.

1.5.2 Taktinen vaihe

Strategisen vaiheen jälkeen siirrytään tutkimuksen taktiseen vaiheeseen, jossa keskitytään siihen, miten tutkimus toteutetaan. Tähän vaiheeseen kuuluu päätöskohdat 5 ja 6, jotka ovat tutkimuksen prosessi eli miten tietoa kerätään sekä tutkimusmenetelmä, eli millä tavoin tutkimus toteutetaan.

Tutkimusprosessi tarkoittaa keinoja, joilla tutkimustietoa kerätään [8]. Tässä työssä tietoa kerätään kyselyillä, jotka sisältävät valinta- ja monivalintakysymyksiä, Likert-asteikollisia väittämiä ja avoimia kysymyksiä. Näiden lisäksi työssä käytetään puoliavoimaa haastattelua, jossa kysymykset on jaettu haastateltavalle etukäteen haastatteluun valmistautumista varten. Näin ollen tutkimuksessa tiedon keräämiseen käytetään kvalitatiivisia sekä kvantitatiivisia menetelmiä.

Tutkimusmenetelmä määrittää, millä keinoin tutkimus tehdään. Tämä tutkimus on toteutettu yhdessä Yrjö ja Hanna -hyvinvointipalveluiden organisaation kanssa. Se täyttää tapaustutkimuksen (case study) tunnusmerkit, joihin kuuluu mm. yksittäisen tai useamman tapauksen tarkastelu [8]. Tässä tapauksessa tutkimus kohdistuu useisiin palveluyksiköihin saman organisaation sisällä, mikä vastaa hyvin tapaustutkimuksen määritelmää.

1.5.3 Operatiivinen vaihe

Aikaisemmissa päätöskohdissa määriteltiin mitä tutkitaan ja miten tutkimus toteutetaan. Wohlinin ja Aurumin [8] jaottelun mukaan operatiivisessa vaiheessa valitaan, millä tavoilla tietoa kerätään sekä menetelmät, joilla kerättyä aineistoa analysoidaan. Tässä vaiheessa päätetään, mitkä aineistonkeruu- ja analyysimenetelmät tutkimuksessa ovat käytössä.

Aineistonkeruussa hyödynnettiin kvantitatiivisia ja kvalitatiivisia menetelmiä. Tietoa kerättiin kyselyillä, jotka sisälsivät valintakysymyksiä, avoimia kysymyksiä ja Likert-asteikollisia väittämiä. Näiden lisäksi tietoa kerättiin myös haastattelulla. Aineisto analysoitiin sekä laadullisilla että määrällisillä menetelmillä. Laadullisessa analyysissä käytettiin teema-analyysia ja määrällisessä analyysissä hyödynnettiin yksinkertaistettua tilastollista tarkastelua.

1.6 Opinnäytetyön rakenne

Tämän opinnäytetyön rakenne on seuraava. Ensimmäisessä kappaleessa esitellään aihe ja aiheen taustaa, avataan työssä käytettyjä tutkimusmenetelmiä, sekä esitellään tarkemmin työn rakenne ja mainitaan työn tekemisessä mukana olleet yritykset.

Toinen luku toimii kevyenä kirjallisuuskatsauksena. Aluksi käsitellään perustietoa kyberturvallisuudesta, kuten mitä se on ja miten se rakentuu. Sen jälkeen siirrytään tarkastelemaan terveydenhuollon toimialaa ja siihen liittyvää lainsäädäntöä, joka määrittää tietoturvan ja tietosuojan vaatimuksia terveydenhuollossa. Lopuksi tarkastellaan terveydenhuoltoalan kyberturvariskejä ja riskienhallinnan perusteita.

Kolmannessa luvussa siirrytään tarkastelemaan käytäntöön vietyä koulutusta. Aluksi kuvataan mitä koulutuksen vaihdos tuo Yrjö ja Hanna hyvinvointipalveluiden organisaatiolle. Tämän jälkeen esitellään uuden koulutuksen toteutuksen vaiheet ja pilotointi organisaatiossa.

Neljäs luku esittää, miten organisaation NIS2-valmiutta mitataan. Siinä esitellään Alwin Van Welien kehittämä viitekehys, joka auttaa arvioimaan NIS2-direktiivin vaatimusten ja todellisten toimien suhdetta.

Viidennessä luvussa käydään läpi työn tulokset. Aluksi esitellään tulokset sellaisenaan ilman tulkintaa ja tulosten pohdinta tapahtuu aliluvussa 5.4, jossa analysoidaan tulosten merkitys laajemmin ja pohditaan työn onnistumisia ja kehityskohteita tulevaisuutta varten.

Kuudes luku on yhteenvetoluku, jossa vastataan työn tutkimuskysymyksiin tulosten perusteella. Lisäksi luvussa kootaan yhteen työn tärkeimmät tulokset ja avataan työn tuloksien yleistettävyyttä ja käyttöä tulevaisuudessa. Alaluvussa 6.2 käsitellään työn rajoituksia ja esitetään kehitysehdotuksia tulevaisuuden tutkimukseen tai käytännön soveltamista varten.

1.7 Tekoälyn käyttö opinnäytetyössä

Tämän opinnäytetyön laatimisessa on käytetty rajatusti apuna tekoälyä. Käytössä on ollut ChatGPT versio 4. Sitä on hyödynnetty yksittäisissä kohdissa, kuten lauserakenteiden selkeyttämisessä, sisällöllinen vastuu tekstistä on tekijällä. Lisäksi tekoälyä on käytetty lähdeluettelon muotoilussa viittaustyylin mukaan. Käytetty kehote lähdeluettelon muokkaamiseen sekä ChatGPT:n vastaus löytyvät liitteestä 5.

2 Teorettinen tausta kyberturvallisuudesta terveydenhuollossa

Luvussa käydään läpi kyberturvallisuuden teoreettista taustaa. Aluksi perehdytään tietosuojaan ja tietoturvaan sekä selvennetään näiden käsitteiden välinen ero. Tämän jälkeen tarkastellaan aiheeseen liittyviä lakeja ja asetuksia. Keskiössä on uusi NIS2-direktiivi, joka tuli voimaan marraskuussa 2024 [3]. Lainsäädäntöosuuden jälkeen siirrytään tyypillisiin tietoturva- ja tietosuojariskeihin terveydenhuollossa sekä keinoihin niiden hallitsemiseksi. Luvun lopussa esitellään kirjallisuudesta esiin nousseita tapoja kyberturvallisuuskulttuurin kehittämiseen.

2.1 Tietosuoja ja tietoturva

2.1.1 Tietosuoja

Tietosuoja ja tietoturva ovat molemmat erittäin tärkeitä terveydenhuollossa. Ne liittyvät toisiinsa, mutta eivät ole sama asia. Tietosuojavaltuutetun toimiston mukaan tietosuojalla tarkoitetaan yleensä omien henkilötietojen suojaa ja oikeutta sanella niiden käyttöä [9]. Tietosuojaa säädellään useilla laeilla ja asetuksilla.

Euroopan tunnetuin tietosuojaa koskeva säädös on yleinen tietosuoja-asetus (GDPR), joka on voimassa kaikissa EU-maissa. Asetus luo yhtenäisen perustan henkilötietojen käsittelylle ja turvaa yksilön tietosuojan koko unionin alueella. GDPR:n yhtenä tavoitteena on varmistaa eurooppalaisten henkilötietojen suojaaminen ja tietojen vapaa liikkuminen Euroopan sisällä [10].

Terveydenhuollon kontekstissa tietosuoja on tärkeä ottaa huomioon [11]. Terveydenhuollon asiakkaat voivat olla terveytensä tai ikänsä puolesta haavoittuvassa asemassa, minkä vuoksi heidän tietosuojansa edellyttää erityistä huolellisuutta. Käytännössä tämä voi tarkoittaa tiedon käytön rajaamista vain välttämättömään ja asettamalla tiedolle selkeät käyttöoikeudet. Tietosuojaan liittyy tietosuojavastaavan asiantuntijarooli, jonka tehtävänä on seurata organisaatiossa tietosuojasäännösten noudattamista, sekä henkilötietojen käsittelyä [12]. Ongelmatilanteissa tai viranomais selvittelyissä tietosuojavastaava toimii linkkinä yrityksen ja valvontaviranomaisten välillä.

2.1.2 Tietoturva

Tietoturva viittaa teknisiin ja organisaation sisäisiin toimiin, joilla pyritään suojaamaan arkaluonteista tietoa estämällä asiattomien pääsy tietoihin ja varmistamalla tiedon eheys ja

saatavuus [13]. Tiedon turvaamisen perusta on rakennettu CIA:n kolmikon päälle. Kolmikko muodostuu kolmesta periaatteesta, jotka ovat luottamuksellisuus (C), muuttumattomuus (I) ja saatavuus (A). Näiden toteutuminen on välttämätöntä, jotta tieto säilyy järjestelmässä turvassa ja hyödynnettävissä tarpeen mukaan [14].

Tietoturva toteutetaan lukuisin teknisin, hallinnollisin ja organisatorisin keinoin. Yhdysvaltain kansallisen standardointi- ja teknologiainstituutin (NIST) raportissa ”An introduction to information security” nämä keinot on jaoteltu teemoittain niin sanottuihin ”perheisiin” [13]. Yksi tällainen perhe on esimerkiksi pääsynhallinta (access control), joka kattaa erilaisia toimenpiteitä käyttäjien pääsyoikeuksien hallitsemiseksi. Näihin kuuluvat muun muassa käyttäjätilien asianmukainen hallinta ja vähimmän oikeuksien taso kaikille käyttäjille.

Raportissa on nimetty yhteensä 20 erilaista perhettä. Nämä perheet kukin sisältävät konkreettisia ratkaisuja tietoturvan takaamiseksi. Laajasti käytettyjä teknisiä tietoturvan tapoja ovat esimerkiksi erilaiset salausjärjestelmät, VPN-yhteydet etätyössä, monivaiheinen tunnistautuminen, verkon suojaus ja segmentointi palomureilla [13]. Nämä kaikki mainitut ovat yleisesti käytössä terveydenhuollossa.

NIST mainitsee käyttäjän inhimillisen toiminnan yleisesti heikoimpana lenkkinä [13]. Tämä ilmenee erityisesti sosiaaliseen manipulaatioon perustuvina hyökkäyksinä, kuten huijaus- ja kalasteluviesteinä, joita kohdistetaan erityisesti terveydenhuollon organisaatioita kohtaan [15]. Tällaiset hyökkäykset korostavat sitä, että vaikka tietoturvan hoitamiseen on paljon tekniikkaa, käyttäjän roolia ei voida sivuuttaa, sillä tekniikka on vain yhtä vahva kuin sen käyttäjä.

2.2 Terveydenhuollon tietoturvaan ja tietosuojaan liittyvät tärkeimmät voimassa olevat lait ja asetukset

Terveydenhuollon toimintaa ohjaa Suomessa useat kansalliset, ja EU-tason lait sekä asetukset. Näiden säädösten tarkoituksena on varmistaa, että terveydenhuollon henkilöiden ja asiakkaiden asiakirjoja tulee käsitellä siten, että käsittely on laillista, turvallista ja läpinäkyvää.

2.2.1 Yleinen Euroopan tietosuoja-asetus (GDPR)

Yleinen tietosuoja-asetus (GDPR) on EU:n laajuinen asetus siitä, miten henkilön henkilötietoja kerätään ja käsitellään [10]. GDPR astui voimaan toukokuussa 2018. Se säädettiin yhdenmukaistamaan henkilötietojen käsittelyä EU:n alueella, sekä vahvistamaan yksilöiden oikeuksia henkilötietojen hallintaan. Tavoitteena oli lisätä läpinäkyvyyttä tietojen keräämisessä

ja käytössä, sekä antaa kansalaisille paremmat mahdollisuudet valvoa omien tietojensa käsittelyä.

Euroopan yleinen tietosuoja-asetus (GDPR) edellyttää, että henkilötietoja tulee käsitellä lainmukaisesti, kohtuullisesti ja läpinäkyvästi [10]. Yksi tietosuoja-asetuksen keskeisistä tavoitteista on varmistaa, että henkilötietoja käsitellään vain laillisella ja perustellulla perusteella. Tiedot voidaan kerätä rekisteröidyn suostumuksella tai laillisella oikeusperustan nojalla [10]. Lisäksi GDPR edellyttää, että tiedot on pidettävä ajan tasalla aina kun se on mahdollista.

GDPR asettaa organisaatioille tietosuojaan liittyviä velvoitteita, ja niiden rikkominen voi johtaa huomattaviin seuraamuksiin, kuten sakkoihin. Sakot voivat nousta jopa 20 miljoonaan euroon tai 4 %:n edellisen tilikauden maailmanlaajuisesta liikevaihdosta sen mukaan kumpi summa on suurempi [10]. Suomessa yksi viimeaikaisista merkittävistä esimerkeistä on Verkkokauppa.com:lle määrätty seuraamusmaksu [16]. Yhtiölle määrättiin 856 000 euron suuruinen sakko tietosuoja-asetuksen rikkomisesta.

2.2.2 Verkko- ja tietojärjestelmien turvallisuudirektiivi 2 (NIS2)

Verkko- ja tietojärjestelmien turvallisuudirektiivi 2 eli NIS2 on Euroopan parlamentin antama asetusta [3]. Se on säädetty vuonna 2022 ja sen voimaantulopäivä oli Euroopassa 17.10.2024 [3]. Suomessa asetuksen käsittely eduskunnassa viivästyivät alkuperäisestä aikataulusta. Direktiivin velvoitteet ovat sen jälkeen tulleet vaiheittain voimaan.

Ensimmäiset direktiivin velvoitteet ovat tulleet voimaan vaiheittain alkaen poikkeamien ilmoittamisvelvollisuudesta. Traficomien tiedotteen mukaan poikkeamien ilmoittaminen on alkanut 8.4.2025 [17]. Samassa tiedotteessa on päivitetty myös muita määräaikoja, jotka ovat muuttuneet aiemmasta aikataulusta. Ilmoitus kuulumisesta keskeisiin tai tärkeisiin toimijoihin on tullut lähettää viranomaiselle 8.5.2025 mennessä. Riskienhallinnan toimintamalli tulee olla laadittuna 8.7.2025 mennessä. Terveystieteiden valvova viranomainen on Valvira. Kaikki keskeiset päivämäärät ja niihin liittyvät toimet on koottu taulukkoon 1.

Taulukko 1. NIS2-direktiivin liittyvät päivämäärät

Päivämäärä	Tapahtuma
17.10.2024	Direktiivin voimaantulo EU:ssa
8.4.2025	Ilmoitusvelvollisuus omalle valvovalle viranomaiselle poikkeamista
8.5.2025	Ilmoitus omalle valvovalle viranomaiselle kuulumisesta direktiivin toimijoihin
8.7.2025	Riskienhallintamallien luominen yritykselle

Uuden asetuksen taustalla on tavoite parantaa kyberturvallisuutta Euroopan Unionin jäsenmaissa. NIS2-direktiivi korvaa aikaisemmin voimassa olleen Network and information security -direktiivin. Uuden direktiivin on tarkoitus parantaa erityisesti kriittisillä aloilla toimivien yritysten kykyä torjua kyberuhkia ja hallita riskejä.

Uusi NIS2-direktiivi laajentaa aiemman direktiivin soveltamisalaa ja tuo lisää toimialoja sääntelyn piiriin. Se kattaa kriittiset ja tärkeät toimialat. Taulukossa 2 on esitetty kriittiset alat ja tärkeät toimialat taulukossa 3.

Taulukko 2. NIS2-direktiivin kriittiset toimialat

Toimiala	Toimialan osa
Energia	Sähkö, kaukolämmitys ja jäähdytys, öljy, kaasu vety
Liikenne	Ilmaliikenne, raideliikenne vesiliikenne tieliikenne
Pankkitoiminta	
Finanssimarkkinoiden infrastruktuurit	
Terveys	
Juomavesi	
Jätevesi	
Digitaalinen infrastruktuuri	
Tieto- ja viestintä tekniikan palvelujen hallinta (yritysten välinen)	
Julkishallinto	
Avaruus	

Taulukko 3. NIS2-direktiivin tärkeät toimialat.

Toimiala	Toimialan osa
Posti ja Kuriiripalvelut	
Jätehuolto	
Kemikaalien valmistus, jakelu ja tuotanto	
Elintarvikkeiden tuotanto, jalostus ja jakelu	
Valmistus	Lääkinnälliset laitteet ja in vitro diagnostiikkaan käytetyt lääkinälliset laitteet, Tietokoneiden sekä elektronisten ja optisten tuotteiden valmistus, Sähkölaitteiden valmistus, Muiden koneiden ja laitteiden valmistus, Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus, Muiden kulkuneuvojen valmistus
Digitaaliset palvelujen tarjoajat	
Tutkimustoiminta	

Direktiivi velvoittaa näihin toimialoihin kuuluvia yrityksiä ja organisaatioita parantamaan tietoturvaa ja sen käytänteitä. Artikloissa 21, 23 ja 26 määritellään tarkemmin käytännön vaatimuksia, jotka koskevat erityisesti kriittisiin toimijoihin kuuluvia ja tietyin ehdoin myös tärkeitä toimijoita [3].

Artikla 21 luettelee joukon teknisiä ja organisatorisia toimia, joiden tavoitteena on suojata verkkoja sekä laitteiden fyysistä koskemattomuutta [3, Art. 21]. Osa mainituista toimista on muun muassa:

- Riskianalyysit ja tietojärjestelmän turvallisuutta koskevat politiikat
- Poikkeamien käsittely
- Toiminnan jatkuvuuden hallinta ja varmistus, sekä kriisinhallinta
- Toimitusketjujen turvallisuus
- Perustason kyberhygieniasäännöt ja kyberturvallisuuskoulutus
- Henkilöstöturvallisuus, pääsynhallinta, sekä omaisuudenhallinta
- MFA tai jatkuvan todennuksen ratkaisut

Artikla 23 keskittyy tietoturvapoikkeamien ilmoitusmenettelyyn. Organisaation on ilmoitettava merkittävästä tietoturvaloukkauksesta kansalliselle CSIRT-viranomaiselle 24 tunnin kuluessa tietoturvaloukkauksen havaitsemisesta [3, Art. 23]. Ilmoitusvelvollisuus koskee tapahtumia, jotka vaikuttavat tai voivat vaikuttaa henkilöihin aiheuttaen huomattavaa aineellista tai aineetonta vahinkoa tai vakavia häiriöitä organisaation toimintaan. Ilmoitusprosessi jatkuu vaiheittain tapahtuman jälkeen poikkeamailmoituksella 72 tunnin kuluttua tapahtuneesta ja lopullisella raportilla kuukauden kuluttua tapahtumasta [3, Art. 23]. Taulukossa 4 esitetään määräajat, ilmoitustyypit sekä kunkin ilmoituksen edellyttämät toimenpiteet.

Taulukko 4. NIS2-direktiivin ilmoitusvelvollisuudet merkittävän kyberturvapoikkeaman jälkeen

Aikaraja havainnosta	Ilmoitus	Toimenpiteet
24 tuntia	Ennakoilmoitus	Ilmoitus CSIRT-viranomaiselle poikkeamasta.
72 tuntia	Poikkeamailmoitus	Päivitetään ennakoilmoituksen tiedot ja annetaan ensimmäinen arvio tapahtuman vakavuudesta.
1 kuukausi	Yksityiskohtainen raportti	Tapahtumien kokonaiskuvaus, juurisyyn esittely tapaukselle ja tehdyt toimenpiteet, sekä tapahtuneen vaikutuksen arviointi

Direktiivissä mainitaan mahdollisuus määrätä uhkasakko artiklassa 26, mikäli näitä artiklassa 21 mainittuja toimenpiteitä ei suoriteta yrityksessä [3, Art. 26]. Kriittisten toimijoiden osalta sakon enimmäismäärä on 10 000 000 euroa tai vastaavasti 2 % yrityksen vuotuisesta liikevaihdosta. Tärkeille toimijoille vastaavat enimmäissakot ovat maksimissaan 7 000 000 euroa tai enimmillään vähintään 1,4 % vuotuisesta liikevaihdosta.

2.2.3 Asiakastietolaki (703/2023)

Asiakastietolaki säätelee sähköisten potilashoitajärjestelmien käyttöä, tietojen käsittelyn turvallisuutta sekä yhteentoimivuutta muiden järjestelmien kanssa [18]. Lain tavoitteena on varmistaa, että asiakastietoja käsitellään turvallisesti ja standardoidulla tavalla kaikissa tilanteissa. Lain keskeisimpiä vaatimuksia laitteistoille on, että ne tulee suunnitella siten, että ne kykenevät jakamaan tietoa luotettavasti eri toimijoiden välillä. Esimerkki tällaisesta järjestelmästä on suomalainen Kanta-palvelu, joka mahdollistaa tiedonvaihdon eri terveydenhuollon yksiköiden välillä.

Lain mukaan potilastiedot on pidettävä suojattuja käyttäen asianmukaista tietoturvaa. Tämä voi tarkoittaa erilaisia tietoturvatoukkoja, kuten kulunvalvontaa tai henkilökohtaisia tunnuksia järjestelmiin käyttäen monivaiheista tunnistautumista. Lisäksi järjestelmästä tulee löytyä lokitiedot siitä, kuka tarkastellut tietoja sekä milloin ja mitä tietoja on tarkasteltu [18].

Asiakkaalla on oikeus tietää, mitä tietoja hänestä tallennetaan ja oikeus tarkistaa tietojen oikeellisuus [18]. Tietyissä tapauksissa henkilöllä on oikeus halutessaan rajoittaa häntä koskevien tietojen näkyvyyttä, kuten sähköisten reseptien tietoja.

Esimerkiksi akuutissa hoitotilanteessa, kuten sydänkohtauksessa henkilö joutuu hoivakodista sairaalaan. Hoitavan lääkärin tulee päästä nopeasti käsiksi potilaan lääkitystietoihin, jotta hoito voidaan toteuttaa turvallisesti. Yhteentoimivat digitaaliset järjestelmät mahdollistavat tiedonvälityksen terveydenhuollon yksiköiden välillä. Samalla pystytään varmistamaan tietosuojan toteutuminen, sillä tietojen käytöstä jää tieto järjestelmän lokitietoihin, mikä tuo läpinäkyvyyttä tietojen käyttöön.

2.2.4 Tietosuojalaki (1050/2018)

Tietosuojalaki on GDPR:n ohella yksi tärkeimmistä laeista, jotka koskevat yksilöiden oikeuksia tietoihin tai tietosuojaan. Tämä laki täydentää Euroopan laajuista GDPR:ää [19] ja on melko uusi, se on säädetty vuonna 2019. Lain keskeisiä näkökohtia ovat lasten tietosuoja sekä työntekijöiden tietosuoja työsuhteessa sekä eräät erityistapaukset, joissa tätä lakia ei sovelleta, yhtenä tapauksena kansallinen turvallisuus.

Tietosuojalaki sanelee myös tietosuojavaltuutetun erilaiset odotukset ja tehtävät [19]. Tehtäviin kuuluu tietosuojarikkomusten tutkiminen tai järjestöjen tai kansalaisten neuvoston antaminen ja sakkojen tai muiden seuraamusten määrääminen tietosuojarikkomuksista. Laki määrää tarvittaessa myös yhteistyöstä muiden maiden oikeusasiamiesten kanssa.

Tietosuojalain tavoitteena on tarjota entistä parempi hallinta yksityisen tiedon, kuten henkilön tunnistamiseen johtavan tiedon käsittelyyn. Tämä kohta on suunnattu erityisesti organisaatioille sen varmistamiseksi, että tällaisten tietojen käsittely tapahtuu säännösten mukaisesti ja läpinäkyvästi. Tämä on erityisen tärkeää sosiaali- ja terveysalalla. Tämä johtuu siitä, että potilastiedoissa on arkaluonteista tietoa [20]. Hoivakotiorganisaatioon asiakkaan muuttaessa annetaan tietosuojaseloste asiakkaalle, jonka perusteella asiakas tietää mitä tietoja hänestä kerätään.

2.2.5 Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) ja Aluevalvontavirasto (AVI) ja Terveiden ja hyvinvoinnin laitos (THL)

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) ja aluehallintovirasto (AVI) ovat kaksi viranomaista, jotka valvovat, että edellä mainittuja lakeja noudatetaan Suomen

terveydenhuollossa. Nämä kaksi ovat eriarvoisessa asemassa. Valvira toimii valtakunnallisesti koko Suomea koskevilla asioilla. Se valvoo, että potilas- ja asiakastietokantajärjestelmät täyttävät vaatimukset [15]. AVI toimii yleisesti paikallisella alueella ja sillä onkin useita virastoja ympäri Suomi [21].

Suurin osa tapauksista päättyy ensin AVI:lle. Jos tapaus koskee koko Suomea, tai AVI tarvitsee apua sen selvittämisessä, silloin Valvira puuttuu asiaan [22]. Valvira korostaa valvonnan merkitystä laadukkaiden ja turvallisten palvelujen varmistamisessa [16]. Tämä rakentuu kolmelle keskeiselle periaatteelle, jotka ovat vastuullisten toimintatapojen vahvistaminen, valvonnan yhdenmukaisuuden ja tasapuolisuuden varmistaminen sekä tiedon hyödyntäminen vaikuttavassa valvonnassa.

Aluehallintovirastot Suomessa vastaavat yhdessä Valviran kanssa siitä, että heidän asiakkaansa saavat laadukasta, oikea-aikaista ja riittävän tasokasta palvelua [23]. AVI toimii yhteistyössä paikallisten toimijoiden kanssa, joita se pyrkii ohjeistamaan ja tukemaan. AVI antaa myös määräyksiä esimerkiksi hoitajamitoitukseen, eli siitä, kuinka paljon hoitajia tarvitsee olla kulloinkin vuorossa suhteessa asukkaiden lukumäärään [24].

Tietoturvan ja -suojan osalta AVI valvoo yhdessä Valviran kanssa sitä, että terveydenhuollossa yleisesti asiakkaiden tietoja käsitellään tietosuojan edellyttämällä tavalla. Jos AVI huomaa yksikön toiminnassa puutteita tai rikkeitä, voi se antaa tarkastuksen kohteena olevalle taholle korjauskehotuksen asian hoitamiseksi.

Terveyden ja hyvinvoinninlaitos (THL) toimii puolestaan kansallisena asiantuntijavirastona, joka tukee terveydenhuollossa muun muassa tiedonhallintaa ja ohjausta. THL voi antaa määräyksiä, joilla täydennetään lainsäädäntöä. THL:n määräys 3/2024 [25] velvoittaa sosiaali- ja terveydenhuollon yksiköitä laatimaan tietoturvasuunnitelman, joka kattaa riskienhallinnan ja sen lisäksi muita teemoja, kuten koulutuksen järjestämisen. THL:n määräyksessä korostetaan, että työntekijän tulee saada koulutusta ja tietoturvaosaaminen täytyy varmistaa.

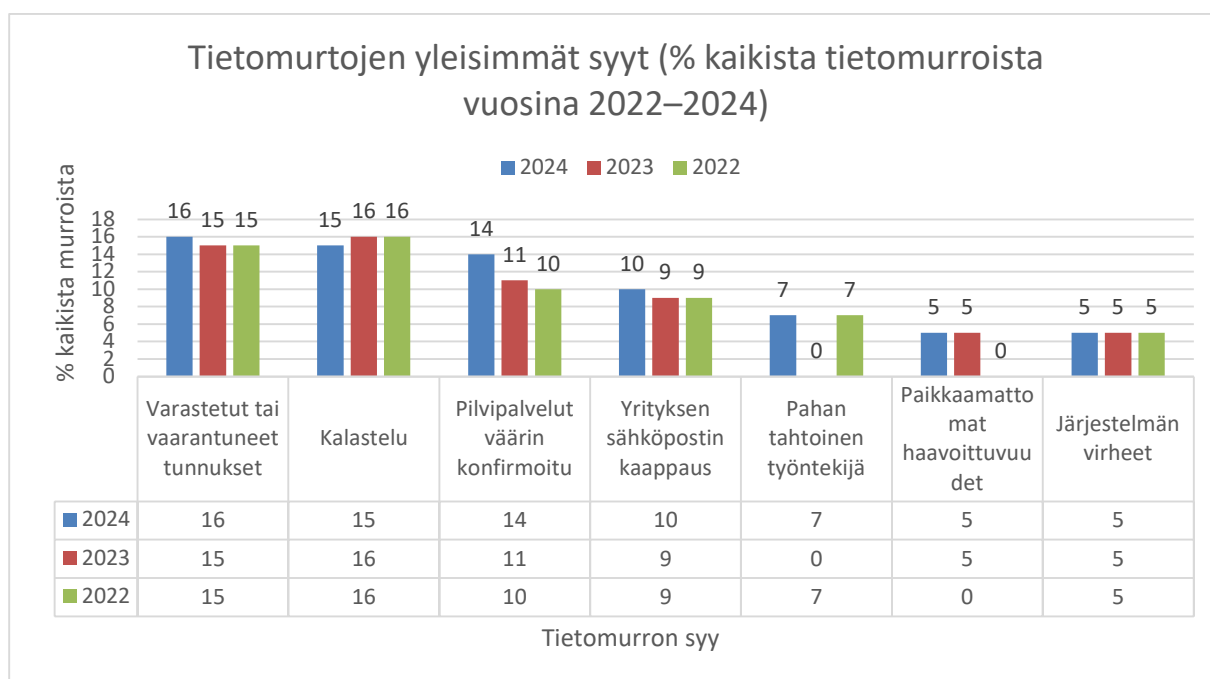
2.3 Tyypillisiä tietoturva- ja tietosuojariskejä terveydenhuollossa

Tässä aliluvussa tarkastellaan tyypillisiä riskejä, joita terveydenhuollossa mahdollisesti esiintyy. Aluksi tarkastellaan kirjallisuuden perusteella tunnistettuja yleisiä riskejä. Näiden yleisten riskien jälkeen siirrytään tapauskohtaisiin esimerkkeihin aiemmista tietoturvaloukkauksista terveydenhuollon alalla. Aikaisemmista tapahtumista käsitellään

WannaCry-kiristyshaittaohjelman aiheuttama hyökkäys, sekä Vastaamon tietomurron tapaus, joissa molemmissa ilmenee rikkeitä tietoturvaa ja tietosuoja kohtaan.

2.3.1 Yleiset tietoturva- ja -suojarikkeet ja niiden jaottelu

Yleisiä tietoturvaan ja -suojaan liittyviä toteutuneita riskejä on lueteltu IBM:n vuosiraporteissa [15], [26], [27]. Raporteista käy ilmi, että suurin osa tietoturvaloukkauksista on peräisin inhimillisistä tekijöistä. Kuvaaja 1 on koottu yleisimpiä keinoja, joilla tietomurrot ovat saaneet alkunsa vuosien 2022, 2023 ja 2024 aikana. Kaikkein tyypillisimmät tavat ovat kaikkien vuosien raporteissa varastetut tai vaarantuneet käyttäjien tunnukset, sekä tunnusten kalastelu ja sitä kautta tunnuksien vaarantuminen.



Kuvaaja 1: Kuvaajassa esitetty vuosina 2022, 2023 ja 2024 tyypillisimmät tietomurtojen aiheuttajat prosentteina kaikista tietomurroista. Kuvaajan tiedot on koottu IBM:n vuosiraporteista [15], [26], [27].

Kalastelulla tarkoitetaan haitallisten sähköpostien lähettämistä, siten, että ne vaikuttavat tulevan luotettavasta lähteestä [28, ss. 167–168], [29, ss. 3–4]. Hadnagy ja Wozniakin kirjan ”Social engineering: The science of human hacking” mukaan kalastelun tavoitteiksi määritellään järjestelmään pääsyn saaminen, käyttäjätunnuksien ja salasanojen tavoittelu sekä muun hyödyllisen tiedon kerääminen tulevia hyökkäyksiä varten [28, ss. 167–168]. Kirjassa käydään läpi keinoja ihmisten harhauttamiseen ja manipuloimiseen. Näitä keinoja ovat esimerkiksi

auktoriteetin hyödyntäminen, velvollisuudentunteen luominen, sekä kiireen tunteen aiheuttaminen [28].

Auktoriteetin käyttämisestä kirjassa mainitaan, että auktoriteettiasemassa oleva henkilö saa toisen tekemään helpommin pyydettyjä tekoja [28, s. 100]. Esimerkkeinä kirjassa käytetään vanhemman ja lapsen suhdetta, sekä armeijan kersanttia-alainen asetelmaa. Molemmissa konteksteissa on selvä auktoriteettiasema, joka saa toisen osapuolen toimimaan toisen haluamalla tavalla.

Velvollisuuden tunto ja kiire voivat yhdessä aiheuttaa paineentunnetta työntekijälle [28, ss. 98–100]. Kirjassa kuvatussa todellisessa tilanteessa käytettiin molempia yhdessä, joiden avulla onnistuttiin erehdyttämään henkilö tekemään vastoin tämän ohjeita. Esimerkissä yhtiön toimitusjohtajan alaista erehdytettiin päästämään vieras henkilö toimitusjohtajan toimistoon korjaamaan tietokonevirusta käyttämällä näitä molempia suostuttelun apuna.

Terveydenhuollossa tietojen kalastelu on merkittävin tietoturvaloukkauksien ja -murtojen aiheuttaja [30]. Samanlainen havainto toistuu IBM:n laatimissa vuosiraporteissa. Nifakos ym. [30] käyvät systemaattisesti katsausartikkelissaan läpi terveydenhuollossa esiintyviä kyberturvariskejä. Kalastelun lisäksi vakavimmiksi riskeiksi nostetaan tekniset haavoittuvuudet, kuten vanhentuneet järjestelmät ja kiristysohjelmat. Muita keskeisiä riskejä ovat työntekijöiden aiheuttamat tietovuodot ja riittämätön riskienhallinta, puutteellinen kyberturvallisuuskoulutus sekä heikko kyberturvakulttuuri.

Tietoturvahkien jaottelu voidaan tehdä useammalla tavalla. NIST:n dokumentaatioihin perustuen uhat jaettaisiin niiden syntymekanismien perusteella neljään eri kategoriaan [13], [31]. Nämä kategoriat voivat auttaa yritystä kohdentamaan toimia tietyn uhan syntyperän mukaan. Tässä työssä keskitytään ihmislähtöisiin uhkiin, sillä niihin voidaan koulutuksen ja kulttuurin parantamisen myötä vaikuttaa.

2.3.2 Tietoturvan ja tietosuojaan resurssit terveydenhuollossa

Terveydenhuollossa henkilöstöllä ensisijaisena tehtävänä on potilaiden hoito, mikä on jokaisen terveydenhuollon alan yrityksen päätoimintaa. Tämän vuoksi henkilöstö koostuu pääosin terveydenhuollon ammattilaisista, joilla on saattaa olla riittämätön koulutus tietoturvaan tai tietosuojaan [30], [32]. Osaamisen puute altistaa organisaatiot hyökkäyksille, sillä niillä on hallussaan arvokasta tietoa, mutta tietojen suojaukset voivat olla heikot [11]. Tämä näkyy myös

toimialaisissa tilastoissa, joiden mukaan terveydenhuolto on usein hyökkäyksen kohteena [11], [15], [26], [27]

He ym. [32] ovat artikkelissaan analysoineet terveydenhuollossa esiintyviä tietoturvan puutteita COVID-19 pandemian jälkeen. Esille nousseet resurssien puutokset olivat tietoturvatietoisuuden puute henkilökunnalta, ajanpuute työtehtäville ja koulutuksille sekä heikko ohjeistus teknologian käyttöön.

Gioulekas ym. [33] toteuttivat kyberturvallisuuteen liittyvän kyselyn useassa Euroopan maassa. Tulosten mukaan budjetti oli monessa terveydenhuollon yrityksessä suurimpana esteenä. IT-budjetista käytettiin hyvin vähän kyberturvan parantamiseen. Terveydenhuollon rahoituksen tila nousee myös muissa artikkeleissa esille yhtenä rajoittavana tekijänä [34]. Käytetyn teknologian osalta keskeinen haaste on korvata vanhentunut infrastruktuuri, jota useat lähteet pitävät merkittävänä tietoturvariskinä [30], [34].

2.3.3 WannaCry

WannaCry oli kiristyshaittaohjelma, joka salasi tartunnan saaneen tietokoneen kaikki tiedostot ja vaati lunnasmaksun tiedostojen vapauttamiseksi [35], [36]. Haittaohjelmassa oli lisäksi toiminnallisuus, joka mahdollisti sen leviämisen automaattisesti muihin tietokoneisiin, mikäli tietyllä haavoittuvalla ohjelmistoversiolla oleva tietokone löytyi. Se toimi siis matona samanaikaisesti, kun se aiheutti tietokoneen tiedostojen salaamisen ja lunnasvaatimuksen. Tämä toiminnallisuus varmisti, että se levisi laajalti ympäri maailmaa [37].

WannaCry kiristyshaittaohjelma pohjautui tarkemmin EternalBlue – haavoittuvuudelle [35], [36]. Tämä haavoittuvuus käytti Windowsin SMB-protokollaa, jota käytetään yleisesti Windows tietokoneissa muun muassa laitteiden ja tiedostojen jakamisessa [38]. Hyökkäys kohdistui paikkaamattomaan versioon SMB-protokollasta, mikä mahdollisti haitallisen koodin suorittamisen kohdejärjestelmässä ilman käyttäjän toimia.

Koodin suorittaminen salasi tiedostot käyttäjän sitä havaitsematta. Salauksen lisäksi haittaohjelma skannasi liitetyt verkot ja etsi automaattisesti samaa SMB-protokollaversiota käyttäneet laitteet ja tietokoneet. Tällä tavoin se pääsi leviämään seuraavaan tietokoneeseen, jossa se salasi tiedostot ja pyrki jälleen siirtymään seuraavaan tietokoneeseen [35], [36].

WannaCry hyökkäys levisi todella laajalle. Sillä oli terveydenhuollossa merkittäviä vaikutuksia erityisesti Iso-Britanniassa. Siellä se levisi noin kolmasosaan kaikista Iso-Britannian

sairaanhoidopiireistä [39]. Leviämisen seurauksena sairaanhoidopiireissä peruutettiin vastaanottoaikoja, sekä merkittävä määrä resursseja jouduttiin käyttämään tietokantojen palauttamiseen.

Ghafur ym. [37] arvioivat, että arviolta n. 13500 sairaalakäyntiä jouduttiin hyökkäyksen takia peruuttamaan. Tämän lisäksi taloudellista tappiota aikojen peruuttamisesta olisi sairaaloille tullut arviolta yhteensä n. 5.9 miljoonaa puntaa. WannaCry hyökkäyksen takana epäillään olevan Pohjois-Korealainen hakkeriryhmä Lazarus. Yhdysvaltain oikeusministeriö on nostanut syytteen kolmea ryhmän jäsentä vastaan, mutta heitä ei ole pystytty pidättämään, joten tuomioita ei ole pystytty langettamaan [40].

2.3.4 Vastaamo

Vastaamon tietomurto tuli julkisuuteen vuonna 2020 [41], [42], [43]. Vastaamo oli suomalainen psykoterapiakeskus, joka tarjosi mielenterveyspalveluita. Vastaamon tietomurtotapaus on suomen historian suurin [41]. Tietomurrossa varastettiin yli 30 000 potilaan tiedot ja niillä koitettiin kiristää sekä Vastaamoa että yksittäisiä henkilöitä.

Tapaus osoittaa, miten organisaation sisäiset heikkoudet, kuten huono johtaminen ja puutteellinen IT järjestelmä yhdessä riskienhallinnan epäonnistumisen myötä voivat johtaa vakavaan tietomurtoon [42]. Yrityksessä esiintyi erilaisia riskejä, kuten puutteellinen järjestelmän suojaus ja heikko tietoturvaosaaminen [41], [42]. Näiden riskien realisoituminen mahdollisti tietomurron syntymisen.

Vastaamon tapaus osoittaa, että teknisten riskien hallinnalla ei pystytä pelkästään suojautumaan tietomurroilta. Tarvitaan myös hyvä kyberturvallisuuden kulttuuri. Vastaamon yrityksessä ei kiinnitetty riittävästi huomiota tietoturvaan kohtaan, ja se on suuri osasy sille, miksi tietomurto pääsi tapahtumaan [41], [42].

Vastaamon tietomurron tapauksessa tekijä saatiin kiinni. Tekijälle luettiin syytteet tietomurrosta ja hänet tuomittiin vankeuteen [44]. Vastaamolle langetettiin 608 000 € suuruinen hallinnollinen seuraamusmaksu GDPR:n rikkomuksista [45]. Vastaamon entinen toimitusjohtaja sai ehdollisen vankeusrangaistuksen huolimattomasta tietoturvan ja tietosuojan järjestämisestä [46].

2.4 Riskienhallinta ja kyberturvallisuuskulttuurin rakentaminen teoriassa

Riskienhallinta on olennainen osa jokaisen kestäväää ja turvallista yritystoimintaa tavoittelevan yrityksen toimintaa. Tässä aliluvussa perehdytään yleisesti riskienhallintaan ja kyberturvallisuuskulttuuriin. Lisäksi etsitään keinoja luoda kyberturvallisuuskulttuuria terveydenhuollossa toimivalle yritykselle.

2.4.1 Riskienhallinta ja riskienhallinnan mallit ja menetelmät

Riskienhallinta on yritysmaailmassa todella tuttu käsite. Thomas Wolke on kirjoittanut riskienhallinnasta hyvän perusteoksen nimeltään ”Risk Management” [47], jossa hän avaa mitä riskienhallinta on, ja mitä käsitteitä siihen liittyy. Kirjassaan hän määrittelee riskienhallinnan siten, että se on riskien mittaamista ja riskien hallintaa koko yrityksen laajuisena prosessina. Hän nostaa esille erikseen riskin ja sen hän määrittelee niin, että se on ”mahdollinen nettovarallisuuden menetys / vahinko ottamatta huomioon mahdollisia voittoja/tuloja” [47, Luku 1].

Riskienhallinta on jatkuva iteratiivinen prosessi. Sen vaiheita on Wolken kirjan mukaan yhteensä 4 [47, Kuv. 1.2]. Vaiheet ovat seuraavat:

1. Riskien tunnistaminen
2. Riskien analysointi
3. Riskien kontrolloinnin keinot
4. Riskien kontrollikeinojen vienti yrityksen toimintaan

Abraham ym. [48] puolestaan käsittelevät kyberturvan riskien hallintaa terveydenhuollon näkökulmasta. He tunnistavat omassa työssään 3 erilaista riskienhallinnan vaihetta [48, Kuv. 1]. Vaiheet ovat:

1. Kyberturvariskien tunnistaminen, jossa selvitetään organisaation keskeiset toiminnot ja niihin liittyvät haavoittuvuudet.
2. Kyberturvariskien arvioiminen, jossa arvioidaan erilaisten hyökkäysten todennäköisyydet ja niistä aiheutuvat seuraukset.
3. Tarvittavien toimenpiteiden viestiminen, joissa korostetaan läpinäkyvyyttä oikea-aikaisuutta, sekä oikein kohdennettua viestintää.

Malleissa on samankaltaisuuksia, mutta myös eroavaisuuksia. Wolken mallissa riskienhallinnasta puhutaan yleisellä tasolla. Hänen esittämää mallia ei ole yksilöity mihinkään tiettyyn alaan. Abrahamin ja kollegoiden mallissa riskienhallintamalli keskittyy erityisesti kyberturvariskeihin, joten siinä toimet ovat kohdennetummat kyberturvariskien hallintaan. Tämä näkyy esimerkiksi kommunikoinnin tärkeyden korostamisena, siitä on oma kohtansa erikseen, mitä taas ei suoraan ole Wolken mallissa. Toki Wolken mallin mukaan kommunikointi on osana riskien kontrollointia, mutta se ei ole pääosassa.

Riskienhallinta tässä työssä keskittyy IT riskeihin. Näille riskeille on olemassa erilaisia riskienhallinnan viitekehyksiä. Yleisesti tunnettuja ja hyväksytyjä viitekehyksiä ovat ISO27001 [49] ja NIST CSF [50]. Nämä auttavat yrityksiä varautumaan paremmin eri tilanteisiin, sillä ne sisältävät kattavan määrän toimia, joita yritys voi ennaltaehkäisevästi tehdä minimoidakseen tunnistamiaan riskejä.

Yhdysvaltain standardi- ja teknologiainstituutin kehittämä kyberturvallisuuskehys eli NIST CSF antaa hyvän perustan kyberturvallisuuden rakentamiselle yrityksen tarpeisiin. NIST CSF antaa eri kypsyydet tietoturvan osalta ja toimet, miten kypsyydet voi saavuttaa. NIST CSF perustuu kuuteen eri perustoimintoon. Nämä perustoiminnot ovat jaettu edelleen alakategorioihin, joka käsittelee tietyn osa-alueen kyberturvallisuudesta [48, Taul. 1]. Nämä perustoiminnot ovat:

- Hallinnointi (Govern)
- Tunnistaminen (Identify)
- Suojaus (Protect)
- Havaitseminen (Detect)
- Reagoi / vastaa (Respond)
- Toipuminen (Recover)

Näiden perustoimintojen lisäksi on olemassa näille toiminnoille alakategoriat. Alakategorioissa syvennyttään perustoimintojen eri osa-alueisiin ja näin saadaan kokonaisvaltaisempi kuvaus kyberturvallisuuden nykytilasta ja kehittämistoimista. Taulukossa 5 listataan sekä perustoiminnot että alakategoriat.

Taulukko 5. NIST kyberturvaviitekehysten rakenne

Taulukko on alkuperäistä mukaillen muokattu ja käännetty suomeksi [48, Taul. 1].

Perustoiminto	Alakategoria
Hallinta (GV)	Organisaation konteksti
	Riskienhallintastrategia
	Roolit, vastuut ja valtuudet
	Käytännöt
	Valvonta
	Kyberturvallisuuden toimitusketjuriskien hallinta
Tunnistaminen (ID)	Omaisuuden hallinta
	Riskinarviointi
	Parantaminen
Suojaus (PR)	Identiteetin hallinta, todennus ja pääsynhallinta
	Tietoisuus ja koulutus
	Tietoturva
	Alustaturvallisuus
	Teknologisen infrastruktuurin kestävyys
Havaitseminen (DE)	Jatkuva seuranta
	Haittatapahtumien analysointi
Reagointi (RS)	Tapahtumien hallinta
	Tapahtumien analyysi
	Tapahtumiin reagointi ja viestintä
	Tapahtumien lieventäminen
Palautuminen (RC)	Tapahtumien palautumissuunnitelman toteutus
	Palautumisviestintä

2.4.2 Kyberturvallisuuskulttuurin kehittäminen terveydenhuollon organisaatiossa

Työilmapiiri ja työskulttuuri vaikuttavat suuresti siihen, mihin työpäivän aikana ja sitä myötä töissä ylipäätään keskitytään. Organisaatiossa voidaan painottaa eri osa-alueita, kuten työn tuottavuutta tai tehokkuutta, laatua, turvallisuutta tai tietoturvaa. Nämä painotukset tulevat yleensä ylimmän johdon linjausten perusteella ja näiden painotusten toteuttamisessa esimiehillä on merkittävä rooli. Yksiköiden välillä saattaa esiintyä eroja siinä, miten vahvasti yksiköiden välillä painotetaan eri osa-alueita, jos yksikön esimiehille on jätetty jonkin verran päätösvaltaa oman tiiminsä johtamiseen. Suuret linjaukset määritellään lähes aina koko organisaation ylimmän johtoportaan mukaan ja siten heijastuvat myös rivityöntekijän jokapäiväiseen työhön.

Abraham ym. haastattelivat omassa tutkimuksessaan [48] eri tietoturva-asiantuntijoita, jotka työskentelivät Yhdysvalloissa eri kokoisissa terveydenhuollon yrityksissä. Tutkimuksen tuloksista selviää, että kyberturvaan panostetaan yrityksissä todella vähän, keskimäärin 3 % kokonaisbudjetista. Tutkijoiden mukaan näin vähäinen rahoitus voi johtaa resurssipulaan. Tämä saattaa ilmetä henkilökunnan säännöllisen koulutuksen puutteena, tai tietoturvajohtajan (CISO) puuttumisena.

Euroopassa Gioulekas ym. toteuttivat laaja-alaisen kyselytutkimuksen [33] kyberturvakulttuurista kolmessa eri Euroopan maassa: Kreikassa, Portugalissa ja Romaniassa. Kyselytutkimuksessa oli tarkoitus arvioida miten hyvällä tasolla näiden maiden terveydenhuollon organisaatioiden tietoturvakulttuuri ja tietoturvatietämys on. Tuloksista ilmeni, että henkilökunta ei ole yhdessä organisaatiossa saanut viimeisen 3 vuoden sisällä kertaakaan koulutusta tietoturvasta ja että kaikilla organisaatioilla ei ole omaa kyberturvaosastoa. Nämä esille nousseet seikat ovat kyselytutkimuksen tutkijoiden mukaan merkittävä riski organisaatioiden kyberturvallisuudelle. Tutkimuksessa mainittiin riskinä myös alhainen budjetointi kyberturvallisuuden kehittämiseen ja ylläpitämiseen, joka tässä oli ollut alle 5 % ICT budjetista.

Argyridou ym. [51] käsittelivät artikkelissaan miten luoda kyberhygienian kulttuuri organisaatioon. He kehittivät artikkelissaan riskianalyysityökalun tietoturvariskien minimoimiseksi. Yhtenä osana tätä riskianalyysityökalua riskien minimoimisessa he käyttävät kyberturvakulttuurin luomista. He esittävät artikkelissaan joukon erilaisia kontrolloikeinoja ja osaa näistä kontrolloikeinoista voidaan käyttää heidän mukaansa kyberturvallisuuskulttuurin luomiseen. Kontrolloikeinot perustuvat yhdysvaltalaisen organisaation Center for Information Security:n (CIS) kriittisiin turvallisuuskontrolleihin keskittyvään dokumenttiin [52].

Kontrolloikeinot kyberturvakulttuurin vahvistamiseksi ja kehittämiseksi on listattu taulukkoon 6. Keinot on koottu Argyridou ym. artikkelista [51], johon he ovat koonneet ne useista eri lähteistä. Taulukkoon 6 on sisällytetty vain ne kontrolloikeinot, joita voidaan heidän artikkelinsa mukaan käyttää kyberkulttuurin luomiseen. Kontrolloikeinojen lisäksi taulukkoon 6 on listattu erikseen vielä tarkemmin, miten nämä keinot auttavat kyberturvallisuuden tietoisuuden lisäämisessä.

Taulukko 6. Kontrollikeinot kyberturvallisuuden tietoisuuden lisäämiseksi

Kontrolli	Kuvaus tietoisuuden lisäämiseksi
Kehitä kyberturvallisuuden tietoisuusohjelma	Luodaan kyberturvallisuuteen liittyvä tietoisuusohjelma, jota toteuttamalla voidaan varmistua siitä, että työntekijät voisivat omaksua tarpeelliset taidot yrityksen turvallisuuden varmistamiseksi.
Päivitä tietoisuusohjelmaa säännöllisesti	Tietoisuusohjelmaa tulee päivittää säännöllisesti ja usein, jotta voidaan muokata tietoisuusohjelma vastaamaan sen ajan uhkia ja teknologioita.
Kouluta työntekijöitä tyypillisimmistä uhista sekä niiden tunnistamisesta ja miten toimitaan tällaisessa tilanteessa.	Kouluttamalla työntekijät tyypillisimmistä uhista, voidaan ehkäistä niiden uhkien realisoitumista. Lisäksi koulutus takaa toimintaohjeet myös tilanteessa, jossa uhka on päässyt realisoitumaan, jolloin voidaan tehokkaammin aloittaa tarvittava toimet.
Sisällytä kyberturvallisuus osaksi arkea ottamalla se ja kyberturvahenkilöstö mukaan kokouksiin ja kokouksien asialistoille.	Tämä keino takaa sen, että kyberturva on läsnä päätöksien teossa, jolloin päätöksien teon yhteydessä voidaan jo miettiä mahdollisia kyberturvaan liittyviä seikkoja, jolloin varmistetaan kyberturvan toteutuminen tehokkaammin.
Anna tunnustusta työntekijöille, jotka noudattavat ja toimivat vastuullisella tavalla tietoturva- ja tietosuoja kysymysten parissa	Tunnusta työntekijät, jotka osoittavat hyvää tietosuojakäytöstä, esimerkiksi ilmoittavat kalasteluviesteistä ja epäilyttävistä tapauksista ja palkitse heidät jollain tavalla, esimerkiksi tittelillä ”Kuukauden kybertyöntekijä” tai vastaavalla.
Otetaan käyttöön tietoturvasta perehtyneen työntekijän rooli.	Ota käyttöön tietoturvaan perehtyneen työntekijän rooli, esimerkiksi jokaisessa yksikössä. Hänen avullaan voidaan kyberturvan ja tietosuojan viemistä edistää jokapäiväiseen työhön, sekä madaltaa avun hakemista tarvittaessa. Työntekijä toimii esimerkkinä muille tietoturvan osalta.
Juhlitaan ja muistutetaan kyberturvasta ja tietosuojasta erikoisilla tilaisuuksilla tai teemapäivillä / viikoilla / kuukausilla.	Otetaan käyttöön jokin tietty ajanjakso, jolloin juhlitaan ja muistutetaan erityisesti kyberturvallisuutta. Tämä voi olla päivä, viikko, kuukausi tai jokin muu aikamääre. Esimerkiksi Euroopassa vietetään Euroopan kyberturvakuukautta (ECSM) aina lokakuussa.

Loonam ym. [53] tutkivat omassa artikkelissaan sitä, miten johtajuus vaikuttaa kyberturvallisuuteen ja sen hallintaan digitaalisissa yrityksissä. He haastattelivat useampaa korkea-arvoista tietoturvahenkilöä johtoasemassa eri yrityksissä ja haastattelujen perusteella loivat listan eri teemoista, joita haastatteluissa nousi esille. Näillä teemoilla on tarkoitus tukea sitä, miten johtajisto voi tuoda kyberturvaa osaksi yrityksen toimintaa.

Heidän tunnistamansa teemat kuvaavat keinoja, joilla yrityksen johto voi tuoda kyberturvallisuuden paremmin osaksi yrityksen päivittäistä toimintaa [53]. Ensimmäisenä korostetaan sitä, että kyberturvan strategian tulee olla linjassa liiketoiminnan strategian kanssa. Toiseksi organisaation tulisi arvioida liiketoimintansa prosessien herkkyys erilaisille kyberuhille. Kolmanneksi luottamuksen kulttuuria tulisi edistää, jotta kyber-resilienssistä muodostuisi luonnollinen osa työntekijän päivittäistä toimintaa. Kyber-resilienssiä pitäisi

lisäksi sisällyttää osaksi yrityksen pitkäaikaista strategiaa. Näiden lisäksi yrityksen täytyy varmistaa, että sen kumppanit ja muut yhteistyötoimijat noudattavat yrityksen kyberturvaperiaatteita. Tutkijat mainitsevat myös selkeät rakenteet ja vastualueet kyberturvallisuuden hallitsemiseksi. Yrityksen pitää huolehtia tietoturvajohhtajan tai tietohallintojohhtajan osallistuminen strategiaan päätöksiin. Lopuksi tutkijat toteavat, että kriittinen data on tunnistettava ja sen suojaaminen on priorisoitava.

Loonamin ym. [53] artikkelin toimia verrattaessa Argyridou ym. [51] kontrollikeinoihin, voidaan niistä nähdä joitain yhtäläisyyksiä. Loonam ym. nostamat johtamisen teemat tukevat Argyridou ym. esittämiä kontrollikeinoja kyberturvallisuuskulttuurin vahvistamiseksi. Molemmissa korostetaan strategisen suunnittelun, kulttuurin rakentamisen ja vastuunjaon merkitystä.

Argyridou ym. painottavat käytännönläheisiä keinoja, kuten tietoisuussuunnitelmaa, koulutusta ja arjessa näkymistä, kun taas Loonam ym. lähestyvät johdon näkökulmasta. Heidän mukaansa kyberturvan integrointi liiketoimintastrategiaan, selkeät roolit ovat avain kyberturvakulttuurin rakentamiselle. Yhteistä molemmille on ajatus siitä, että ylimmän johdon sitouttaminen ja henkilöstön arjen toiminta ovat tärkeitä kyberturvallisuuden onnistumiselle.

3 Tietoturva ja -suoja koulutusohjelman toimeenpano ja vaikutukset organisaatiossa

Tässä kappaleessa kerrotaan, mitä uuteen koulutukseen kuuluu ja miten sitä on aloitettu viemään käytäntöön palveluyksiköissä. Samalla koulutus liitetään aiempaan taustamateriaaliin ja pyritään selittämään, miksi koulutus on sellainen kuin se on, ja miksi koulutus on päätetty ottaa käyttöön juuri tällä tavalla.

Ensimmäiseksi käydään läpi vanha koulutus, sen jälkeen uusi koulutus, kuten mistä se koostuu ja miten se suoritetaan. Sen jälkeen siirrytään siihen, miten johtajien rooli vaikuttaa koulutuksen jalkauttamiseen ja siirrytään viimeiseksi pilotoituun yksikköön.

3.1 Vanhan tietosuojakoulutuksen kuvaus

Yrjö ja Hanna hyvinvointipalveluiden edeltävä tietoturva ja -suojakoulutus on osa suurempaa Skhole-koulutusjärjestelmää, joka on ollut hoivakotiorganisaatiolla käytössä [54]. Sen painopiste on vahvasti hoitotyön tietosuojassa. Siinä käsitellään tarkasti mitä edellytetään asiakkaiden tietosuojan varmistamiseksi kaikissa tilanteissa.

Koulutuksessa käydään lakitasolla läpi hoivatyötä koskevat lait ja niiden edellyttämät toimintatavat eri tilanteissa työympäristössä. Esimerkkeinä koulutuksessa käsitellään GDPR:n rekisteröidyn oikeuksia, henkilötietojen käsittelyä, tietojen luovutusta potilasasiakirjoista, sekä yleisiä tietoturvatavoimia. Yleinen tietoturvaan liittyvä osio jää kuitenkin kevyeksi verrattaessa uuteen valittuun koulutukseen.

Vanhan koulutuksen rakenne eroaa uudesta koulutuksesta. Molemmat suoritetaan verkkopohjaisena itseopiskeluna. Suoritusmerkinnän saa vanhassa koulutuksessa sillä, kun itse kuittaa, että on lukenut ja ymmärtänyt oppimismateriaalin. Oppimista ei millään tavalla varmenneta, vaan vastuu oppimisesta jää täysin työntekijälle. Tällä menetelmällä on riskinsä kokonaisturvallisuutta ajatellen siinä, että vaikka kirjanpidollisesti kaikki näyttävät käyneen tietoturva ja -suojakoulutuksen, ei voida täysin varmistua siitä, että työntekijä osaa toimia asetusten ja lakien edellyttämällä tavalla.

3.2 Uuden tietoturva ja -suoja koulutuksen toteuttaminen

Yrjö ja Hanna hyvinvointipalveluiden tietosuoja- ja tietoturvakoulutuksesta vastaa uusi palveluntarjoaja [55]. Se toimittaa verkkopohjaisen koulutusalan, joka on käytettävissä sekä

tietokoneella että mobiililaitteella, ja joka sisältää useita eri kursseja eri teemoihin liittyen. Uuden palveluntarjoajan peruskurssi kattaa yleisimmät tietosuojan ja -turvaan liittyvät teemat, kuten tietosuoja ja -turva yleisesti, kalasteluviestit, etätyöskentelyn tietoturvan.

Tämän lisäksi heidän kurssitarjontaansa kuuluu hoitohenkilökunnalle suunnattu erillinen kurssi. Sillä kurssilla käsitellään erityisesti hoiva-alan työntekijöille suunnattuja säännöksiä. Kyseinen kurssi vastaa sisällöltään vanhaa tietosuojan keskittyntä koulutusta, joka esiteltiin kappaleessa 3.1. Kurssi käsittelee hoivakodin asiakkaiden oikeuksia, jotka perustuvat eri lakeihin ja asetuksiin, kuten GDPR:ään sekä asiakastietolakiin ja tietosuojalakiin. Nämä koulutukselliset vaatimukset listataan Terveiden ja hyvinvoinnin laitoksen määräyksessä 3/2024 [25, Luku 6.3].

Koulutuksien tavoitteena on varmistaa, että työntekijöillä on perustason ymmärrys tietosuojasta, sekä tietoturvasta. Tämä osaaminen on tärkeää, jotta he voivat toimia turvallisesti erilaisissa tilanteissa.

Koulutuksen toteutus

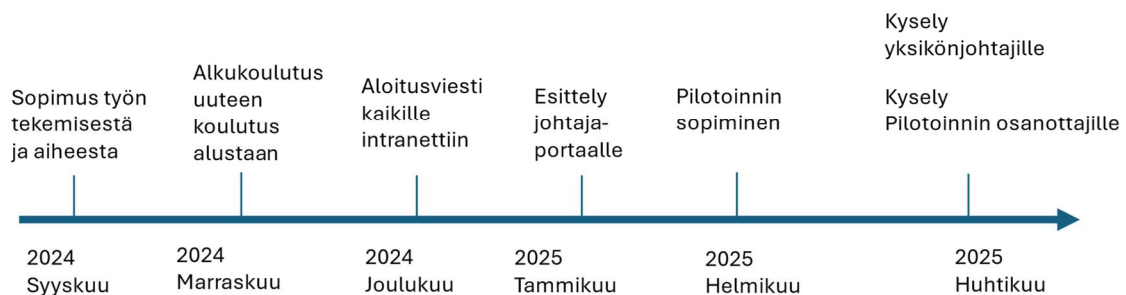
Koulutus toteutetaan itseopiskeluna vuosittain verkkopohjaisen itseopiskelumateriaalin avulla. Opiskelemisen jälkeen henkilön osaaminen varmistetaan lyhyellä tentillä, joka koostuu monivalintakysymyksistä. Opiskelumateriaali koostuu teemoittain eri kursseista, jotka sisältävät useamman osa-alueen. Jokaisesta osa-alueesta on oma testinsä. Kaikkien osioiden hyväksyty suorittaminen on edellytys kurssin suorittamiseksi.

Koulutuksen käyttöönotto koko Yrjö ja Hanna hyvinvointipalveluiden organisaatiossa aloitettiin syksyllä 2024 IT-tietohallintojohtajan ja henkilöstöhallinnon kanssa. Ensin tietyille henkilöille järjestettiin käyttökoulutus alustan käytöstä. Uudesta koulutuksesta tiedotettiin koko organisaation henkilökuntaa joulukuussa 2024 sisäisessä viestintäkanavassa. Tammikuussa 2025 organisaation hyvinvointipalveluyksiköiden johtajien kokouksessa koulutuksesta pidettiin esitys, koulutuksen sisällöstä ja suorittamiseen liittyvistä käytännöistä.

Yritykselle on laadittu opastevideoita ja kirjalliset ohjeet koulutuksen käyttöön liittyen. Näissä ohjeistetaan mistä koulutuksen löytää, miten sen aloittaa, sekä mitä koulutuksen suorittaminen edellyttää. Koulutuksen käyttöönotto tapahtuu vaiheittain sen mukaan, milloin henkilökunta on suorittanut edellisen vuoden koulutuksen. Koulutus tulee suorittaa vähintään kerran vuodessa.

Pilottivaiheeseen valikoitui yksi palveluyksikkö organisaation sisältä. Tavoitteena oli saada henkilökunta suorittamaan koulutus mahdollisimman kattavalla prosentilla. Palveluyksikölle teetettiin lyhyt kyselytutkimus huhtikuussa 2025. Pilotoinnin kyselyssä oli tarkoitus selvittää henkilökunnan mielipiteitä ja asennetta uutta koulutusta kohtaan. Kuvassa 1 on havainnollistettu työn eri vaiheet aikajanalle.

Työn eri vaiheet organisaation suhteen



Kuva 1: Työn tärkeimmät vaiheet aikajanalle sijoitettuna.

3.3 Johdon rooli koulutusohjelman toteuttamisessa

Johtajilla on merkittävä rooli uuden koulutuksen käytäntöön viemisessä. Tämän ovat todenneet useat tutkijat ja teokset [51], [53], [56], [57], [58]. Argyridou ym. [51] eivät suoraan mainitse johtajia tai esimiehiä heidän kontrollirakenteissaan, mutta heidän esittämistään rakenteista käy ilmi, että esimerkiksi kyberhenkilökunnan sisällyttäminen kokouksiin tuo näkemyksensä mukaan päätöksentekoon. Päätökset tehdään yleisesti ylimmällä johtajatasolla. Toinen heidän mainitsemansa kontrollikeino on tietoturvaan erikoistuneen työntekijän nimittäminen. Tämä vaatii perehtyneisyyttä myös johdolta tietoturvaan liittyen. Myös tunnustuksen antaminen työntekijälle, joka toimii kunnioitettavalla tavalla tietoturvan ja -suojan osalta, edellyttää johdon ymmärrystä asiasta.

Loonam ym. [53] nostavat johtajien esimerkin yhdeksi tärkeäksi johdon tehtäväksi kyberturvakulttuurin rakentamisessa. He mainitsevat muun muassa kyberturvastrategian

linjauksen liiketoimintastrategian kanssa ja selvien hallintorakenteiden ja vastuualueiden luomisen kyberturvallisuuden hallintaa varten. Näiden lisäksi mainitaan tietohallintojohtajan tai tietoturvaajohtajan osallisuus johtoryhmässä.

Mehner ym. [56], Ismail ym. [57] ja Walker ym. [58] ovat tutkineet tekijöitä, jotka johtavat onnistuneisiin tuloksiin käyttöönotettaessa uutta koulutusohjelmaa. Kaikissa näissä artikkeleissa korostuu johdon rooli. Mehner ym. [56] havaitsivat tutkimuksessaan, että johtajat, jotka aktiivisesti kannustavat ja tukevat alaisiaan uuden koulutuksen käytössä saavat parempia tuloksia, kuin ne, jotka eivät näin tee.

Ismail ym. [57] löysivät tutkimuksessaan selkeän yhteyden johtajien asenteen ja koulutuksen vastaanoton välille. Mitä myönteisempi johtajan suhtautuminen on, sitä motivoituneempia työntekijät ovat koulutusta kohtaan. Walker ym. [58] puolestaan havaitsi, että koulutukseen valmistautuminen on todella tärkeää. Koulutusta varten pitää varata riittävät määrät resursseja, kuten aikaa, kannustava ilmapiiri uuden koulutuksen ympärille, sekä motivoitunut johto.

Viestinnän osalta useammassa tutkimuksessa [59], [60], [61] on todettu, että onnistunut ja selkeä viestintä on avain siihen, että yrityksessä pystytään viemään uudistuksia eteenpäin mahdollisimman tehokkaasti. Fidler ja Lori [59] korostavat viestintää ja viestinnässä oikeita kanavia, sillä oikeiden viestikanavien valinnalla voidaan vaikuttaa viestin aiheuttamaan reaktioon.

Peng ja Litteljohn [60] löysivät yhteyden sen välille, että selkeällä viestinnällä on ensisijainen rooli onnistuneissa investoinneissa, mutta samalla he toteavat, että se ei ole ainoa asia onnistuneen investoinnin tai uudistuksen taustalla. Lewis [61] korostaa omassa artikkelissaan, että muutoksista viestittäessä viestinnän määrä ei yksin riitä hyvään viestintään, vaan siihen tarvitaan sopivan määrän lisäksi vielä hyvä viestinnän laatu. Hyvällä laadulla Lewis tarkoittaa artikkelissaan sitä, että mitä selvemmin esimerkiksi johtajien visio tulee viestistä esille tai mitä paremmin työntekijät tunsivat itsensä arvostetuksi omalla panoksellaan, sitä paremmin uusi muutos koettiin onnistuneen.

Yhteenvedona useiden tutkimuksien mukaan voidaan todeta, että johdolla on keskeinen merkitys yrityksen kyberturvakulttuurin parantamisessa. Kun johto pitää kyberturvallisuutta tärkeässä asemassa, se heijastuu myös työntekijöihin johtajien asenteiden kautta.

Tähän teoriaan nojaten luotiin kyselytutkimus johtajille. Kyselyn tarkoituksena oli selvittää, miten palveluyksiköiden johtajat kokivat uuden koulutuksen jalkauttamisen onnistuneen ja

miten he näkivät oman roolinsa koulutuksen viemisessä käytäntöön. Kyselyn kysymykset ovat löydettävissä liitteestä 1. Kyselyn tulokset ja pohdinta esitellään myöhemmin kappaleessa 5.

3.4 Palveluyksikön pilotointi ja palautekysely koko henkilökunnalle

Pilotointi sovittiin tietyn palveluyksikön kanssa ja se toteutettiin maaliskuun 2025 aikana. Valittu yksikkö oli sellainen, jossa koulutuksen sisällöllä nähtiin olevan erityistä merkitystä. Yrityksen osalta yksikön pilotoinnin valintaan vaikutti suuresti halu vahvistaa siellä työskentelevän henkilökunnan osaamista tietoturvan ja -suojan käytänteistä. Tähän tarkoitukseen pilotointi sopi todella hyvin.

Pilotoinnin tarkoituksena oli testata, että kurssien suorittaminen sujuu ongelmitta ennen kuin koko työyhteisö ottaa käyttöön uuden koulutuksen. Lisäksi siihen sisältyi kalasteluviestitesti, jonka tarkoituksena oli kartoittaa henkilöstön reagointia tietojenkalasteluun liittyviin uhkiin. Suurimmalla osalla kauemmin yrityksessä työskennelleistä työntekijöistä edellinen tietosuojakoulutus oli suoritettu syksyllä 2024, joten suurimmalle osalle työntekijöistä tämän koulutuksen suorittaminen ei ollut ajankohtaista tämän tutkimuksen aikana, vaan vasta syksyllä 2025.

Tämän lisäksi tarkoituksena oli, että muut olennaiset toiminnot, kuten kurssien muistutus ja niiden näkyvyyden määrittely tiettyyn rooliin perustuen onnistuvat toivotulla tavalla. Pilotointi oli tärkeää myös sen vuoksi, että yritys palkkaa koko ajan uusia työntekijöitä, joiden pitää suorittaa koulutus niin pian kuin mahdollista, jolloin on tärkeää varmistua uuden järjestelmän toimivuudesta. Pilotoinnilla haluttiin selvittää myös henkilökunnan näkemystä siitä, miten tällainen merkittävä muutos voidaan tuoda osaksi työyhteisöä. Erityisesti pyrittiin selvittää missä toteutuksen kanssa onnistuttiin ja mitä olisi pitänyt tehdä toisin.

Palveluyksikön johtaja on vienyt aktiivisesti koulutusta omalle henkilökunnalle kokouksissa, muistuttanut siitä suullisesti, sekä erikseen ilmoitustauluilla. Johtaja ei ole saanut alaisiltaan juurikaan palautetta koulutukseen liittyen, mutta, muutamissa on noussut esille puutteita tietosuojan osalta. Tämä on nostettu yrityksen henkilöstöhallinnon tietoon ja tähän on reagoitu ottamalla erillinen kurssi tietosuojaan liittyen mukaan koulutusrakenteeseen.

Pilotoinnin aloittamisessa koettiin haasteita palveluun kirjautumisessa. Se saatiin toimimaan ja pilotti lähti käyntiin hyvin nopealla aikataululla. Näin tiedotus pilotoinnin aloituksesta pilottiyksikölle jäi osittain puutteelliseksi. Tämä nousi pilotoinnista vastanneen yksikön johtajan palautteessa esille, että pilotoinnin aloituksen viestinnässä oli epäselvyyttä.

Argyridou ym. [51] esittävät, henkilöstön tietoisuuden vahvistaminen on keskeinen osa kyberturvallisuuskulttuurin kehittämistä. Pilotointi tuki tätä tavoitetta lisäämällä tietoa tietoturvasta ja tietosuojasta valitussa yksikössä. Lisäksi Loonam ym. [53] korostavat selkeän roolituksen merkitystä. Pilotoinnin onnistumisessa näkyi yksikön johtajan aktiivinen rooli viestinnässä ja jalkautuksessa, mikä osaltaan vahvisti koulutuksen vastaanottoa.

Terveystieteiden tutkimuksessa henkilötiedot ovat arvokkaita [20] ja siksi, kuten useat tutkimukset ja raportit ovat todenneet [15], [26], [27], [30] tietojen kalastelu on todellinen uhka terveydenhuollon sektorilla. Pilotin ohella palveluyksikköön päätettiin toteuttaa kalasteluviestitesti. Tämä liittyy uuteen koulutukseen sisällön puolesta siten, että yhtenä osana uutta koulutusta on tietojen kalasteluun liittyvä itseopiskeluosio.

Kalasteluviestitesti toteutettiin siten, että viesti lähetettiin yksikön johtajan nimissä tätä käyttötarkoitusta varten luodulla Gmail tilillä. Tarkoituksena oli selvittää huomataanko viestin olevan kalasteluviesti. Viestissä kehoitettiin vaihtamaan salasana oheisesta linkistä ja sen lisäksi avaamaan linkki. Viestissä liitteenä olleet PowerPoint tiedostot keräsivät tiedostossa vierailleet henkilöt, joista sai tiedon, kuinka moni työntekijä oli erehtynyt linkkejä painamaan. Viestit lähetettiin kahdella eri kerralla. Viesti löytyy liitteestä 4 muunneltuna siten, ettei yksikköä voi viestin perusteella tunnistaa.

Pilotoinnin palveluyksikön henkilökunnalle sekä muille, jotka olivat määräpäivään mennessä suorittaneet uuden koulutuksen lähetettiin vastauskutsu kyselyyn. Siinä pyrittiin kartoittamaan sitä, miten henkilökunta on suhtautunut muutokseen ja uuteen koulutukseen. Kysely koostui erilaisista kysymyksistä. Pääosin kyselyssä oli Likert asteikollisia väittämiä, avoimia kysymyksiä ja muutaman valintakysymys.

Vastauskutsu oli voimassa yhden viikon ajan. Vastaajia motivoitiin vastaamaan kyselyyn ja palkinnoksi vastaamisesta arvottiin lahjakorttipalkinto yhdelle vastanneelle. Henkilöstöltä kerättävä palaute toimii tärkeässä roolissa arvioitaessa sitä, miten hyvin jalkautus on onnistunut. Kysely löytyy liitteestä 2.

4 Terveydenhuollon yrityksen NIS2-valmiuden mittaaminen

NIS2-direktiivi luo selkeät vaatimukset Euroopassa organisaatioiden kyberturvallisuuden hallinnalle ja vastuun jakamiselle. Terveydenhuoltoala kuuluu aiemmin käsiteltyihin kriittisiin toimijoihin, joiden palvelut ovat yhteiskunnan toimivuuden kannalta lähes välttämättömiä. Direktiivi ei kuitenkaan määrittele miten organisaation valmiutta tulisi mitata tai arvioida.

Tässä luvussa organisaation kyberturvavalmiutta arvioidaan käyttäen Alwin Van Welien kehittämää viitekehystä, joka pohjautuu NIS2:n vaatimukseen ja on laadittu terveydenhuollon kontekstiin Alankomaissa [62].

4.1 NIS2 valmiuden mittaamisen viitekehys

Viitekehystenä käytetään Van Welien maisterityössään kehittämää mallia NIS2-valmiuden arvioimiseksi [63]. Kehys on suunniteltu Alankomaiden terveydenhuollon yrityksille. Siinä tarkastellaan tyypillisiä aukkoja NIS2-direktiivin vaatimusten ja alan osaamisen nykytilan välisestä erosta. Malli on kuitenkin yleistettävissä myös muualle Eurooppaan, sillä se perustuu direktiiviin, joka määrittää kaikille EU-maille yhteiset minimivaatimukset.

Kehyksessä aukot ovat jaettu neljään osa-alueeseen: tietoturvapoliittikat ja hallinta, käytännön toteutus, valvonta ja raportointi sekä tietoisuus ja koulutus. Jokaisesta osa-alueesta kehyksessä nostetaan muutama kohta, jotka perustelevat aukon sisällyttämisen viitekehykseen. Esimerkiksi tietoturvapoliittikan ja hallinnan osa-alueeseen kuuluvista aukoista on voinut puuttua kunnollinen tietoturvapoliittikka, tai tietoturvan vastuuhenkilöt eivät ole tiedossa.

Käytännön toteutuksien osalta hän nostaa esiin yleisiä puutteita riskienhallinnassa tai ettei sitä toteuteta säännöllisesti. Lisäksi säännölliset toimet, kuten tietoturvatarkastukset saattavat puuttua kokonaan yrityksiltä. Hänen löydöksensä osoittavat myös, että kolmansien osapuolien riskienhallinnassa on parannettavaa.

Valvonnan ja raportoinnin osalta terveydenhuollon yrityksillä on parannettavaa. Van Welien mukaan joskus tietoturvaloukkauksia ei aina havaita lainkaan, ja vaikka havaittaisiinkin, ei niistä välttämättä ilmoiteta asianmukaisesti. Ilmoittamiseen ei usein ole dokumentoituja prosesseja. Tapahtumien kirjaamista ei myöskään aina tehdä riittävällä tasolla, eikä kirjauksia tarkasteta riittävän usein.

Myös tietoisuudessa ja koulutuksessa esiintyy puutteita. Henkilöstö ei välttämättä saa säännöllisesti tai lainkaan koulutusta tietoturvasta ja -suojausta. Suoritetun koulutuksen vaikuttavuusarvioita ei myöskään aina tehdä. Lisäksi käytännön harjoittelu todellisten tilanteiden varalle jää usein hyvin vähäiseksi, vaikka se olisi olennainen osa riskeihin varautumista.

Tämä viitekehys valittiin työhön koska se kohdistuu nimenomaan terveydenhuoltoalalle. Marraskuussa 2024 tehdyssä kirjallisuushaussa ei löytynyt muita valmiita, tieteellisesti julkaistuja NIS2-viitekehyskiä, joita olisi voinut soveltaa tutkimukseen suoraan. Haussa löytyi ainoastaan yksittäisiä korkeakoulujen opinnäytetöitä, mutta ei vertaisarvioituista lähteistä.

4.2 Viitekehuksesta luotu haastattelu

Haastattelulla oli tarkoitus kartoittaa Yrjö ja Hanna kotien hyvinvointipalveluiden organisaation tilannetta uuden NIS2-direktiivin osalta. Direktiivi koskettaa organisaatiota suoraan, sillä se lukeutuu NIS2-direktiivin jaottelun mukaisesti kriittisiin toimijoihin. Direktiivin vaatimuksien laiminlyönnistä voi seurata merkittävät uhkasakot. Haastateltavana oli yrityksen IT- ja tietohallintojohtaja (CIO, CISO), jonka vastuulla on IT-toiminnot ja tietoturvajohdaminen.

NIS2-direktiivin velvoitteet liittyvät suoraan henkilökunnan osaamiseen ja tietoisuuteen tietoturvasta ja tietosuojasta. Tämän työn tavoite vahvistaa yrityksen tietosuojaa ja tietoturvaa tukee siten myös direktiivin velvoitteita. Haastattelun tarkoituksena oli tunnistaa palveluyksiköiden ja organisaation mahdolliset puutteet suhteessa NIS2-direktiivin ja tukea yritystä NIS2-valmiuden kehittämistä.

Haastattelu toteutettiin etäpalaverina 29.4.2025. Kysymykset jaettiin IT-johtajalle ennakkoon tutustumista varten. Ne oli jaoteltu neljään eri osa-alueeseen Van Welien viitekehysten mukaisesti. Osa-alueet olivat ”Organisaatorakenne ja vastuu”, ”Resurssit ja osaaminen”, ”Kulttuuri ja tietoturvatietoisuus” sekä ”Kokonaisarvio ja kehitysnäkymät”.

Haastattelu oli puolistrukturoitu, jossa kysymysten käsittely tapahtui keskustellen. Haastattelu nauhoitettiin ja sen perusteella vastaukset koottiin analysointia varten. Haastattelun tulokset esitetään luvussa 5.3. Haastattelun kysymykset löytyvät liitteestä 3.

5 Työn tulokset

Tässä luvussa esitellään tutkimuksen tulokset. Ensin tarkastellaan henkilöstölle suunnatun kyselyn vastauksia, minkä jälkeen siirrytään esihenkilöiden kyselyn havaintoihin. Ennen tulosten analyysiä, käsitellään NIS2-haastattelun tulokset. Luvun lopussa tarkastellaan tuloksia analyttisesti.

5.1 Pilotointi ja henkilökunnan kyselyn tulokset

Pilotointi toteutettiin valitussa palveluyksikössä, ja sen tavoitteena oli kerätä tietoa uudesta koulutuksen käytettävyydestä ja vaikutuksista. Yksiköstä osallistui 74 henkilöä, joihin kuului hoitajia, esihenkilöitä ja muuta henkilökuntaa. Koulutuksen suoritti kuitenkin vain 25 henkilöä, eli suoritusten määrä jäi odotettua vähäisemmäksi. Koulutuksen suorittamiseen varattiin kuukauden verran aikaa ennen kuin vastausprosentin tarkistettiin ja kysely lähetettiin.

Pilotoinnin aikana koulutuksen suoritusten määrään jäätyä alhaiseksi kysely päätettiin lähettää myös kaikille muille, jotka olivat itsenäisesti suorittaneet koulutuksen. Palveluyksikön johtajat rajattiin pois, sillä johtajille lähetettiin erillinen kysely. Vastauskutsu kyselyyn lähetettiin yhteensä 98 henkilölle, joista 27 vastasi viikon sisällä. Vastausaikaa kyselyyn annettiin niukasti, joka on saattanut rajoittaa vastauksien määrää.

Kyselyssä kartoitettiin ensin koulutuksen ohjeistusta sekä viestinnän ja aikataulun toimivuutta. Taulukossa 7 esitellään näihin teemoihin liittyvien väittämien tuloksia. Vastaajista 66 % koki, että koulutuksen suorittamisesta on annettu selkeät ohjeet. Vastaavasti 70 %:n mielestä aikataulu ja suoritustapa olivat sopivat. Kaikista vastauksista 59 % tunsu koulutuksesta tiedottamisen olleen riittävää. Tekniset ohjeet olivat selkeät 81 %:n mukaan ja 74 % piti koulutuksen suorittamiseen varattua aikaa riittävänä. Avoimissa vastauksissa esiin nousi toive siitä, että koulutuksen suorittamiseen olisi enemmän aikaa työajalla. Muutamat vastaajat toivoivat ohjeistuksia lisäksi sähköpostiin, eikä pelkästään sisäiseen viestintäkanavaan.

Taulukko 7. Henkilökunnan vastaukset ohjeistuksen, viestinnän ja aikataulun väittämiin

Väittämä	Samaa mieltä	Neutraali	Eri mieltä
Sain koulutuksesta ja sen suorittamisesta selkeät ohjeet.	66 %	19 %	15 %
Koulutuksen aikataulu ja suoritustapa oli minulle selkeä.	70 %	15 %	15 %
Koulutuksen tiedottaminen (esim. sähköposti, intra, esihenkilö) oli riittävää.	59 %	15 %	26 %
Koulutuksen suorittamiseen liittyvät tekniset ohjeet olivat selkeitä	81 %	19 %	0 %
Koen, että minulla oli riittävästi aikaa suorittaa koulutus	74 %	11 %	15 %

Koulutus koettiin kyselyvastausten perusteella selkeäksi ja helposti ymmärrettäväksi 81 %:n mielestä. Sen sisältö ja esimerkit arvioitiin käytännönläheiseksi 85 %:ssa vastauksista. Koulutus koettiin sopivan pituiseksi 81 %:n mukaan ja loput vastaukset koulutuksen pituudesta olivat neutraaleja. Nämä väittämät ja vastausten jakautuminen niissä on esitelty taulukossa 8.

Taulukko 8. Henkilökunnan yleinen arvio koulutuksesta

Väittämä	Samaa mieltä	Neutraali	Eri mieltä
Koulutuksen sisältö oli selkeää ja helposti ymmärrettävää.	81 %	11 %	8 %
Koulutusmateriaalit ja esimerkit olivat käytännönläheisiä.	85 %	15 %	0 %
Koulutus oli sopivan pituinen ja eteni selkeässä tahdissa.	81 %	19 %	0 %

Taulukossa 9 esitellään henkilökunnan itsearvio oppimisestaan. Suurin osa vastaajista koki, että heidän osaamisensa tietoturvasta ja tietosuojasta parani koulutuksen aikana. Peräti 89 % ilmoitti, että koulutus lisäsi heidän tietämystään tietoturvasta ja tietosuojasta, ja paransi ymmärrystä asiakastietojen suojaamisesta. Tyypillisten uhkien tunnistaminen oli parantunut 93 %:n mukaan. Huijausviestiin lankesi yhteensä vain noin 5 %, eli 4 henkilöä 74:stä.

Taulukko 9. Oppiminen ja osaamisen kehittyminen

Väittämä	Samaa mieltä	Neutraali	Eri mieltä
Koulutus lisäsi tietämystäni tietoturvasta ja tietosuojasta.	89 %	11 %	0 %
Ymmärrän nyt paremmin, miten voin suojata asiakastietoja ja estää tietomurtoja.	89 %	11 %	0 %
Osaan tunnistaa yleisimpiä tietoturvauhkia hoivakodissa.	93 %	7 %	0 %
Koulutus auttoi minua ymmärtämään, miksi tietoturva on tärkeää hoivatyössä.	85 %	15 %	0 %

Kyselyn seuraavassa osassa kartoitettiin koulutuksen vaikutuksia työskentelytapoihin henkilökunnan oman arvion mukaan. Taulukko 10 esittää näiden väittämien tulokset. Suurin osa työntekijöistä, 73 %, ilmoitti muuttaneensa omia tietoturvakäytäntöjään koulutuksen myötä. Vastaajat kokivat itsensä myös varmemmaksi ja arvioivat tietävänsä miten toimia kohdatessaan mahdollisen tietoturvariskin. Tulokset viittaavat siihen, että koulutuksella on ollut vaikutus käytännön työhön.

Taulukko 10. Koulutuksen vaikutus työhön

Väittämä	Samaa mieltä	Neutraali	Eri mieltä
Koulutuksen jälkeen olen muuttanut tai tarkentanut tietoturvakäytäntöjäni työssäni.	73 %	23 %	4 %
Tunnen oloni varmemmaksi koulutuksen myötä käyttäessäni digitaalisia järjestelmiä.	81 %	15 %	4 %
Tiedän, miten toimia, jos kohtaan mahdollisen tietoturvariskin tai epäilyttävän tilanteen.	89 %	11 %	0 %

Kyselyssä uutta koulutusta verrattiin aiempaan. Vertailussa nousi esille muun muassa käyttöliittymän selkeys ja sisällön käytännönläheisyys. Suurin osa vastaajista koki uuden koulutuksen selkeämmäksi ja mielekkäämmäksi käydä kuin vanhan.

Taulukossa 11 esitetään henkilökunnan vastauksia uuden ja vanhan koulutuksen vertailusta. Vastaajista 63 % oli sitä mieltä, että uusi koulutus oli selkeämpi ja vastaavasti 68 % koki sen käytännönläheisempänä. Koulutus on 54 %:ssa vastauksia lisännyt varmuutta tietoturvaan kohtaan. Neutraaleja vastauksia oli useammassa väittämässä ja osa vastaajista ei ollut käynyt aikaisempaa koulutusta lainkaan.

Taulukko 11. Uuden ja vanhan koulutuksen vertailu

Väittäjä	Samaa mieltä	Neutraali	Eri mieltä	En ole käynyt vanhaa koulutusta
Tämä koulutus oli selkeämpi kuin aiempi tietoturvakoulutus.	63 %	33 %	0 %	4 %
Tämä koulutus oli käytännönläheisempi kuin aiempi tietoturvakoulutus.	68 %	29 %	0 %	4 %
Tämä koulutus antoi enemmän hyödyllistä tietoa työhöni kuin aiempi koulutus.	68 %	29 %	0 %	4 %
Koin tämän koulutuksen mielenkiintoisemmaksi kuin aiemman koulutuksen.	63 %	33 %	0 %	4 %
Vanhan koulutuksen jälkeen tunsin oloni yhtä varmaksi tietoturva-asioissa kuin nyt uuden käytyäni.	54 %	25 %	17 %	4 %

Taulukoissa 12 ja 13 tarkastellaan vastaajien asennetta uutta koulutusta kohtaan sekä kiinnostusta jatkokoulutukseen. Taulukko 13 esittelee tarkemmin koulutuksen mielekkyyttä ja motivaatiota koskevat vastaukset ja taulukossa 14 taas käsitellään muun muassa halukkuutta osallistua lisäkoulutuksiin.

Taulukon 12 perusteella koulutus on koettu yleisesti motivoivaksi ja mielekkääksi käydä. Vastaajista 81 % ilmoitti olleensa motivoituneita suorittamaan koulutuksen. Loput vastaajista suhtautuivat koulutukseen neutraalisti. Jatkokoulutukseen liittyen 45 % vastaajista ilmaisi halukkuutensa osallistua lisäkoulutukseen tietoturvaan ja tietosuojaan liittyen. Noin 40 % oli neutraaleja lisäkoulutukseen osallistumisesta ja noin 15 % on sitä mieltä, ettei haluaisi suorittaa lisäkoulutusta. Nämä vastaukset käyvät ilmi taulukosta 13.

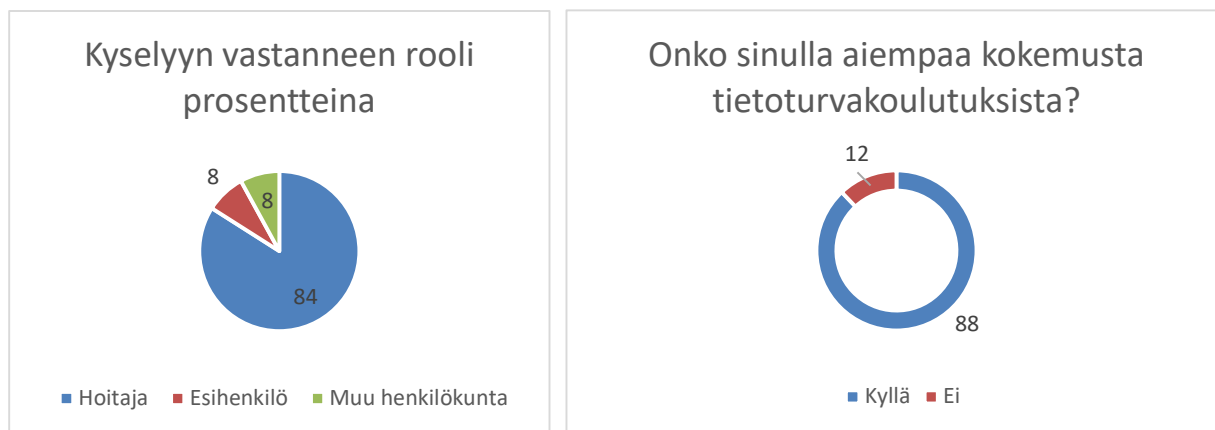
Taulukko 12. Henkilökunnan asenne ja motivaatio

Väittäjä	Samaa mieltä	Neutraali	Eri mieltä
Koin koulutuksen mielekkääksi.	81 %	19 %	0 %
Olin motivoitunut suorittamaan koulutuksen.	81 %	19 %	0 %
Koulutus vahvisti omaa sitoutumistani tietoturvaan ja tietosuojaan.	89 %	11 %	0 %

Taulukko 13. Henkilökunnan kiinnostus ja jatkokoulutus

Väittämä	Samaa mieltä	Neutraali	Eri mieltä
Koulutus oli liian yksinkertainen enkä oppinut paljoa uutta.	19 %	26 %	55 %
Olisin kiinnostunut oppimaan lisää ja osallistumaan useampiin koulutuksiin tietoturvasta ja tietosuojasta.	44 %	41 %	15 %
Näen tietoturva- ja tietosuojakoulutuksen tärkeänä osana ammatillista kehittymistä.	92 %	4 %	4 %

Kuvaajissa 2 ja 3 on esitelty vastanneiden taustatietoja. Kuvaaja 2 näyttää vastaajien roolin ja kuvaaja 3 aikaisemman tietoturvakoulutuksiin osallistumisen. Vastaajista suurin osa, 84 %, työskenteli hoivahenkilökunnan tehtävissä. Esihenkilöitä sekä muuta henkilökuntaa oli 8 %. Valtaosalla, 88 %, on ollut aikaisemmin jotain tietoturvaan ja tietosuojaan liittyvää koulutusta, kun taas noin 12 % ei ole saanut koulutusta aikaisemmin lainkaan.



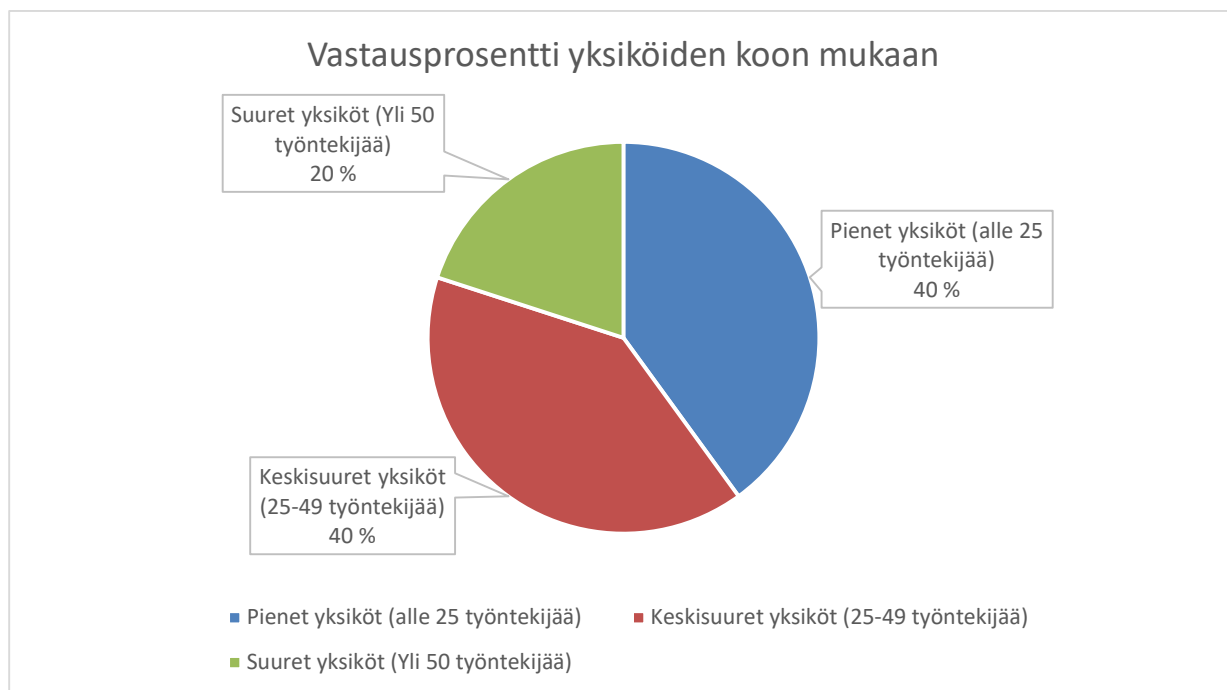
Kuvaajat 2 ja 3: Henkilökunnan kyselyyn vastanneen rooli (vasemmalla) ja aiempi kokemus tietoturvakoulutuksesta (oikealla).

5.2 Johtajien kyselyn tulokset

Johtajien kyselyyn vastauksia saatiin viisi vastausta. Kysely lähetettiin yhteensä 21 johtajalle, joten vastausprosentti jäi alle 25 %:n. Vastausaika oli kaksi viikkoa, ja sen aikana lähetettiin viisi muistutusviestiä. Kysely sisälsi Likert-asteikollisia väittämiä, monivalintakysymyksiä sekä avoimia kysymyksiä. Sen alussa kartoitettiin yksikön koko, jonka jälkeen selvitettiin koulutuksen käyttöönoton sujuvuutta, mielipidettä koulutuksen viestintään liittyen, sekä omien alaisten motivaatiota koulutukseen. Näiden lisäksi selvitettiin johtajien tekemiä toimia koulutuksen jalkauttamiseksi, kohdattuja haasteita sekä mahdollisia kehitysehdotuksia.

Lopuksi haluttiin selvittää, että mitkä asiat olivat toimineet hyvin koulutuksen viemisessä käytäntöön.

Kyselyyn vastanneiden johtajien yksiköiden koko vaihteli. Pienistä yksioistä (alle 25 työntekijää), vastasi kaksi johtajaa, keskisuurista (25-49 työntekijää) myös kaksi johtajaa ja suurista yksiköistä (yli 50 työntekijää) yksi johtaja. Vastaukset on esitetty visuaalisesti kuvaajassa 4.



Kuvaaja 4: Kyselyyn vastanneiden johtajien johtaman yksikön koko.

Kyselyssä tarkasteltiin seuraavaksi koulutuksen käyttöönottoa ja viestintää. Taulukossa 14 ja kuvaajassa 4 on esitetty vastausten jakaumat selkeästi. Suurin osa johtajista koki saaneensa ainakin osittain riittävästi tietoa koulutuksen sisällöstä ja tavoitteista. Taulukosta 14 nähdään, että 40 % koki saaneensa riittävästi tietoa uudesta koulutuksesta sekä sen sisällöstä. Loput johtajista tunsivat saaneensa osittain riittävästi tietoa uudesta koulutuksesta. Koulutuksen organisoinnin viestinnästä 60 % johtajista oli sitä mieltä, että viestintä oli erittäin selkeää, 20 piti sitä selkeänä, ja 20 % tunsu sen olleen epäselvää.

Kyselyssä lisäinformaation tarpeesta nousi esiin toive järjestää erillinen tiedotustilaisuus yksikön johtajille uudesta sekä julkaista lisätiedote intranettiin. Viestintään ja koulutuksesta tiedottamiseen liittyen toivottiin yleisesti enemmän ennakkotietoa koulutuksesta.

Taulukko 14. Johtajien vastaukset viestintään ja käyttöönottoon liittyen

Väittämä	Täysin samaa mieltä	Samaa mieltä
Olen saanut riittävästi tietoa uuden tietosuojan / tietoturvakoulutuksen sisällöstä ja tavoitteista?	40 %	60 %
Koulutuksen käyttöönotto ollut helppo toteuttaa	20 %	80 %



Kuvaaja 3: Johtajien mielipide viestinnän selkeydestä uuteen koulutukseen liittyen.

Johtajista 20 % piti koulutuksen käyttöönottoa helppona ja 80 % melko helppona. Onnistuneiksi tekijöiksi koettiin erityisesti koulutuksen selkeä ja ymmärrettävä sisältö, sen helppo saavutettavuus intranetissä sekä oikea-aikainen ja selkeä ohjeistu koulutukseen.

Yksiköiden johtajat ovat vieneet uutta koulusta käyttöön erilaisin keinoin. He ovat tiedottaneet koulutuksesta palaverissa ja sisäisissä kokouksissa, asettaneet takarajan koulutuksen suorittamiselle, sekä motivoineet henkilökuntaa keskusteluilla. Osa vastaajista kertoi, ettei ole vielä ehtinyt aloittaa uuden koulutuksen viemistä alaisilleen.

Koulutuksen käyttöönotossa ilmeni myös haasteita. Kyselyn mukaan ongelmia liittyi erityisesti aikatauluttamisessa, viestinnässä henkilökunnalle, sekä internetyhteyksissä. Aikatauluttamisesta on noussut kaksi eri haastetta. Pääallekkäisiä koulutuksia on käynnissä

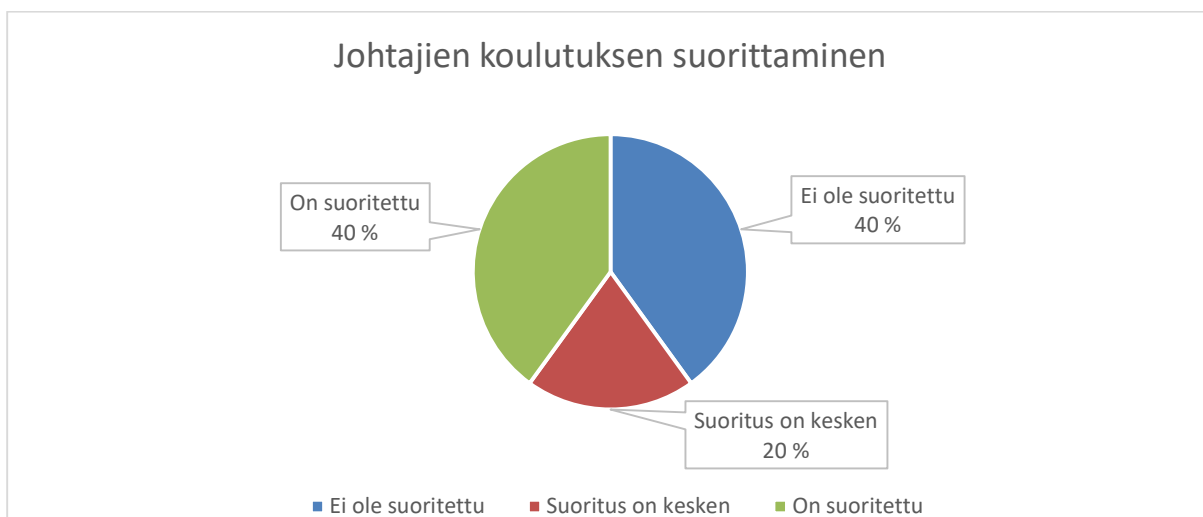
useampia, jonka takia osa henkilökunnasta kokee samanaikaiset koulutukset kuormittaviksi muiden töiden ohessa. Toinen aikataulutukseen liittyvä haaste on ollut, että koulutuksien sovittaminen työajalle on haasteellista.

Taulukossa 15 esitellään johtajien arvio alaistensa sitoutumisesta koulutukseen sekä heidän oma suhtautumisensa koulutukseen. Yksikön johtajat arvioivat henkilökuntansa sitoutuvan koulutukseen pääosin neutraalisti tai myönteisesti: 60 % arvioi henkilökunnan sitoutuvan neutraalisti, ja 20 % myönteisesti, ja 20 % erittäin myönteisesti. Motivoinnin tueksi ehdotettiin automaattisia muistutuksia tekstiviestillä ja sähköpostilla, sekä esihenkilön aktiivisempaa roolia esimerkiksi palkitsemisella. Johtajat uskovat, että koulutus parantaa heidän alaistensa tietoturvan ja tietosuojan ymmärrystä ja sitä myötä parantaa yksikön tietoturvaa ja suojaa.

Johtajien oma asenne oli suurimmaksi osaksi myönteinen, 20 %:lla asenne koulutukseen oli erittäin myönteinen, 60 %:lla myönteinen ja 20 %:lla neutraali. Kuvaajassa 5 havainnollistetaan johtajien koulutuksen suoritusprosentti. Johtajista 40 % oli suorittanut uuden koulutuksen, 20 %:lla suoritus oli vielä kesken ja 40 % ei ollut ehtinyt aloittaa suorittamaan koulutusta.

Taulukko 15. Alaisten suhtautumisen arvio ja oma koulutuksen suoritus

Väittämä	Erittäin myönteinen	Myönteinen	Neutraali
Miten arvioisit henkilökuntasi suhtautumista koulutukseen?	20 %	20 %	60 %
Oletko itse suorittanut koulutuksen?	20 %	60 %	20 %



Kuvaaja 4: Johtajien koulutuksen suorittaminen.

Johtajien kyselyn vastausprosentti jäi alle 25 %. Vastauksia saatiin eri kokoisista yksiköistä, mikä tuo vaihtelua näkökulmaan. Kyselyn perusteella koulutuksen viestintä ja tekninen toteutus, kuten ohjeistus ja koulutuksen löydettävyyden koettiin toimiviksi. Suurimmat haasteet liittyivät koulutuksen aikatauluttamiseen suhteessa muihin koulutuksiin ja työtehtäviin. Johtajien oma asenne koulutusta kohtaan oli selvästi myönteinen ja alaistensa suhtautumista arvioitiin pääosin neutraaliksi.

5.3 NIS2-haastattelun tulokset

Tässä luvussa käsitellään Yrjö ja Hana -kotien IT-johtajan NIS2-haastattelun tulokset. Haastattelu pohjautui luvussa 4.2. esitettyyn viitekehykseen ja jakautui neljään osioon: organisaatorakenne ja vastuut, resurssit ja osaaminen, kulttuuri ja tietoturvatietoisuus sekä kokonaisarvio ja kehitysnäkymät. Tulokset esitetään näiden teemojen mukaisesti omissa alaluvuissaan.

5.3.1 Organisaatorakenne ja vastuut

Yrityksellä on perustason tietoturvakäytännöt. Haastattelussa nousi esiin, että ilmoituskäytäntöjä on harjoiteltu ja niitä käytännössä testattu. Vastuut on pyritty jakamaan selkeästi yrityksen sisällä. Yrityksessä on erikseen nimetty tietoturvavastaava, tietosuojavastaava, sekä näiden lisäksi tietoturvapoikkeamista vastaava työryhmä. Työryhmän tehtävä on käsitellä mahdolliset tietoturva- ja tietosuojapoikkeamat.

Haastateltavalla on rooli tietoturvajohtajana, ja sen lisäksi hän on toimitut IT-vastaavana, ja siten laatinut tarvittavat dokumentaatiot myös NIS2-direktiivia näkökulmasta. Vaikka tietoturva on edustettuna organisaation johdon kokouksissa, sitä ei ole vielä tiiviisti integroitu osaksi kaikkea päätöksentekoa. Haastattelussa kävi ilmi, että tietohallintojohtajan työ hyvinvointipalveluiden organisaatiossa päättyy.

5.3.2 Resurssit ja osaaminen

Haastattelun perusteella suurin resurssija koskeva haaste on aika. Ajankäytön rajallisuus nousi esiin toistuvasti haastattelun aikana. Tietoturvaan ja tietosuojaan vastaavien henkilöiden työkuorma on täysi, vaikka NIS2-direktiivin kaikkia vaatimuksia ei ole vielä otettu käyttöön. Vaikka osaamista ja motivaatiota tietoturvan ja tietosuojan kehittämiseen löytyy, riittävää aikaa ei ole kuitenkaan aina mahdollista järjestää.

Henkilökunnan osaamiseen IT-johtajalla on luottamusta. Osaamista vahvistetaan vuosittain suoritettavalla koulutuksella, jossa oppimista mitataan testauksella ja suorituksia seurataan säännöllisesti online-alustalla. Tietoturvan osalta yritys on suorittanut oman kalasteluviestikampajan aikaisempaan vuonna. Tulokset olivat erittäin positiiviset, yli 90 % henkilökunnasta tunnisti viestin kalasteluviestiksi eikä tietojen kalastelu onnistunut.

5.3.3 Kulttuuri ja tietoturvatietoisuus

IT-johtajan mukaan henkilöstön suhtautuu tietoturvaan ja -suojaan vakavasti. Hänen mukaansa tietosuoja koetaan keskeisenä osana työtä ja yksiköiden johtajat ovat motivoituneita tietoturvaan ja -suojaan kohtaan. Arjen kiire ja operatiivinen työ vievät kuitenkin suurimman osan johtajien työajasta, mikä rajoittaa panostamista tietoturvan kehittämiseen.

Tietoturvasta IT-johtajan mukaan ei käydä keskustelua työpaikkojen epävirallisissa tilanteissa. Hänen näkemyksensä mukaan tämä voi olla jopa hyvä merkki, jos aiheesta keskusteltaisiin enemmän arjessa, saattaisi se viitata siihen, että aihepiiri herättää huolta tai epävarmuutta.

5.3.4 Kokonaisarvio ja kehitysnäkymät

Seuraavaksi haastattelussa siirryttiin käsittelemään yrityksen nykytilaa ja sen kehittämistarpeita suhteessa NIS2-direktiivin vaatimuksiin. Haastattelun perusteella suurimmat haasteet liittyivät ylimmän johdon sitoutumiseen ja ymmärrykseen direktiivin velvoitteista. IT-johtajan mukaan ylimmän johdon sitoutuminen vaatii selkeämpää ymmärrystä johdon roolista ja vastuista NIS2-direktiivin mukaisesti.

NIS2-direktiivin hyödyt hän näkee olevan sidoksissa siihen, että kyseessä on direktiivi, joka pakottaa toimijoita toimimaan sen edellyttämällä tavalla. IT-johtajan mukaan tämä kohottaa yleisesti tietoturvatietoisuutta automaattisesti koko terveydenhuollon sektorin sisällä, mukaan lukien myös Yrjö ja Hanna hyvinvointipalveluiden organisaatiossa.

IT-johtajan mukaan tietoturvanperusta on hyvinvointipalveluiden organisaatiossa hyvällä tasolla, mutta kehitettävää on hyvinvointipalveluiden organisaation ylimmän johdon sitoutumisen osalta. Organisaatiossa on parhaillaan käynnissä rakenneuudistus, jonka myötä roolitus tietoturvan ja tietosuojan ympärillä muuttuu. Tietohallintojohtajan paikka jää kokonaan pois ja se jaetaan tulevaisuudessa tietosuojavaastaavan ja tietoturvavaastaavan kesken.

5.4 Tulosten analyysi ja pohdintaa

Koulutuksen viemisessä käytäntöön ja sitä kautta kyberturvallisuuden parantamisessa palveluyksiköissä viestintä uudesta koulutuksesta on suuressa roolissa. Koulutuksen käyttöönottoa varten tehtiin useita viestintään liittyviä toimia. Johtajistolle pidettiin infotilaisuus kuukausikatsauksen yhteydessä tammikuun lopussa. Tämän lisäksi tästä on tiedotettu intranet-viesteillä. Näiden lisäksi henkilöstölle jaettiin käyttöohjeet koulutuksen suorittamiseen, sekä sen tueksi tuotettiin ohjevideot, miten koulutukseen pääsee ja miten koulutuksen voi suorittaa.

5.4.1 Henkilökunnan kysely

Nämä edellä mainitut toimet ovat vaikuttaneet viestinnän onnistumiseen. Henkilökunnan vastauksista käy ilmi, että 59 % piti koulutuksesta annettua viestintää selkeänä. Suurimmalle osalle viestintää oli ollut riittävästi. Viestinnästä oli ymmärtänyt, että organisaatioon tulee uusi koulutus tietoturvaan ja tietosuojaan liittyen ja se korvaa vanhan koulutuksen. Tekniset ohjeet koulutuksen suorittamiseksi olivat selkeät 82 %:n mielestä. Muistutuksia ja erillisiä ohjeita sähköpostiin intraviestien lisäksi toivottiin muutamassa avoimessa vastauksessa koskien viestinnän ja tiedottamisen ja suoritusohjeiden kysymystä.

Koulutusta kohtaan henkilökunnalla on hyvä asenne. Koulutus koettiin tarpeelliseksi 96 %:ssa vastauksia. Monessa vastauksessa myös korostuu, että koulutus koetaan mielekkääksi ja vastaaja oli motivoitunut suorittamaan koulutuksen. Tämä saattaa selittyä hyvällä koulutuksen käytäntöön viemisellä. Toinen selitys tälle on, että koulutus on uusi, ja nämä henkilöt, jotka ovat suorittaneet koulutuksen heti sen voimaantullessa ovat uteliaita uutta koulutusta kohtaan. Tällöin johtajien panoksella ei ole tähän ollut suurta vaikutusta. Tuloksien perusteella voidaan olettaa, että molemmilla on voinut olla vaikutusta myönteisiin kokemuksiin koulutuksesta. Kyselyissä ei suoraan eritelty näitä tekijöitä mielekkyyden mittaamisessa, eikä siten voida varmasti sanoa, kummasta tekijästä mielekkyys johtuu.

Riippumatta siitä mikä perimmäinen syy tälle hyvälle motivaatiolle on, on yleisesti tärkeää, että henkilökunnan keskuudessa vallitsee hyvä motivaatio ja asenne koulutusta kohtaan. Kunnollinen asenne vahvistaa kokonaisuudessa tietoturvan ja -suojan kulttuuria yrityksessä. Tämän on myös nostettu jo Argyridou ym. [51] teoksessa esille, jossa painotetaan, että henkilöstön asenne ja motivaatio ovat keskeisiä hyvän kyberturvakulttuurin luomisen edellytyksiä. Palveluyksiköiden näkökulmasta paras tilanne olisi, että hyvä motivaatio ja sitä

myötä asenne kumpuaisivat onnistuneesta johtamisesta. Se mahdollistaisi vähemmän motivoituneen henkilökunnan oppia tietoturvaa ja tietosuojaa tehokkaasti tehokkaan johtamisen avulla. Tosin työyhteisössä esimerkillisesti toimimalla voi myös parantaa ympärillä toimivien työntekijöiden kiinnostusta koulutusta kohtaan.

Koulutuksessa käytävät teemat ovat vastausten mukaan käytännönläheisiä, ja sitä kautta niiden voi olettaa tarjoavan ratkaisuja työssä eteen tuleviin haasteisiin. Tyypillinen tilanne työntekijälle on salasanan vaihto tietyin väliajoin. Koulutuksissa käydään perustietoturvaan liittyvät salasanakäytännöt läpi, joten sen myötä esimerkiksi henkilöstön salasanakäytännöt voivat koulutuksen käytyä vahvistua. Kyselyiden tuloksien perusteella koulutus on muovannut henkilöstön tietoturvakäytäntöjä.

Kyselyiden tuloksista nousee esiin, että koulutus on lisännyt henkilöstön varmuutta toimia tietoturvaan ja tietosuojaan liittyvissä tilanteissa. Henkilöstö kokee olevansa entistä valmiimpia tunnistamaan tietoturvariskejä ja muita epäilyttäviä tilanteita arjessa. Tämän perusteella voidaan päätellä, että koulutuksen päivittämisellä on ollut myönteinen vaikutus työntekijöiden toimintaan työssään. Tämä varmuus edistää sujuvampaa ja turvallisempaa työskentelyä hoivakodin ympäristössä. Samalla voidaan todeta, että koulutus tukee tietoturvakulttuurin vahvistumista, kun tietoturvan periaatteet omaksutaan paremmin osaksi päivittäistä työtä.

Yleisesti vastauksista käy ilmi, että koulutus koettiin sisällöllisesti onnistuneeksi. Erityisesti mainintana useassa kommentissa nousi käytännönläheisyys, sekä helppous omaksua uusi koulutus. Tämä on äärimmäisen tärkeässä osassa, sillä jos koulutus on epäselvä, jää opittava asia myös epäselväksi. Koulutuksen ollessa helppo omaksua, paranee myös sen myötä tietoturvan taso yleisesti yrityksessä. Yli 85 % koki, että koulutus tukee heidän ammatillista kasvuaan ja kehittymistä, jonka voi tulkita siten, että motivaatio kehittymiselle on olemassa. Koulutukseen liittyvä viestintä sai paljon kehuja yhdessä teknisten ohjeiden kanssa, avoimien kysymyksien vastauksista nousi tosin hieman kehitettävää tulevaa varten. Kehitysehdotukset liittyvät työajan lomassa tehtävään koulutukseen ja koulutuksiin varatun ajan niukkuuteen.

5.4.2 Johtajien kysely

Palveluyksiköiden johtajilla on tärkeä työ viedä uusi koulutusohjelma alaistensa tietoisuuteen ja sitä kautta käyttöön koko organisaatiossa. Johtajat toimivat ikään kuin linkkinä päätösten ja käytännön välillä. Tätä varten yksiköiden johtajilla on välttämätöntä olla riittävän hyvät

pohjatiedot tällaisesta kokonaisuudesta, sen tavoitteista ja aikatauluista, sekä muista käytännön toimista.

Koulutuksen jalkauttamista varten tehdyillä toimilla on pyritty antamaan palveluyksikön johtajille mahdollisimman hyvät edellytykset viedä käytäntöön eli siis jalkauttaa tämä uusi koulutus. Johtajat saivat lyhyen esityksen uudesta koulutuksesta johtajille tarkoitetussa kuukausittaisessa palaverissa tammikuussa. Tämän lisäksi yrityksen intraviestinnässä asiasta on kerrottu useammassa viestissä. Nämä näkyvät myös kyselyn vastauksissa, sillä yleisesti kysyttäessä viestintään liittyen johtajilta, palaute on ollut hyvää. Annettu viestintä on ollut erittäin selkeää suurimman osan mielestä. Koulutuksen käyttöönotto on sitä myötä ollut helppo toteuttaa.

Vaikka viestintää pidettiin pääosin selkeänä ja onnistuneena, avoimissa vastauksissa esitettiin toive ylimääräisestä kokouksesta tiedottamisen tueksi. Erityisesti pilotoinnin aloitukseen liittyi epävarmuutta sen aikataulusta. Koulutuksen käynnistymistä viivästyttivät tekniset yhteensopivuusongelmat, joiden vuoksi aloitusta jouduttiin siirtämään useaan otteeseen. Lopulta ongelmat saatiin ratkaistua odotettua nopeammin, ja pilotti päätettiin käynnistää nopealla aikataululla. Tämä kuitenkin jätti yksikön johtajalle vain vähän aikaa valmistautua koulutuksen toteuttamiseen.

Walker ym. [58] korostavat, että onnistunut koulutuksen käyttöönotto edellyttää riittäviä resursseja, kuten valmistautumisaikaa. Tässä tapauksessa useaan kertaan muuttunut aikataulu teknisen yhteensopimattomuuden vuoksi ei antanut parasta mahdollista valmistautumista koulutuksen käyttöönottoon. Pilotoidun yksikön johtaja toi tämän esille pilotoinnin palautteessa.

Yksikön johtajilta kysyttiin heidän alaistensa suhtautumista uuteen koulutukseen. Tarkoituksena oli selvittää, poikkeako yksiköiden johtajien käsitys alaistensa asenteesta henkilöstön itsearvioihin vertaamalla. Tämä vertailu on tärkeää, sillä kyberturvakulttuurin kehittäminen vaatii myönteisen asenteen henkilöstöltä, mutta myös johtajien kykyä tunnistaa ja tukea näitä asenteita. Argyridou ym. [51] mukaan tietoturvan tietoisuus on tärkeää. Mehner ym. [56] ja Ismail ym. [57] totesivat omissa tutkimuksissaan esihenkilön asenteella ja tuella olevan keskeinen vaikutus alaistensa motivaatioon osallistua koulutuksiin.

Verrattaessa vastauksia havaittiin, että johtajien ja työntekijöiden arviot asenteista ovat pääosin linjassa keskenään. Johtajat olivat hieman varovaisemmin arvioineet alaistensa motivaatiota,

yleisin vastaus oli neutraali, kun taas henkilökunnalla yleisin vastaus oli ”samaa mieltä”. Johtajien oma asenne kirjallisuuden perusteella olisi riittävä tukemaan koulutuksen käymistä ja siten vahvistaa kyberturvakulttuuria.

Johtajilta kysyttiin keinoista motivoida alaisiaan koulutuksen suorittamiseen. Näissä korostui viestinnän merkitys, erityisesti muistutuksien lähettäminen ja koulutuksesta tiedottaminen. Viestinnän tärkeydestä on mainittu useissa lähteissä [59], [60], [61], jotka korostavat selkeää, oikea-aikaista, riittävää ja laadukasta viestintää. Palkitseminen nousi esille vastauksissa myös keinona lisätä sitoutumista. Se nostetaan myös kirjallisuudessa yhtenä sitoututtamisen keinona [51].

Koulutuksen viemistä käytäntöön on saattanut helpottaa se, että niin johtajat, kuin henkilökuntakin piti koulutusta tarpeellisena. Kyselyn tuloksien mukaan johtajista 80 % piti koulutusta tarpeellisena ja ajankohtaisena. Tämä yhdessä liitettynä henkilökunnan vastauksiin koulutuksen tarpeellisuudesta, joka oli yli 95 %, kertoo siitä, että koulutus on koettu tarpeelliseksi omassa työssä. Näin ollen koulutus on todennäköisesti otettu vastaan paremmin verrattaessa tilanteeseen, jossa molemmat, yksiköiden johtajat, sekä henkilökunta on sitä mieltä, ettei koulutusta olisi tarvittu.

Haasteita mitä johtajat nostavat koulutuksen käyttöönotossa ja yleisesti koulutuksen ympärillä on aikataululliset haasteet. Erityisesti mainitaan se, että koulutuksia on paljon käytävänä ja sen vuoksi koulutuksia pitäisi lomittaa käymällä niitä eri aikaan vuoden mittaan. Osa henkilöstöstä onkin käynyt koulutuksen edeltävänä syksynä, eikä sitä varten käy koulutusta kuin vasta syksyllä 2025. Aikatauluhaasteiden lisäksi yhdessä yksikössä on koettu haasteita teknologian kanssa, sillä kyseisessä yksikössä ei nettiyhteys ole aina toiminut koulutusta käydessä.

5.4.3 NIS2-haastattelu

Organisaation nykytila ja vahvuudet

Haastattelun perusteella yrityksen henkilöstöllä on hallussaan perustiedot tietoturvasta ja niitä osataan soveltaa myös käytännössä. Tätä tukee aikaisemmin toteutettu kalasteluviestisimulaatio sekä yrityksen oma kalasteluviestisimulaatio, joihin vain harva lankesi. Uusi koulutus vahvistaa näitä perustietoturvakäytänteitä ja sen hyvä vastaanotto tukee yrityksen kyberturvakulttuurin kehittämistä.

Organisaatorakenne on pääosin kunnossa. Yrityksessä on erikseen nimetty tietoturvavastaava, sekä tietosuojavastaava. Näiden lisäksi yrityksessä toimii tietoturvapoikkeamien työryhmä,

joka vastaa tietoturvapoikkeamien käsittelystä. Nämä rakenteet täyttävät NIS2-direktiivissä vaatimuksia vastuun jakamisesta. Myös Loonam ym. [53] nostavat selkeän roolituksen esiin kyberturvan sietokyvyn parantamisessa.

Roolimuutokset ja vastuunjaon selvittämistarpeet

Tietohallintojohtajan rooli tullaan sulauttamaan muihin rooleihin ja vastuut siirretään tietoturvavastaavalle ja tietosuojavastaavalle. Muutoksessa vastuunjako tulee toteuttaa erityisen selkeästi dokumentoiden, sillä NIS2-direktiivi edellyttää selkeää vastuunjakoja ja rooleja. Lisäksi kirjallisuudessa korostetaan, että yrityksen ylimmässä johdossa tulisi olla kyberturvallisuudesta nimetty henkilö, esimerkiksi CIO tai CISO [51], [53], mikä tukisi kyberturvakulttuurin kehittämistä ja strategista johtamista.

Poikkeamien hallinta ja koulutuksen rooli

NIS2-direktiivi edellyttää poikkeamien hallintaa ja sen käytäntöjen dokumentointia. Haastattelussa kävi ilmi, että poikkeamien hallintaa on harjoiteltu, ja poikkeamailmoituksia on tehty käytännön tilanteiden vuoksi. Organisaatio on pyrkinyt oppimaan poikkeamista ja kehittänyt käytänteitään niiden perusteella.

Henkilöstön koulutus vuosittain on yksi direktiivin keskeisistä vaatimuksista. Uusi koulutus vastaa tähän velvoitteeseen. Suorituksen seuraaminen tapahtuu palveluyksiköiden johtajien ja tietoturva- ja tietosuojavastaavien toimesta onlinealustalla. Johtajien tehtävä on varmistaa alaistensa koulutuksen suoritukset ajallaan. Näihin perusteella voidaan todeta osaamisen tason olevan hyvä.

Toimitusketjujen hallinta

Yrityksen oma tietohallinto valvoo alihankkijoiden toimitusketjuja. Yhteistyökumppaneilta edellytetään ISO 27001-sertifiontia. Auditoinnista ja toimittajien tarkistuksesta vastaavat nimetyt henkilöt, joiden vastuulla on varmistaa direktiivin noudattaminen toimitusketjujen turvallisuuden osalta.

Kehityskohteet ja avoimet kysymykset

Vaikka osa direktiivin vaatimuksista on täytetty, haastattelu ja tarkentavat lisäkysymykset paljastavat kehitettävää muutamilla osa-alueilla. Avoimiksi kysymyksiksi jäivät

tietoturvaliikkeen päivitystiheys ja riskienhallinnan käytännön toteutus. Nämä molemmat ovat NIS2-direktiivin edellyttämiä vaatimuksia.

Haastattelussa ilmeni, että organisaatiolla on tietoturvaliikka, mutta sen päivityskäytännöistä ei saatu tarkkaa tietoa. Riskienhallinta on ollut tietohallintojohtajan vastuulla ja se sisälsi riskien vakavuuden ja todennäköisyyden arviointia, joista laadittiin riskimatriisi. Tämä matriisi raportoidaan johtoryhmälle.

Haastattelun perusteella suurimmaksi direktiivin vaatimuksien täyttämisen esteeksi nousee ajanpuute. Ajanpuute on noussut kaikissa kolmessa kyselyssä tai haastattelussa esille, ja se on kirjallisuudessaakin tunnistettu yhdeksi esteeksi tietoturvan edistämiseksi [32].

5.5 Onnistumisia, parannettavaa ja kehitysehdotuksia

Tässä kappaleessa tarkastellaan työn onnistumisia ja haasteita. Aluksi käsitellään toimia, jotka ovat onnistuneet tai toteutuneet hyvin ja sen jälkeen siirrytään osa-alueille, joissa on ollut ongelmia tai parannettavaa. Epäonnistumisien yhteydessä pohditaan mitä olisi voitu tehdä toisin ja lopuksi esitetään kehitysehdotuksia tulevaisuutta varten.

5.5.1 Onnistumiset

Kappaleissa 5.1 ja 5.2 käsiteltiin henkilökunnalle ja palveluyksiköiden johtajille suunnattuja kyselyitä. Näiden tavoitteena oli arvioida uuden koulutuksen jalkauttamista. Molempien kyselyiden perusteella viestintä uudesta koulutuksesta on ollut onnistunutta. Intraviestintä, ohjeistus ja esihenkilöille annettu esitelmä ja tiedotteet on koettu selkeiksi, ja viestintää on ollut suurimman osan mielestä riittävästi. Koulutuksen suorittamisen tekniset ohjeet arvioitiin erittäin hyviksi. Teknisiä ohjeita koulutuksen käyttöön on laadittu sekä kirjallisina ohjeina että ohjevideoina, jossa näytetään mistä koulutuksen löytää ja miten koulutukseen pääsee ja miten koulutusalueita käytetään.

Johtajat jalkauttivat koulutusta yksiköihinsä eri tavoin. Jalkautus on onnistunut yksiköihin kyselyiden perusteella pääsääntöisesti hyvin. Asenne uutta koulutusta kohtaan on myönteinen, mikä näkyi vastauksista henkilöstön ja esihenkilöiden vastauksien lisäksi myös IT-johtajan haastattelussa. Tämä on tärkeä havainto yrityksen kyberturvallisuuden tietoisuuden kehittämistä ajatellen. Argyridou ym. [51] korostavat kyberturvallisuuden tietoisuuden kehittämistä ja henkilökunnan myönteinen asenne tukee tätä.

5.5.2 Parannettavaa ja kehitysehdotuksia

Kokonaisuudessaan koulutuksen suorittaneiden määrä organisaatiossa jäi alhaiseksi. Yhtenä syynä tähän on se, että työntekijöillä on velvollisuus suorittaa tietoturvakoulutus vain vuosittain. Suurimmalla osalla henkilökunnasta koulutus on suoritettu syksyllä 2024, jolloin heillä koulutuksen suorittaminen on ajankohtainen vasta syksyllä 2025. Tähän olisi mahdollista puuttua motivoimalla tai pakottamalla henkilökuntaa suorittaa tämä uusi koulutus nopeammin. Motivointiin keinoja kirjallisuudesta nostetaan muutama. Argyridou ym. [51] mainitsevat palkinnot, sekä teemaviikot, joiden avulla voidaan lisätä tietoisuutta ja motivoida työntekijöitä suorittaa tämä uusi koulutus nopeammalla tahdilla. Toinen mahdollisuus on lyhentää koulutusväliä esimerkiksi kaksi kertaa vuodessa suoritettavaksi.

Sekä henkilökunnan, että johtajien avoimissa vastauksissa tuotiin esille kehitysehdotuksia tulevaisuuden koulutuksien käyttöönottoa varten. Vaikka viestintä saikin yleisesti positiivista palautetta kyselyiden perusteella, osa vastaajista koki, että olisivat tarvinneet ylimääräisen intraviestin tai esimerkiksi palaverin uuden koulutuksen käyttöönotosta. Tulevia koulutuksia käyttöönotettaessa tulee varmistaa riittävä viestintä järjestämällä esimerkiksi kaikille avoin kyselytuokio koulutusta varten. Pilotin osalta tekniset murheet hankaloittivat pilotoinnin aloitusta ja sekoittivat sen aikataulua, mikä korostui pilotoinnin palautteessa.

Myös NIS2-direktiiviin liittyen havaittiin kehitettävää. Haastattelussa ei kaikkia osa-alueita käyty kattavasti läpi, mutta esimerkiksi säännöllisistä toimista tietoturvapoliitiikan säännöllinen tarkistus ja riskien säännöllinen arviointi vaativat vielä jatkotoimia tietohallintojohtajan roolin loputtua. Aikaisemmin nämä ovat olleet tietohallintojohtajan vastuulla. Tehtävät tulee jakaa sopiville henkilöille ja jako tulee dokumentoida selkeästi.

Johdon sitouttaminen direktiivin vaatimuksiin on tehtävä ennen määräajan umpeutumista 8.7.2025. Johdon tulee ymmärtää oma vastuunsa erityisesti riskienhallinnan osalta. Tähän mennessä pitää olla myös selkeät käytänteet riskien arvioimiselle, sekä niiden dokumentoimiselle ja seurantaan.

Riskienhallintaprosessiin voidaan hyödyntää NIST:n CSF-viitekehystä. Se tarjoaa kattavat ja yleisesti hyväksytyt keinot riskienhallintaan monelta eri osa-alueelta. CSF:n Governance osiossa (Gov.RM) eritellään riskienhallintaprosessien määrittelyä, prosessien arviointia ja parantamista [50, s. 16].

Jatkossa organisaation tulee laatia käytännönläheinen kuvaus riskienhallinnan toteutukseen. Dokumentista pitäisi käydä ilmi arvioinnin ajankohta, sen vastuuhenkilöt, riskien vakavuuden arviointitapa, sekä riskien dokumentointikäytännöt. Tavoitteena tällä tavoin toimiessa olisi varmistaa, että prosessi on mahdollisimman läpinäkyvä ja helposti omaksuttavissa myös vastuiden siirtyessä uusille henkilöille.

6 Yhteenveto

Tämän diplomityön tavoitteena oli tukea Yrjö ja Hanna kotien hyvinvointipalveluiden organisaatiota uuden tietoturva- sekä tietosuojakoulutuksen käyttöönotossa, sekä arvioida organisaation valmiutta NIS2-direktiivin vaatimuksiin. Tutkimuksessa vastattiin kolmeen tutkimuskysymykseen (TK), jotka käsittelivät koulutuksen käyttöönottoa, sen vaikutuksia kyberturvallisuuskulttuuriin ja NIS2-valmiutta. Tutkimuskysymykset ovat:

TK1: Millä tavoin voidaan mahdollisimman hyvin ottaa käyttöön uusi koulutusohjelma?

TK2: Onko uudella koulutuksella havaittavissa vaikutuksia kyberturvallisuuskulttuurin edistymiseen hoivakotiyrityksessä?

TK3: Kuinka hyvin hoivakotiorganisaatio on valmistautunut NIS2:een?

Tutkimus toteutettiin tapaustutkimuksena. Tutkimuskysymyksiin vastaamisen aloitettiin tiedonkeruusta. Tietoa kerättiin kirjallisuudesta ja kyselyillä henkilökunnalta ja johtajilta, sekä haastattelulla. Kyselyihin pyydettiin vastaukset etenkin pilotoiduilta henkilöiltä, mutta myös muilta koulutuksen suorittaneilta. Haastatteluun osallistui organisaation tietohallintojohtaja.

Henkilökunnan ja johtajien kyselyissä pyrittiin selvittämään kunkin ryhmän asennetta uutta koulutusta kohtaan. Tämän lisäksi tavoitteena oli selvittää sekä työntekijän että johtajan näkökulmista, miten hyvin koulutus oli organisoitu, miten hyvin siitä oli viestitty ja kuinka hyvin se oli onnistuttu viemään organisaation käyttöön. Johtajilta kysyttiin tarkemmin keinoja, joita he ovat käyttäneet koulutuksen käyttöönotossa omassa yksikössään.

Kyselyissä henkilökunnan tulokset olivat, että henkilökunnan asenne uutta koulutusta kohtaan on myönteinen. Lisäksi koulutus koettiin hyväksi ja helposti ymmärrettäväksi sisältönsä puolesta. Koulutuksen suorittamiseen varattu aika koettiin suurimmaksi esteeksi sen suorittamiselle.

Palveluysiköiden johtajien kyselyssä selvitettiin heidän asennettaan koulutukseen, joka oli vastausten perusteella myönteinen. Heidän toimistaan koulutuksen jalkauttamiseksi esille nousi viikoittaiset palaverit, joissa koulutuksesta kerrottiin useampaan otteeseen. Palveluysiköiden johtajat näkivät suurimpana esteenä koulutuksen käyttöönotolle ajanpuutteen. Organisaatiossa on päällekkäin monta koulutusta, joita tulee suorittaa vuosittaisella aikajaksolla, eikä hoitotyöstä voi koulutuksien vuoksi paljoa joustaa.

Organisaation tietohallintojohtajalle pidettiin haastattelu yrityksen NIS2-valmiuteen liittyen. Haastattelun tavoitteena oli saada kattava kuva Yrjö ja Hanna kotien valmiuden tilasta. Tällä pyrittiin auttamaan yritystä tunnistamaan täytetyt velvoitteet ja puutokset niissä, ja siten keskittyä velvoitteisiin, jotka vaativat vielä toimia.

IT-johtajan mukaan organisaation NIS2-valmius on kokonaisuutena melko hyvällä tasolla. Vaatimuksien täyttämiseksi hän nostaa esille ylimmän johdon roolia ja vastuun ymmärtämistä, joita tulisi vielä vahvistaa ennen määräajan umpeutumista. Ajanpuute nousee haastattelun perusteella keskeiseksi rajoittavaksi tekijäksi näille tavoitteille.

6.1 Vastaukset tutkimuskysymyksiin

Vastattaessa tutkimuskysymykseen 1 ”Millä tavoin on paras tapa ottaa käyttöön uusi koulutusohjelma?” keskeisiä tekijöitä on löydetty aiemmin esitellystä kirjallisuudesta. Useissa tutkimuksissa korostettiin johdon roolia erityisesti aktiivisen tukemisen, kannustamisen ja esimerkin näyttämisenä. Muita tärkeitä seikkoja onnistuneessa käyttöönotossa on selkeä, oikea-aikainen ja riittävä viestintä, sekä yleisesti riittävät resurssit, kuten myönteinen ilmapiiri ja riittävä aika koulutukselle.

Tutkimuskysymykseen 2, eli ”Onko uudella koulutuksella havaittavissa vaikutuksia kyberturvallisuuskulttuurin edistymiseen hoivakotiyrityksessä?” voidaan vastata myöntävästi kyselyiden tulosten perusteella. Tuloksista käy ilmi, että koulutuksella on ollut vaikutuksia henkilöstön asenteisiin ja käyttäytymiseen tietoturva- ja tietosuojasioissa. Vastanneista 96 % koki koulutuksen olleen tarpeellinen ja 90 % vastaajista arvioi heidän tietotaitonsa tietoturvaa kohtaan parantuneen. Lisäksi yli 70 % ilmoitti muokanneensa koulutuksen myötä omia aikaisempia toimintatapoja tietoturvaan liittyen. Lähes 95 % piti tietoturva- ja tietosuojakoulutusta tärkeänä osana omaa ammatillista kehitystä, sekä lähes 45 % vastanneista ilmaisi halunsa saada lisää tietoturvaan ja -suojaan liittyvää koulutusta. Näiden kaikkien tulosten perusteella voidaan todeta, että koulutus on vaikuttanut positiivisesti kyberturvakulttuurin kehittymiseen organisaatiossa.

Tutkimuskysymykseen 3 ”Miten hyvin hoivakoti on valmistautunut NIS2-direktiiviin?” vastaus perustuu NIS2-haastatteluun ja tarkentaviin kysymyksiin. Näiden perusteella hyvinvointipalveluiden organisaation valmius on pääosin hyvällä tasolla. Useat direktiivin keskeiset vaatimukset täyttyvät nykyisellään. Joiltain osin vaatimuksenmukaisuuden täyttäminen vaatii kuitenkin vielä lisätoimia. Kehittämistarpeita tunnistettiin erityisesti

riskienhallinnan prosessien dokumentoinnissa ja johdon roolin ja vastuun määrittelyssä direktiivin edellyttämällä tasolla.

6.2 Työn rajoitukset ja tulevaisuuden kehityskohteet

Tämän työn tulosten yleiselle käytettävyydelle esteenä on vastausten vähäisyys. Vastauksia saatiin kyselyiden avulla henkilökunnalta niukasti ja se vaikuttaa vastauksien yleistettävyyteen suuremmissa mittakaavassa. Johtajien osalta vastauksia on todella niukasti ja siellä yksittäisellä vastauksella on paljon vaikutusta tuloksiin, joka täytyy ottaa huomioon tuloksia yleistettäessä Yrjö ja Hanna kotien organisaation ulkopuolelle.

Työn tulosten perusteella kehityskohteita yksilöiden näkökulmasta olisivat kohdennetut koulutukset motivoituneimmille henkilökunnassa. Kyselyiden mukaan lähes 45 % olisi valmis jatkokoulutukseen tietoturvasta ja -suojasta. Tämä mahdollistaisi organisaation sisällä paremman kyberturvallisuustilanteen, jos henkilökunnalle on tarjolla enemmän kursseja kyberturvaan liittyen.

Työ tarjoaa selkeän rungon, jonka varaan organisaatio voi rakentaa tulevien koulutuksien jalkauttamisen. Tämän avulla voitaisiin laatia vaiheittainen ohjeistus käytännön toimista koulutuksien käyttöönoton toteutukseen. Uuden koulutuksen vastaanotto on ollut myönteinen. Kehitettävää kuitenkin on erityisesti motivoinnissa palautteen antamiseen. Laajempi palaute mahdollistaisi kattavamman kuvan onnistumisista ja parannettavista kohteista koulutuksen jalkauttamisessa.

Vaikka tutkielman tulokset ovat lupaavia, ne eivät ole riittävän kattavia, niin, että niitä voisi suoraan yleistää yhteiskunnalliselle tasolle. Jotta tämän työn tuloksia voitaisiin soveltaa laajemmin esimerkiksi kansallisen tason kehitystyössä, tarvittaisiin tarkempi ja systemaattisempi menetelmä koulutuksen vaikuttavuuden arviointiin. Tällainen menetelmä voisi mitata esimerkiksi henkilökunnan käytöksen ja asenteen muuttumista nykyistä ajanjaksoa pidemmällä aikavälillä ja siten tarjota tarkemman kuvan koulutuksen vaikutuksista. Kun menetelmän voidaan osoittaa tuottavan luotettavia tuloksia, voisi sitä käyttää esimerkiksi alan suosituksissa. Tämä voisi siten luoda perustan tehokkaalle kyberturvallisuustyölle koko terveydenhuoltosektorin läpi.

Lähdeluettelo

- [1] ENISA, ”Education and career path”. Viitattu: 21. toukokuuta 2025. [Verkossa]. Saatavissa: <https://www.enisa.europa.eu/topics/education-and-career-path>
- [2] European Union Agency for Cybersecurity., *2024 report on the state of cybersecurity in the Union*. LU: Publications Office, 2024. Viitattu: 21. toukokuuta 2025. [Verkossa]. Saatavissa: <https://data.europa.eu/doi/10.2824/0401593>
- [3] Euroopan Unioni, *Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555*, vsk. 333. 2022. Viitattu: 2. tammikuuta 2025. [Verkossa]. Saatavissa: <http://data.europa.eu/eli/dir/2022/2555/oj/fin>
- [4] Yrjö ja Hanna Kodit, ”Kodit”. Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://yrjojahanna.fi/kodit/>
- [5] Yrjö ja Hanna Kodit, ”Arvot”. Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://yrjojahanna.fi/saatio/arvot/>
- [6] Euroopan Unioni, *Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148*, vsk. 194. 2016. Viitattu: 11. kesäkuuta 2025. [Verkossa]. Saatavissa: <http://data.europa.eu/eli/dir/2016/1148/oj/fin>
- [7] Uniqkey, ”Why NIS2?”, The NIS2 Directive. Viitattu: 21. toukokuuta 2025. [Verkossa]. Saatavissa: <https://nis2directive.eu/why-nis2/>
- [8] C. Wohlin ja A. Aurum, ”Towards a decision-making structure for selecting a research design in empirical software engineering”, *Empirical Software Engineering*, vsk. 20, nro 6, ss. 1427–1455, joulukuuta 2015, doi: 10.1007/s10664-014-9319-7.
- [9] Tietosuojavaltuutetun toimisto, ”Data protection”. Viitattu: 2. tammikuuta 2025. [Verkossa]. Saatavissa: <https://tietosuoja.fi/en/data-protection>
- [10] European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council*. Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- [11] L. Coventry ja D. Branley, ”Cybersecurity in healthcare: A narrative review of trends, threats and ways forward”, *Maturitas*, vsk. 113, ss. 48–52, heinäkuuta 2018, doi: 10.1016/j.maturitas.2018.04.008.
- [12] Tietosuojavaltuutetun toimisto, ”Tietosuojavastaavat”. Viitattu: 22. toukokuuta 2025. [Verkossa]. Saatavissa: <https://tietosuoja.fi/tietosuojavastaavat>
- [13] M. Nieves, K. Dempsey, ja V. Y. Pillitteri, ”An introduction to information security”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-12r1, kesäkuuta 2017. doi: 10.6028/NIST.SP.800-12r1.
- [14] I. Neil, *CompTIA Security+: SY0-601 Certification Guide: Complete coverage of the new CompTIA Security+ (SY0-601) exam.*, 2. p. Birmingham: Packt Publishing Limited, 2020.
- [15] IBM Security, ”Cost of a Data Breach Report 2024”, heinäkuuta 2024, Viitattu: 10. tammikuuta 2025. [Verkossa]. Saatavissa: <https://www.ibm.com/reports/data-breach>
- [16] A. Kolehmainen, ”Verkkokauppa.com sai Suomessa ennätysuuret gdpr-sakot”, Tivi. Viitattu: 17. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://www.tivi.fi/uutiset/verkkokauppa-com-sai-suomessa-ennatysuuret-gdpr-sakot/1c029976-de8a-47e3-9444-832bc8c22275>
- [17] Traficom, ”Kyberturvallisuuslaki on hyväksytty eduskunnassa - NIS2-direktiivin mukaiset velvoitteet astuvat voimaan 8.4.2025”, Traficom. Viitattu: 29. huhtikuuta 2025. [Verkossa]. Saatavissa: <https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksytty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet>
- [18] *Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 703/2023*. Oikeusministeriö, Edita Lakitieto Oy. Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://www.finlex.fi/fi/lainsaadanto/saadoksokokoelma/2023/703>
- [19] *Tietosuojalaki 1050/2018*. Oikeusministeriö, Edita Lakitieto Oy. Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>
- [20] H. Liu, K. Li, Y. Chen, ja X. (Robert) Luo, ”Is personally identifiable information really more valuable? Evidence from consumers’ willingness-to-accept valuation of their privacy

- information”, *Decision Support Systems*, vsk. 173, s. 114010, loka 2023, doi: 10.1016/j.dss.2023.114010.
- [21] Aluehallintovirasto, ”Tietoa meistä”. Viitattu: 3. helmikuuta 2025. [Verkossa]. Saatavissa: <https://avi.fi/tietoa-meista>
- [22] Aluehallintovirasto, ”Valvomme - Toimintamme - Tietoa meistä”. Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://avi.fi/tietoa-meista/toimintamme/valvomme>
- [23] Valvira, ”Sosiaali- ja terveydenhuollon viranomaisvalvonta”. Viitattu: 3. helmikuuta 2025. [Verkossa]. Saatavissa: <https://valvira.fi/sosiaali-ja-terveydenhuolto/viranomaisvalvonta>
- [24] Aluehallintovirasto, ”Vanhuspalvelulain toimeenpanoa on tuettu aktiivisella ohjauksella ja neuvonnalla, Tiedote 4.1.2021”. Viitattu: 3. helmikuuta 2025. [Verkossa]. Saatavissa: <https://avi.fi/tiedote/-/tiedote/69897671>
- [25] THL, ”Määräys 3/2024 Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista”. Terveyden ja Hyvinvoinnin laitos, 20. helmikuuta 2024. Viitattu: 3. huhtikuuta 2025. [Verkossa]. Saatavissa: https://thl.fi/documents/155392151/190361269/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf/9123733d-c1ae-09f5-e05d-a33894441c6c/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf?t=1708438054468
- [26] IBM Security, ”Cost of a Data Breach Report 2023”, heinä 2023, [Verkossa]. Saatavissa: <https://www.ibm.com/downloads/cas/E3G5JMBP>
- [27] IBM Security, ”Cost of a Data Breach Report 2022”, heinä 2022, [Verkossa]. Saatavissa: <https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf>
- [28] C. Hadnagy ja S. Wozniak, *Social engineering: the science of human hacking*. Indianapolis, Indiana: Wiley, 2018. doi: 10.1002/9781119433729.
- [29] G. Bridgers, C. Hausman, A. Tomeo, ja G. Vellala Umapathy, *Phishing for Dummies*, Cisco Special Edition. teoksessa *For Dummies*. Hoboken, NJ: Wiley, 2023.
- [30] S. Nifakos *ym.*, ”Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review”, *Sensors*, vsk. 21, nro 15, s. 5119, heinä 2021, doi: 10.3390/s21155119.
- [31] Joint Task Force Transformation Initiative, ”Guide for conducting risk assessments”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.
- [32] Y. He, A. Aliyu, M. Evans, ja C. Luo, ”Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review”, *Journal of Medical Internet Research*, vsk. 23, nro 4, s. e21747, huhti 2021, doi: 10.2196/21747.
- [33] F. Gioulekas *ym.*, ”A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures”, *Healthcare*, vsk. 10, nro 2, s. 327, helmi 2022, doi: 10.3390/healthcare10020327.
- [34] S. T. Argaw *ym.*, ”Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks”, *BMC Medical Informatics and Decision Making*, vsk. 20, nro 1, s. 146, joulu 2020, doi: 10.1186/s12911-020-01161-7.
- [35] Q. Chen ja R. A. Bridges, ”Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware”, teoksessa *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, Mexico: IEEE, joulu 2017, ss. 454–460. doi: 10.1109/ICMLA.2017.0-119.
- [36] Z. Liu, C. Chen, L. Y. Zhang, ja S. Gao, ”Working Mechanism of Eternalblue and Its Application in Ransomworm”, teoksessa *Cyberspace Safety and Security*, X. Chen, J. Shen, ja W. Susilo, Toim., Cham: Springer International Publishing, 2022, ss. 178–191. doi: 10.1007/978-3-031-18067-5_13.
- [37] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, ja P. Aylin, ”A retrospective impact analysis of the WannaCry cyberattack on the NHS”, *NPJ Digital Medicine*, vsk. 2, nro 1, s. 98, loka 2019, doi: 10.1038/s41746-019-0161-6.
- [38] IBM, ”SMB protocol”. Viitattu: 5. helmikuuta 2025. [Verkossa]. Saatavissa: <https://www.ibm.com/docs/ai/7.3?topic=management-smb-protocol>

- [39] National Audit Office, "Investigation: WannaCry cyber attack and the NHS - NAO report". Viitattu: 4. helmikuuta 2025. [Verkossa]. Saatavissa: <https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/>
- [40] NSA, "United States of America v. Park Jin Hyok – Criminal Complaint in the United States District Court for the Central District of California. | National Security Archive". NSA, 8. kesäkuuta 2018. Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://nsarchive.gwu.edu/document/18208-national-security-archive-2018-09-06-park>
- [41] H. Ghanbari ja K. Koskinen, "When data breach hits a psychotherapy clinic: The Vastaamo case", *Journal of Information Technology Teaching Cases*, s. 20438869241258235, kesä 2024, doi: 10.1177/20438869241258235.
- [42] J. C. Looi *ym.*, "Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers", *Australasian Psychiatry*, vsk. 33, nro 1, ss. 106–110, helmi 2025, doi: 10.1177/10398562241291340.
- [43] Yle, "Vastaamo board fires CEO, says he kept data breach secret for year and a half", News. Viitattu: 13. helmikuuta 2025. [Verkossa]. Saatavissa: <https://yle.fi/a/3-11614603>
- [44] J. Harju, "Vastaamon tietomurto | Vastaamo-jutun Kivimäki välttyi uusilta syyteiltä, koska tuomio ei voisi enää paljon koventua", *Helsingin Sanomat*, loka 2024, Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://www.hs.fi/suomi/art-2000010786908.html>
- [45] Tietosuojaavaltuutetun toimisto, "Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista". Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://tietosuoja.fi/-/psykoterapiakeskus-vastaamolle-seuraamusmaksu-tietosuojarikkomuksista>
- [46] S. Korhonen, "Vastaamon entinen toimitusjohtaja tuomittiin tietosuojarikoksesta", Tivi. Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://www.tivi.fi/uutiset/yle-vastaamon-entinen-toimitusjohtaja-tuomittiin-tietosuojarikoksesta/0807b333-cca3-400a-aaec-436255b23c2b>
- [47] T. Wolke, *Risk management*. Berlin ; Boston: De Gruyter Oldenbourg, 2017.
- [48] C. Abraham, D. Chatterjee, ja R. R. Sims, "Muddling through cybersecurity: Insights from the U.S. healthcare industry", *Business Horizons*, vsk. 62, nro 4, ss. 539–548, heinä 2019, doi: 10.1016/j.bushor.2019.03.010.
- [49] International Organization for Standardization, "ISO/IEC 27001:2022". Viitattu: 16. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://www.iso.org/standard/27001>
- [50] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0", National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, helmi 2024. doi: 10.6028/NIST.CSWP.29.
- [51] E. Argyridou *ym.*, "Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study", *Journal of Medical Internet Research*, vsk. 25, s. e41294, heinä 2023, doi: 10.2196/41294.
- [52] Center for Internet Security, "CIS Controls v8.1". Center for Information Security, elokuuta 2024. Viitattu: 21. maaliskuuta 2025. [Verkossa]. Saatavissa: <https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf>
- [53] J. Loonam, J. Zwiegelaar, V. Kumar, ja C. Booth, "Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective", *IEEE Transactions on Engineering Management*, vsk. 69, nro 6, ss. 3757–3770, joulukuuta 2022, doi: 10.1109/TEM.2020.2996175.
- [54] Skhole, "Hoitoalan koulutukset henkilökunnallesi kustannustehokkaasti verkossa". Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://www.skhole.fi/>
- [55] Navisec, "Tietosuojakoulutus verkossa". Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://www.navisec.fi/>
- [56] L. Mehner, S. Rothenbusch, ja S. Kauffeld, "How to maximize the impact of workplace training: a mixed-method analysis of social support, training transfer and knowledge sharing", *European Journal of Work and Organizational Psychology*, vsk. 34, nro 2, ss. 201–217, maaliskuuta 2025, doi: 10.1080/1359432X.2024.2319082.
- [57] A. Ismail, M. J. Asha'ari, S. N. A. Foboy, W. N. W. Hanafi, A. M. Nor, ja T. Husin, "Moving Up Trainees' Motivation for Using On-job Training: Relationship between Leaders' Support and Trainees' Motivation for Learning", *The South East Asian Journal of Management*, vsk. 18, nro 1, ss. 28–53, huhtikuuta 2024, doi: 10.21002/seam.v18i1.1475.

- [58] T. J. Walker *ym.*, ”Development of a comprehensive measure of organizational readiness (motivation \times capacity) for implementation: a study protocol”, *Implementation Science Communications*, vsk. 1, nro 1, s. 103, joulu 2020, doi: 10.1186/s43058-020-00088-4.
- [59] L. A. Fidler ja J. D. Johnson, ”Communication and Innovation Implementation”, *The Academy of Management Review*, vsk. 9, nro 4, s. 704, loka 1984, doi: 10.2307/258492.
- [60] W. Peng ja D. Litteljohn, ”Organisational communication and strategy implementation – a primary inquiry”, *International Journal of Contemporary Hospitality Management*, vsk. 13, nro 7, ss. 360–363, joulu 2001, doi: 10.1108/EUM0000000006005.
- [61] L. K. Lewis, ”Employee Perspectives on Implementation Communication as Predictors of Perceptions of Success and Resistance”, *Western Journal of Communication*, vsk. 70, nro 1, ss. 23–46, helmi 2006, doi: 10.1080/10570310500506631.
- [62] A. van Welie, ”Legislation within cybersecurity: preparing for NIS2 – a detailed framework in the healthcare sector in the Netherlands”, Pro Gradu-tutkielma, Turun yliopisto, 2024. Viitattu: 5. marraskuuta 2024. [Verkossa]. Saatavissa: <https://www.utupub.fi/handle/10024/178884>

Liitteet

Liite 1: Palautekysely johtajille uudesta tietosuoja- ja tietoturvakoulutuksesta.

Taustatiedot

Kirjoita palveluyksikkösi _____

Kuinka suuri yksikkö sinulla on johdettavana?

- Alle 25 työntekijää
- Yli 25, mutta alle 50 työntekijää
- Yli 50, mutta alle 75 työntekijää
- Yli 75 työntekijää

Käyttöönoton viestintä ja selkeys

Koulutuksen käyttöönotto ja viestintä (Rastita sopiva kohta joka riviltä):

TSM = Täysin samaa mieltä, SM = Samaa mieltä, N = Neutraali, OER = Osittain eri mieltä, TER= Täysin eri mieltä

	TSM	SM	N	OER	TER
Olen saanut riittävästi tietoa koulutuksen sisällöstä ja tavoitteista	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Koulutuksen käyttöönotto ollut helppo toteuttaa	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Miten arvioisit koulutuksen viestinnän selkeyttä?

- Erittäin selkeää
- Selkeää
- Epäselvää
- Erittäin epäselvää

Oletko onnistunut viemään koulutuksen palveluyksikkösi?

- Olen onnistunut täysin
- Olen onnistunut osittain
- En ole onnistunut lainkaan
- En ole aloittanut vielä
- Koen, että se ei ole minun tehtäväni

Olisitko kaivannut lisää informaatiota? (Valitse kaikki sopivat)

- En kaivannut
- Erillinen ylimääräinen tiedote
- Oma kokous
- Enemmän intraviestintää
- Muu, mikä: _____

Miten parantaisit viestintää ja koulutuksen käyttöönottoa jatkossa?

Sitoutuminen ja osallistuminen

Kuinka suuri osa henkilökunnastasi on suorittanut tai aloittanut koulutuksen?

- 100 %
- 75–99 %
- 50–74 %
- Alle 50 %
- En osaa sanoa

Miten arvioisit henkilökuntasi suhtautumista koulutukseen?

- Erittäin myönteinen
- Myönteinen
- Neutraali
- Kielteinen
- Erittäin kielteinen

Millaisena itse koet suhtautumisesi koulutukseen?

- Erittäin myönteinen
- Myönteinen
- Neutraali
- Kielteinen
- Erittäin kielteinen

Oletko itse suorittanut koulutuksen?

- En ole
- Kesken – olen aloittanut mutta koulutus on kesken
- Olen suorittanut koulutuksen

Millä keinoin parantaisit henkilökunnan sitoutumista koulutukseen?

Vaikutukset ja käytännön toteutus

Koulutus on parantanut henkilökunnan ymmärrystä tietosuojasta ja tietoturvasta:

- Täysin samaa mieltä
- Osittain samaa mieltä
- Neutraali
- Osittain eri mieltä
- Täysin eri mieltä

Kuinka paljon uskot koulutuksella olevan vaikutusta yksikkösi tietoturvaan ja tietosuojaan?

- Selvästi
- Jonkin verran
- Vähäisesti
- Ei lainkaan
- En osaa sanoa

Mitkä asiat koulutuksessa olivat onnistuneita? (Valitse kaikki sopivat)

- Selkeä ja ymmärrettävä sisältö
- Helppo saavutettavuus

- Ajankohtaisuus ja tarpeellisuus
- Selkeä ja ajoitettu viestintä
- Riittävä tuki ja ohjeistus
- Muu, mikä: _____

Mitä haasteita kohtasit koulutuksen jalkauttamisessa? (Valitse kaikki sopivat)

- En ole kohdannut merkittäviä haasteita
- Tekniset ongelmat
- Aikataulutus
- Henkilöstön asenne
- Epäselvä viestintä
- Tuen puute
- Sisällön epäsopivuus käytäntöön
- Muu, mikä: _____

Mitä kehitysehdotuksia sinulla on uusien koulutusten viestintään, käytettävyyteen ja saavutettavuuteen liittyen?

Liite 2: Palautekysely henkilökunnalle uuteen tietoturva- ja tietosuojakoulutukseen

KOULUTUKSEN ORGANISOINTI JA TIEDOTTAMINEN

1. Koulutuksen organisointi ja tiedottaminen

(Arvioi asteikolla 1–5: 1 = Täysin eri mieltä, 5 = Täysin samaa mieltä)

Sain koulutuksesta ja sen suorittamisesta selkeät ohjeet.

1 2 3 4 5

Koulutuksen aikataulu ja suoritustapa oli minulle selkeä.

1 2 3 4 5

Koulutuksen tiedottaminen (esim. sähköposti, intra, esihenkilö) oli riittävää.

1 2 3 4 5

Koulutuksen suorittamiseen liittyvät tekniset ohjeet olivat selkeitä.

1 2 3 4 5

Koen, että minulla oli riittävästi aikaa suorittaa koulutus.

1 2 3 4 5

2. Miten koulutuksista tiedottamista tai suoritusohjeita voisi jatkossa parantaa?

YLEINEN ARVIO KOULUTUKSESTA

3. Koulutuksen sisältö ja toteutus (Arvioi asteikolla 1–5)

Koulutuksen sisältö oli selkeää ja helposti ymmärrettävää.

1 2 3 4 5

Koulutusmateriaalit ja esimerkit olivat käytännönläheisiä.

1 2 3 4 5

Koulutus oli sopivan pituinen ja eteni selkeässä tahdissa.

1 2 3 4 5

OPPIMINEN JA OSAAMISEN KEHITTYMINEN

4. Arvioi seuraavia väittämiä

(Arvioi asteikolla 1–5: 1 = Täysin eri mieltä, 5 = Täysin samaa mieltä)

Koulutus lisäsi tietämystäni tietoturvasta ja tietosuojasta.

1 2 3 4 5

Ymmärrän nyt paremmin, miten voin suojata asiakastietoja ja estää tietomurtoja.

1 2 3 4 5

Osaan tunnistaa yleisimpiä tietoturvauhkia hoivakodissa.

1 2 3 4 5

Koulutus auttoi minua ymmärtämään, miksi tietoturva on tärkeää hoivatyössä.

1 2 3 4 5

KOULUTUKSEN VAIKUTUS TYÖHÖN

5. Arvioi seuraavia väittämiä

(Arvioi asteikolla 1–5: 1 = Täysin eri mieltä, 5 = Täysin samaa mieltä)

Koulutuksen jälkeen olen muuttanut tai tarkentanut tietoturvakäytäntöjäni työssäni.

1 2 3 4 5

Tunnen oloni varmemmaksi koulutuksen myötä käyttäessäni digitaalisia järjestelmiä.

1 2 3 4 5

Tiedän, miten toimia, jos kohtaan mahdollisen tietoturvariskin tai epäilyttävän tilanteen.

1 2 3 4 5

VERTAILU AIEMPAAN KOULUTUKSEEN

6. Arvioi seuraavia väittämiä

(Arvioi asteikolla 1–5: 1 = Täysin eri mieltä, 5 = Täysin samaa mieltä)

Tämä koulutus oli selkeämpi kuin aiempi tietoturvakoulutus.

1 2 3 4 5

Tämä koulutus oli käytännönläheisempi kuin aiempi tietoturvakoulutus.

1 2 3 4 5

Tämä koulutus antoi enemmän hyödyllistä tietoa työhöni kuin aiempi koulutus.

1 2 3 4 5

Koin tämän koulutuksen mielenkiintoisemmaksi kuin aiemman.

1 2 3 4 5

Vanhan koulutuksen jälkeen tunsin oloni yhtä varmaksi kuin uuden koulutuksen käytyäni.

1 2 3 4 5

7. Miten tämä koulutus erosi aiemmasta koulutuksesta?

8. Oliko uudessa koulutuksessa jotain, mitä vanhassa ei ollut, mutta koit hyödylliseksi?

9. Mitä vanhassa koulutuksessa oli paremmin kuin tässä uudessa?

KOULUTUKSEN TOTEUTUS JA PALAUTE

10. Mikä koulutuksessa toimi mielestäsi parhaiten?

11. Oliko koulutuksessa jotain, mitä et ymmärtänyt tai koit vaikeaksi omaksua?

12. Onko sinulla muuta palautetta koulutuksen järjestämisestä tai sisällöstä?

SUHTAUTUMINEN KOULUTUKSEEN

13. Oliko koulutus mielestäsi tarpeellinen?

Kyllä

Ei

14. Asenne ja motivaatio (Arvioi asteikolla 1–5)

Koin koulutuksen mielekkääksi.

1 2 3 4 5

Olin motivoitunut suorittamaan koulutuksen.

1 2 3 4 5

Koulutus vahvisti omaa sitoutumistani tietoturvaan ja tietosuojaan.

1 2 3 4 5

15. Kokemus ja kiinnostus jatkossa (Arvioi asteikolla 1–5)

Koulutus oli liian yksinkertainen enkä oppinut paljoa uutta.

1 2 3 4 5

Oloisin kiinnostunut oppimaan lisää ja osallistumaan useampiin koulutuksiin.

1 2 3 4 5

Näen tietoturva- ja tietosuojakoulutuksen tärkeänä osana ammatillista kehittymistä.

1 2 3 4 5

TAUSTATIEDOT

16. Mikä on roolisi hoivakodissa?

Hoitaja

Esihenkilö

Muu: _____

17. Onko sinulla aiempaa kokemusta tietoturvakoulutuksista?

Kyllä

Ei

Liite 3: NIS2 valmiuden haastattelukysymykset

NIS2 Vaatimukset

EU:n NIS2-direktiivi (2024 lokakuu) tuo seuraavia velvoitteita terveydenhuollon organisaatioille, joita pidetään "olennaisina toimijoina":

Tietoturvapoikkeamien raportointi:

Ilmoitus Traficomille *24 tunnin kuluessa* tapahtumasta.

Seurantatiedot *72 tunnin kuluessa*.

Lopullinen raportti *1 kuukauden kuluessa*.

Tietoturvatoinenpiteet ja riskienhallinta:

Riskienarviointi (esim. uhkamallit, vaikutusarviot).

Teknisten ja organisatoristen toimenpiteiden (hallinta, teknologia, prosessit) dokumentointi ja toteutus.

Tietoturvatietoisuuden ja -koulutuksen parantaminen:

Säännölliset koulutukset koko henkilöstölle vuosittain.

Johdon osallistaminen ja vastuiden määrittely.

Tietoturvajohtaminen osana liiketoiminnan johtamista:

Tietoturva integroitu osaksi johtamisrakenteita.

Vastuuhenkilö(t) nimetty.

Toimittajaketjun hallinta:

Arvioidaan ja hallitaan ulkoisten kumppaneiden kyberturvariskejä.

Dokumentointi ja raportointivalmiudet:

Suunnitelmat, toimenpiteet ja raportit tallessa, tarvittaessa viranomaisille esitettävissä.

I: Organisaatorakenne ja vastuut

1. Miten NIS2-direktiivin vaatimukset näkyvät tällä hetkellä yrityksen johtamisessa ja hallintorakenteessa?
-
2. Onko organisaatiossa selkeä vastuunjako kyberturvallisuuteen liittyen?
-
3. Millainen rooli sinulla on NIS2:n edellyttämässä turvallisuusprosesseissa?
-
4. Onko tietoturva osa liiketoiminnan strategista suunnittelua?
-

II: Resurssit ja osaaminen

5. Koetko, että organisaatiolla on riittävästi resursseja (aikaa, osaamista, työkaluja) vastata NIS2:n vaatimuksiin?
-
6. Mitkä resurssit ovat tällä hetkellä riittämättömät tai haastavimmat?
-
7. Miten henkilökunnan osaamista kyberturvallisuudessa kehitetään tällä hetkellä?
-

III: Kulttuuri ja tietoturvatietoisuus

8. Millaisena koet henkilöstön yleisen suhtautumisen kyberturvaan?
-
9. Onko kyberturva osa jokapäiväistä keskustelua yksiköissä, vai jääkö se irralliseksi?
-
10. Miten organisaatio reagoi tietoturvapoikkeamiin tällä hetkellä?
-
11. Ovatko johdon esimerkki ja sitoutuminen havaittavissa tietoturva-asioissa?
-

IV: Kokonaisarvio ja kehitysnäkymät

12. Mitkä ovat keskeisimmät haasteet, joita näet matkalla kohti NIS2-vaatimusten täyttämistä?
-
13. Mitä mahdollisuuksia tai hyötyjä näet NIS2-direktiivissä organisaationne kannalta?
-
14. Miten arvioisit nykytilanteen kypsyystasoa NIS2:n näkökulmasta (esim. asteikolla 1–5)?

-

Liite 4: Henkilöstölle lähetetty kalasteluviesti

Hei,

Minulla on tällä hetkellä ongelmia oman työtilini (etunimi.sukunimi@yrjojahanna.fi) salasanan toimimisen kanssa ja jouduin sen päivittämään, jotta ongelma katosi. Teethän sinäkin niin, jos ongelmaa on tililläsi esiintynyt, jotta voit käyttää tiliäsi.

Sen vuoksi lähetän tämän PowerPointin toisesta sähköpostistani.

Muista käydä päivittämässä salasanasasi!

Voit tehdä sen tästä linkistä: [Salasanan vaihtolinkki](#)

Liitteenä on materiaali koskien uusia yleisiä käytänteitä. Käythän sen läpi mahdollisimman pian sillä sisältö liittyy käytännön toimintaan kevään aikana.

[Uudet käytänteet 2025.pptx](#)

Kiitos ja aurinkoista viikon jatkoa!

Ystävällisin terveisin,

Palveluyksikkö XX

Hoivakodin johtaja

Etunimi Sukunimi

Liite 5: Tekoälyn käyttö työssä

Linkki keskusteluun

<https://chatgpt.com/share/685009da-22c0-8007-b5a6-364a8f6fec15>

Keskustelun kehote ja ChatGPT (versio 4) vastaus kehotteeseen alla.

- [1] ENISA, ”Education and career path”. Viitattu: 21. toukokuuta 2025. [Verkossa]. Saatavissa: <https://www.enisa.europa.eu/topics/education-and-career-path>
- [2] European Union Agency for Cybersecurity., 2024 report on the state of cybersecurity in the Union. LU: Publications Office, 2024. Viitattu: 21. toukokuuta 2025. [Verkossa]. Saatavissa: <https://data.europa.eu/doi/10.2824/0401593>
- [3] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, vsk. 333. 2022. Viitattu: 2. tammikuuta 2025. [Verkossa]. Saatavissa: <http://data.europa.eu/eli/dir/2022/2555/oj/fin>
- [4] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, vsk. 194. 2016. Viitattu: 11. kesäkuuta 2025. [Verkossa]. Saatavissa: <http://data.europa.eu/eli/dir/2016/1148/oj/fin>
- [5] ”Why NIS2?”, The NIS2 Directive. Viitattu: 21. toukokuuta 2025. [Verkossa]. Saatavissa: <https://nis2directive.eu/why-nis2/>
- [6] C. Wohlin ja A. Aurum, ”Towards a decision-making structure for selecting a research design in empirical software engineering”, *Empir. Softw. Eng.*, vsk. 20, nro 6, ss. 1427–1455, joulou 2015, doi: 10.1007/s10664-014-9319-7.
- [7] ”Kodit - Yrjö ja Hanna Kodit”. Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://yrjojahanna.fi/kodit/>
- [8] ”Arvot - Yrjö ja Hanna Kodit”. Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://yrjojahanna.fi/saatio/arvot/>
- [9] ”Data protection | Data Protection Ombudsman’s Office”, Tietosuojavaltuutetun toimisto. Viitattu: 2. tammikuuta 2025. [Verkossa]. Saatavissa: <https://tietosuoja.fi/en/data-protection>
- [10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://eur-lex.europa.eu/eli/dir/2016/680/oj>
- [11] L. Coventry ja D. Branley, ”Cybersecurity in healthcare: A narrative review of trends, threats and ways forward”, *Maturitas*, vsk. 113, ss. 48–52, heinä 2018, doi: 10.1016/j.maturitas.2018.04.008.
- [12] ”Tietosuojavastaavat”, Tietosuojavaltuutetun toimisto. Viitattu: 22. toukokuuta 2025. [Verkossa]. Saatavissa: <https://tietosuoja.fi/tietosuojavastaavat>
- [13] M. Nieves, K. Dempsey, ja V. Y. Pillitteri, ”An introduction to information security”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-12r1, kesä 2017. doi: 10.6028/NIST.SP.800-12r1.

- [14] I. Neil, CompTIA Security+: SY0-601 Certification Guide: Complete coverage of the new CompTIA Security+ (SY0-601) exam., 2. p. Birmingham: Packt Publishing Limited, 2020.
- [15] IBM Security, ”Cost of a Data Breach Report 2024”, 2024, Viitattu: 10. tammikuuta 2025. [Verkossa]. Saatavissa: <https://www.ibm.com/reports/data-breach>
- [16] ”Kyberturvallisuuslaki on hyväksytty eduskunnassa - NIS2-direktiivin mukaiset velvoitteet astuvat voimaan 8.4.2025”, Traficom. Viitattu: 29. huhtikuuta 2025. [Verkossa]. Saatavissa: <https://traficom.fi/fi/ajankohtaista/kyberturvallisuuslaki-hyvaksyty-eduskunnassa-nis2-direktiivin-mukaiset-velvoitteet>
- [17] FINLEX ® - Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 703/2023. Oikeusministeriö. Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://www.finlex.fi/fi/lainsaadanto/saaduskokoelma/2023/703>
- [18] E. L. Oy, FINLEX ® - Tietosuojalaki 1050/2018. Oikeusministeriö, Edita Lakitieto Oy. Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://www.finlex.fi/fi/laki/ajantasa/2018/20181050>
- [19] H. Liu, K. Li, Y. Chen, ja X. (Robert) Luo, ”Is personally identifiable information really more valuable? Evidence from consumers’ willingness-to-accept valuation of their privacy information”, Decis. Support Syst., vsk. 173, s. 114010, loka 2023, doi: 10.1016/j.dss.2023.114010.
- [20] ”Tietoa meistä”, Aluehallintovirasto. Viitattu: 3. helmikuuta 2025. [Verkossa]. Saatavissa: <https://avi.fi/tietoa-meista>
- [21] ”Valvomme - Toimintamme - Tietoa meistä”, Aluehallintovirasto. Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://avi.fi/tietoa-meista/toimintamme/valvomme>
- [22] ”Sosiaali- ja terveydenhuollon viranomaisvalvonta”, Valvira. Viitattu: 3. helmikuuta 2025. [Verkossa]. Saatavissa: <https://valvira.fi/sosiaali-ja-terveydenhuolto/viranomaisvalvonta>
- [23] ”Vanhuspalvelulain toimeenpanoa on tuettu aktiivisella ohjauksella ja neuvonnalla, Tiedote 4.1.2021”, Aluehallintovirasto. Viitattu: 3. helmikuuta 2025. [Verkossa]. Saatavissa: <https://avi.fi/tiedote/-/tiedote/69897671>
- [24] ”Valvira - Strategia”, Valvira. Viitattu: 25. tammikuuta 2025. [Verkossa]. Saatavissa: <https://valvira.fi/strategia>
- [25] THL, ”THL Määräys 3/2024 Tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista”. Terveyden ja Hyvinvoinnin laitos, 20. helmikuuta 2024. Viitattu: 3. huhtikuuta 2025. [Verkossa]. Saatavissa: https://thl.fi/documents/155392151/190361269/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf/9123733d-c1ae-09f5-e05d-a33894441c6c/THL_Maarays_3_2024_Tietoturvasuunnitelmaan_sisallytettavista_sevityksista_ja_vaatimuksista.pdf?t=1708438054468
- [26] IBM Security, ”Cost of a Data Breach Report 2023”, [Verkossa]. Saatavissa: <https://www.ibm.com/downloads/cas/E3G5JMBP>
- [27] IBM Security, ”Cost of a Data Breach Report 2022”.

- [28] C. Hadnagy ja S. Wozniak, *Social engineering: the science of human hacking*. Indianapolis, Indiana: Wiley, 2018. doi: 10.1002/9781119433729.
- [29] G. Bridgers, C. Hausman, A. Tomeo, ja G. Vellala Umopathy, *Phishing for Dummies*, Cisco Special Edition. teoksessa *For Dummies*. Hoboken, NJ: Wiley.
- [30] S. Nifakos ym., ”Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review”, *Sensors*, vsk. 21, nro 15, s. 5119, heinä 2021, doi: 10.3390/s21155119.
- [31] Joint Task Force Transformation Initiative, ”Guide for conducting risk assessments”, National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.
- [32] Y. He, A. Aliyu, M. Evans, ja C. Luo, ”Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review”, *J. Med. Internet Res.*, vsk. 23, nro 4, s. e21747, huhti 2021, doi: 10.2196/21747.
- [33] F. Gioulekas ym., ”A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures”, *Healthcare*, vsk. 10, nro 2, s. 327, helmi 2022, doi: 10.3390/healthcare10020327.
- [34] S. T. Argaw ym., ”Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks”, *BMC Med. Inform. Decis. Mak.*, vsk. 20, nro 1, s. 146, joulu 2020, doi: 10.1186/s12911-020-01161-7.
- [35] X. Chen, J. Shen, ja W. Susilo, Toim., *Cyberspace Safety and Security: 14th International Symposium, CSS 2022, Xi’an, China, October 16–18, 2022, Proceedings*, vsk. 13547. teoksessa *Lecture Notes in Computer Science*, vol. 13547. Cham: Springer International Publishing, 2022. doi: 10.1007/978-3-031-18067-5.
- [36] Q. Chen ja R. A. Bridges, ”Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware”, teoksessa *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Cancun, Mexico: IEEE, joulu 2017, ss. 454–460. doi: 10.1109/ICMLA.2017.0-119.
- [37] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, ja P. Aylin, ”A retrospective impact analysis of the WannaCry cyberattack on the NHS”, *Npj Digit. Med.*, vsk. 2, nro 1, s. 98, loka 2019, doi: 10.1038/s41746-019-0161-6.
- [38] ”SMB protocol -IBM”. Viitattu: 5. helmikuuta 2025. [Verkossa]. Saatavissa: <https://www.ibm.com/docs/ai/aix/7.3?topic=management-smb-protocol>
- [39] ”Investigation: WannaCry cyber attack and the NHS - NAO report”, National Audit Office (NAO). Viitattu: 4. helmikuuta 2025. [Verkossa]. Saatavissa: <https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/>
- [40] NSA, ”United States of America v. Park Jin Hyok – Criminal Complaint in the United States District Court for the Central District of California. | National Security Archive”. NSA, 8. kesäkuuta 2018. Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://nsarchive.gwu.edu/document/18208-national-security-archive-2018-09-06-park>

- [41] H. Ghanbari ja K. Koskinen, "When data breach hits a psychotherapy clinic: The Vastaamo case", *J. Inf. Technol. Teach. Cases*, s. 20438869241258235, kesä 2024, doi: 10.1177/20438869241258235.
- [42] J. C. Looi ym., "Cybersecurity lessons from the Vastaamo psychotherapy data breach for psychiatrists and other mental healthcare providers", *Australas. Psychiatry*, vsk. 33, nro 1, ss. 106–110, helmi 2025, doi: 10.1177/10398562241291340.
- [43] "Vastaamo board fires CEO, says he kept data breach secret for year and a half", *News*. Viitattu: 13. helmikuuta 2025. [Verkossa]. Saatavissa: <https://yle.fi/a/3-11614603>
- [44] J. Harju, "Vastaamon tietomurto | Vastaamo-jutun Kivimäki välttyi uusilta syytteiltä, koska tuomio ei voisi enää paljon koventua", *Hels. Sanomat*, loka 2024, Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://www.hs.fi/suomi/art-2000010786908.html>
- [45] Tietosuojavaltuutetun toimisto, "Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista", Tietosuojavaltuutetun toimisto. Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://tietosuoja.fi/-/psykoterapiakeskus-vastaamolle-seuraamusmaksu-tietosuojarikkomuksista>
- [46] S. Korhonen, "Vastaamon entinen toimitusjohtaja tuomittiin tietosuojarikoksesta", *Tivi*. Viitattu: 12. kesäkuuta 2025. [Verkossa]. Saatavissa: <https://www.tivi.fi/uutiset/yle-vastaamon-entinen-toimitusjohtaja-tuomittiin-tietosuojarikoksesta/0807b333-cca3-400a-aaec-436255b23c2b>
- [47] T. Wolke, *Risk management*. Berlin ; Boston: De Gruyter Oldenbourg, 2017.
- [48] C. Abraham, D. Chatterjee, ja R. R. Sims, "Muddling through cybersecurity: Insights from the U.S. healthcare industry", *Bus. Horiz.*, vsk. 62, nro 4, ss. 539–548, heinä 2019, doi: 10.1016/j.bushor.2019.03.010.
- [49] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0", National Institute of Standards and Technology, Gaithersburg, MD, NIST CSWP 29, helmi 2024. doi: 10.6028/NIST.CSWP.29.
- [50] E. Argyridou ym., "Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations: Concept Study", *J. Med. Internet Res.*, vsk. 25, s. e41294, heinä 2023, doi: 10.2196/41294.
- [51] "CIS Controls v8.1". Center for Information Security, elokuuta 2024. Viitattu: 21. maaliskuuta 2025. [Verkossa]. Saatavissa: <https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf>
- [52] J. Loonam, J. Zwiendelaar, V. Kumar, ja C. Booth, "Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective", *IEEE Trans. Eng. Manag.*, vsk. 69, nro 6, ss. 3757–3770, joulu 2022, doi: 10.1109/TEM.2020.2996175.
- [53] "Hoitoalan koulutukset henkilökunnallesi kustannustehokkaasti verkossa | Skhole". Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://www.skhole.fi/>
- [54] "Tietosuojakoulutus verkossa". Viitattu: 23. toukokuuta 2025. [Verkossa]. Saatavissa: <https://www.navisec.fi/>

- [55] L. Mehner, S. Rothenbusch, ja S. Kauffeld, ”How to maximize the impact of workplace training: a mixed-method analysis of social support, training transfer and knowledge sharing”, *Eur. J. Work Organ. Psychol.*, vsk. 34, nro 2, ss. 201–217, maaliskuu 2025, doi: 10.1080/1359432X.2024.2319082.
- [56] A. Ismail, M. J. Asha’ari, S. N. A. Foboy, W. N. W. Hanafi, A. M. Nor, ja T. Husin, ”Moving Up Trainees’ Motivation for Using On-job Training: Relationship between Leaders’ Support and Trainees’ Motivation for Learning”, *South East Asian J. Manag.*, vsk. 18, nro 1, ss. 28–53, huhtikuu 2024, doi: 10.21002/seam.v18i1.1475.
- [57] T. J. Walker ym., ”Development of a comprehensive measure of organizational readiness (motivation × capacity) for implementation: a study protocol”, *Implement. Sci. Commun.*, vsk. 1, nro 1, s. 103, joulukuu 2020, doi: 10.1186/s43058-020-00088-4.
- [58] L. A. Fidler ja J. D. Johnson, ”Communication and Innovation Implementation”, *Acad. Manage. Rev.*, vsk. 9, nro 4, s. 704, lokakuu 1984, doi: 10.2307/258492.
- [59] W. Peng ja D. Litteljohn, ”Organisational communication and strategy implementation – a primary inquiry”, *Int. J. Contemp. Hosp. Manag.*, vsk. 13, nro 7, ss. 360–363, joulukuu 2001, doi: 10.1108/EUM0000000006005.
- [60] L. K. Lewis, ”Employee Perspectives on Implementation Communication as Predictors of Perceptions of Success and Resistance”, *West. J. Commun.*, vsk. 70, nro 1, ss. 23–46, helmikuu 2006, doi: 10.1080/10570310500506631.
- [61] A. van Welie, ”Legislation within cybersecurity: preparing for NIS2 – a detailed framework in the healthcare sector in the Netherlands”, *Pro Gradu-tutkielma*, Turun yliopisto, 2024. Viitattu: 5. marraskuuta 2024. [Verkossa]. Saatavissa: <https://www.utupub.fi/handle/10024/178884>

Voitko auttaa muotoilemaan lähteet kuntoon. Voitko poistaa ne lähteet mille ei tarvitse tehdä mitään tästä listasta ja jättää ne mitä tarvitsee muokata. Kaikissa pitäisi olla kirjoittajat alussa aina! Lisäksi kaikki kirjoittajat pitäisi olla mainittuna, jos niitä ei ole enemmän kuin 10, eli EI esim. Nifakos ym. Lisäksi pitäisi koittaa avata kaikki lehtien lyhenteet, niitä ei saisi olla.

Käytän Zotero plug inia Wordin mukana, jos sen asetuksia voisi muokata jotenkin?

ChatGPT sanoi:

Mietti 1m 14s

Alla ovat vain ne lähteet, jotka yhä rikkovat antamiasi sääntöjä – kaikki muut (numerot, joita ei näy) olivat jo ok. Suluissa on lyhyt muistilappu siitä, mikä kunkin kohdalla täytyy korjata.

[5] ”Why NIS2?”, *The NIS2 Directive*. Viitattu: 21. toukokuuta 2025. (Puuttuu kirjoittaja/organisaatio alussa)

- [6] C. Wohlin ja A. Aurum, ”Towards a decision-making structure for selecting a research design in empirical software engineering”, *Empir. Softw. Eng.* vsk. 20, nro 6, ss. 1427–1455, jouluku 2015. (Lehden nimen lyhenne)
- [7] ”Kodit - Yrjö ja Hanna Kodit”. Viitattu: 23. toukokuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [8] ”Arvot - Yrjö ja Hanna Kodit”. Viitattu: 23. toukokuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [9] ”Data protection | Data Protection Ombudsman’s Office”, Tietosuojavaltuutetun toimisto. Viitattu: 2. tammikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [12] ”Tietosuojavastaavat”, Tietosuojavaltuutetun toimisto. Viitattu: 22. toukokuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [16] ”Kyberturvallisuuslaki on hyväksytty ...”, Traficom. Viitattu: 29. huhtikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [19] H. Liu, K. Li, Y. Chen ja X. (R.) Luo, ”Is personally identifiable information really more valuable? ...”, *Decis. Support Syst.* vsk. 173, 2023. (Lehden nimen lyhenne)
- [20] ”Tietoa meistä”, Aluehallintovirasto. Viitattu: 3. helmikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [21] ”Valvomme - Toimintamme - Tietoa meistä”, Aluehallintovirasto. Viitattu: 23. toukokuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [22] ”Sosiaali- ja terveydenhuollon viranomaisvalvonta”, Valvira. Viitattu: 3. helmikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [23] ”Vanhuspalvelulain toimeenpanoa ...”, Aluehallintovirasto. Viitattu: 3. helmikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [24] ”Valvira - Strategia”, Valvira. Viitattu: 25. tammikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [30] S. Nifakos ym., ”Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review”, *Sensors*, vsk. 21, nro 15, 2021. (“ym.” → listaa kaikki kirjoittajat)
- [32] Y. He, A. Aliyu, M. Evans ja C. Luo, ”Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review”, *J. Med. Internet Res.*, vsk. 23, nro 4, 2021. (Lehden nimen lyhenne)
- [33] F. Gioulekas ym., ”A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures”, *Healthcare*, vsk. 10, nro 2, 2022. (“ym.” → kaikki kirjoittajat)
- [34] S. T. Argaw ym., ”Cybersecurity of Hospitals ...”, *BMC Med. Inform. Decis. Mak.*, vsk. 20, nro 1, 2020. (Lehden nimen lyhenne + “ym.”)
- [37] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi ja P. Aylin, ”A retrospective impact analysis of the WannaCry cyberattack on the NHS”, *NPJ Digit. Med.*, vsk. 2, nro 1, 2019. (Lehden nimen lyhenne)
- [38] ”SMB protocol - IBM”. Viitattu: 5. helmikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)

- [39] ”Investigation: WannaCry cyber attack and the NHS - NAO report”, National Audit Office. Viitattu: 4. helmikuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [41] H. Ghanbari ja K. Koskinen, ”When data breach hits a psychotherapy clinic: The Vastaamo case”, *J. Inf. Technol. Teach. Cases*, 2024. (Lehden nimen lyhenne)
- [42] J. C. Looi ym., ”Cybersecurity lessons from the Vastaamo psychotherapy data breach ...”, *Australas. Psychiatry*, vsk. 33, nro 1, 2025. (Lehden nimen lyhenne + ”ym.”)
- [43] ”Vastaamo board fires CEO, says he kept data breach secret for year and a half”, *Yle*. Viitattu: 13. helmikuuta 2025. (Puuttuu kirjoittaja)
- [44] J. Harju, ”Vastaamon tietomurto ...”, *Hels. Sanomat*, loka 2024. (Lehden nimen lyhenne)
- [48] C. Abraham, D. Chatterjee ja R. R. Sims, ”Muddling through cybersecurity ...”, *Bus. Horiz.*, vsk. 62, nro 4, 2019. (Lehden nimen lyhenne)
- [50] E. Argyridou ym., ”Cyber Hygiene Methodology for Raising Cybersecurity and Data Privacy Awareness in Health Care Organizations”, *J. Med. Internet Res.*, vsk. 25, 2023. (Lehden nimen lyhenne + ”ym.”)
- [51] ”CIS Controls v8.1”. Center for Internet Security, elokuu 2024. (Puuttuu organisaatio kirjoittajaksi)
- [52] J. Loonam, J. Zwiendelaar, V. Kumar ja C. Booth, ”Cyber-Resiliency for Digital Enterprises ...”, *IEEE Trans. Eng. Manag.*, vsk. 69, nro 6, 2022. (Lehden nimen lyhenne)
- [53] ”Hoitoalan koulutukset henkilökunnallesi ...”, *Skhole*. Viitattu: 23. toukokuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [54] ”Tietosuojakoulutus verkossa”, *Navisec*. Viitattu: 23. toukokuuta 2025. (Puuttuu organisaatio kirjoittajaksi)
- [55] L. Mehner, S. Rothenbusch ja S. Kauffeld, ”How to maximize the impact of workplace training ...”, *Eur. J. Work Organ. Psychol.*, vsk. 34, nro 2, 2025. (Lehden nimen lyhenne)
- [56] A. Ismail ym., ”Moving Up Trainees’ Motivation ...”, *South East Asian J. Manag.*, vsk. 18, nro 1, 2024. (Lehden nimen lyhenne + ”ym.”)
- [57] T. J. Walker ym., ”Development of a comprehensive measure of organizational readiness ...”, *Implement. Sci. Commun.*, vsk. 1, nro 1, 2020. (Lehden nimen lyhenne + ”ym.”)
- [58] L. A. Fidler ja J. D. Johnson, ”Communication and Innovation Implementation”, *Acad. Manage. Rev.*, vsk. 9, nro 4, 1984. (Lehden nimen lyhenne)
- [59] W. Peng ja D. Litteljohn, ”Organisational communication and strategy implementation ...”, *Int. J. Contemp. Hosp. Manag.*, vsk. 13, nro 7, 2001. (Lehden nimen lyhenne)
- [60] L. K. Lewis, ”Employee Perspectives on Implementation Communication ...”, *West. J. Commun.*, vsk. 70, nro 1, 2006. (Lehden nimen lyhenne)

Vinkit Zoteron kanssa

Täydet lehden nimet:

Avaa Zotero → Edit → Preferences → Cite → Word Processors → Style Manager.

Valitse käyttämäsi CSL-tyyli ja paina Edit Style → korvaa <short-title form="short"> jne. niin, että journal-kentässä käytetään title eikä container-title-short. Helpompi: hae valmiiksi “IEEE (with Full Journal Names)” tai vastaava tyylirepositoriosta.

”Et al.”-sääntö:

Samassa Preferences → Cite → Styles -ikkunassa klikkaa “et-al min” ja “use et-al” arvoja (asetta vaikka 11), jotta kaikki <10 kirjoittajaa listataan.

Jos tyylissä ei ole tätä asetusta, muokkaa CSL-koodi: etsi <et-al min="..."> ja säädä et-al="false" tai sopiva min="11".

Organisaatiot kirjoittajiksi:

Tarkista, että Zoterossa item-tyyppi on Report tai Web Page ja Author-kenttään on syötetty organisaation nimi (“Traficom”, “Aluehallintovirasto” ...).

Älä jätä Author-kenttää tyhjäksi; jos henkilöä ei ole, organisaatio riittää.

Kun päivität nämä kentät Zoterossa ja käytät tyyliä, jossa et-al raja on ≥ 11 ja journal-abbr on pois päältä, Wordin lisäosa tuottaa automaattisesti oikeanlaisen viiteluettelon. Tarvittaessa voit duplikoida/editoida CSL-tiedoston, jos valmista tyyliä ei löydy.

Sinä sanoit:

Saisinko nämä ohjeet vielä suomenkieliselle Zoterolle

ChatGPT sanoi:

Totta kai! Tässä ovat ohjeet Zoteroon suomenkielisellä käyttöliittymällä, jotta saat lähdeluettelot kuntoon ohjeidesi mukaisesti (esim. kaikki kirjoittajat näkyviin, lehden nimet kokonaisina, organisaatiot mukaan).

 Zoteron asetukset suomeksi

1. Kaikki kirjoittajat näkyviin (ei "ym.")

Näin saat kaikki kirjoittajat esiin (jos heitä on enintään 10):

Avaa Zotero.

Mene ylävalikosta: Muokkaa → Asetukset.

Siirry välilehteen Viitteet (Cite).

Klikkaa oikeasta reunasta painiketta Tyylieditori (Style Editor), jos käytössä on oma tyyli – tai:

Klikkaa Hae lisää tyyliä...

Hae tyyli, jossa kaikki kirjoittajat listataan (esim. “APA 7th edition (no et al.)” tai muokattava pohja)

Jos muokkaat omaa tyyliä:

Etsi kohta <et-al ...> ja muuta esim. näin:

```
<et-al min="11" use-first="10"/>
```

Tämä näyttää kaikki kirjoittajat, jos heitä on 10 tai vähemmän.

2. Lehtien nimet kokonaisina (ei lyhenteitä)

Näin otat käyttöön täydet lehtien nimet:

Avaa jälleen Muokkaa → Asetukset → Viitteet (Cite).

Klikkaa Tyylieditori, ja valitse käyttämäsi tyyli (esim. IEEE, Vancouver...).

Etsi tyylistä rivi, jossa lukee:

```
<text variable="container-title" form="short"/>
```

→ Vaihda form="short" → form="long" tai poista kokonaan form-osa, jolloin käytetään oletuksena koko nimeä.

Esimerkiksi:

```
<text variable="container-title"/>
```

Vinkki: Hae valmiina esim. tyyli: “IEEE (with full journal names)” → se käyttää jo pitkiä nimiä.

Organisaation lisääminen kirjoittajaksi

Jos lähteessä ei ole yksittäistä henkilöä vaan organisaatio (kuten “Traficom”):

Lisää lähde Zoterossa normaalisti (esim. verkkosivuna).

Kirjoita Kirjoittaja (Author) -kenttään organisaation nimi:

Klikkaa nuolen kuvaketta kirjoittajakentän vieressä.

Valitse Organisaatio (engl. "Corporate Author") → näin esimerkiksi Traficom näkyy oikein viitteessä.

Älä jätä kirjoittajakenttää tyhjäksi – tämä johtaa usein puutteellisiin viitteisiin.

Esimerkki käytännössä

Esim. lähteestä:

”Tietosuojavastaavat”, Tietosuojavaltuutetun toimisto.

Lisää Zoterossa:

Tyyppi: Verkkosivu (Web Page)

Kirjoittaja: Tietosuojavaltuutetun toimisto (valitse organisaatio!)

Otsikko: Tietosuojavastaavat

Julkaisuvuosi: 2025

Viitattu: 22.5.2025

URL: <https://tietosuoja.fi/tietosuojavastaavat>

 Bonus: Vie koko tyylimuutos myös Wordiin

Kun muokkaat tyyliä (tai lataat uuden .csl-tiedoston):

Tallenna tiedosto omalle koneellesi (automaattisesti esim. Omat tyylit -kansioon).

Avaa Zotero → Asetukset → Viitteet → Tyylit.

Klikkaa + ja valitse oma .csl-tiedosto → se näkyy nyt Wordin Zotero-lisäosassa käytettävänä.

Jos haluat, voin myös tehdä sinulle valmiiksi muokatun .csl-tyylitiedoston (esim. IEEE- tai APA-pohjalta), jossa:

Näkyvät kaikki kirjoittajat

Käytetään täydellisiä lehtien nimiä

Voit valita tyyliäsi lähellä olevan rungon

Haluatko tällaisen valmiina?