LAPIN AMK
Lapland University of Applied Sciences

PESTEL-ANALYYSITYÖKALUN LUOMINEN ORGANISAATION KYBERTURVALLISUUDEN TUEKSI

Jertta Vildhjärta

Opinnäytetyö

Tiedolla johtamisen asiantuntija
Tradenomi YAMK

2023

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tiedolla johtamisen asiantuntija
Tradenomi YAMK

Tekijä	Jertta Björkman	**Vuosi**	2023
Ohjaaja	Milla Immonen		
Toimeksiantaja	Oy Apotti Ab		
Työn nimi	PESTEL-analyysityökalun luominen organisaation kyberturvallisuuden tueksi		
Sivumäärä	93		

Opinnäytetyön aiheena oli PESTEL-analyysityökalun luominen Oy Apotti Ab:n kyberturvallisuuden tueksi. PESTEL-analyysin avulla voidaan arvioida organisaation toimintaympäristöä ja siihen vaikuttavia muutosvoimia poliittisesta, ekonomisesta, sosiaalisesta, teknologisesta, ekologisesta ja lainsäädännöllisestä näkökulmasta. Opinnäytetyön toimeksiantaja Oy Apotti Ab tuottaa Uudellamaalla toimiville sosiaali- ja terveydenhuollon organisaatioille toiminnanohjausjärjestelmää. Tutkimuksessa keskityttiin Oy Apotti Ab:n kyberturvallisuuden kehittämiseen hallinnollisesta näkökulmasta.

Tutkimuksen tarkoituksena oli muodostaa PESTEL-analyysiin analyysikysymykset, joiden perusteella Oy Apotti Ab:n tulisi vuosittain tarkastella toimintaympäristönsä muutosvoimia. Tutkimuksessa haettiin vastausta kysymyksiin: Mitä kyberturvallisuuden toimintaympäristön muutosvoimia kohdistuu Oy Apotti Ab:hen? Millaiset PESTEL-analyysin kysymykset ohjaavat löytämään Oy Apotti Ab:n kyberturvallisuuteen vaikuttavat muutosvoimat?

Tutkimuksen lähestymistapana oli kvalitatiivinen eli laadullinen tutkimus. Tutkimuksessa hyödynnettiin tietoperustaan koottua kansainväliseen tutkimukseen pohjautuvaa tietoutta sekä teemahaastattelujen avulla kerättyä aineistoa. Tietoperustaan kerättiin tietoa kansainvälisistä ja kansallisista kyberturvallisuuden trendeistä ja kansallisista tietoturvan ja kyberturvallisuuden ohjeistuksista. Teemahaastattelut, seitsemän kappaletta, toteutettiin verkkohaastatteluina marraskuussa 2022, eli juuri ennen hyvinvointialuemuutoksen voimaan astumista. Haastateltavat työskentelevät tietoturvan ja kyberturvallisuuden asiantuntijoina Oy Apotti Ab:ssa.

Tutkimuksessa saatiin kerättyä laaja-alainen käsitys niistä muutosvoimista, jotka vaikuttavat Oy Apotti Ab:n kyberturvallisuuden toimintaympäristöön. Tietoperustaan ja kansallisiin oheistuksiin tukeutuen sekä haastatteluissa saatujen vastausten perusteella saatiin kerättyä tarvittava määrä taustatietoa. Kerättyjen tietojen pohjalta luotiin PESTEL-analyysityökalun kysymykset Oy Apotti Ab:n kyberturvallisuuden tueksi.

Avainsanat kyberturvallisuus, tietoturva, PESTEL-analyysi, tietojohtaminen, tiedolla johtaminen

Thesis Abstract

LAPIN AMK
Lapland University of Applied Sciences

Knowledge Management Expertise
Master of Business Administration

Author	Jertta Björkman	**Year**	2023
Supervisor	Milla Immonen		
Commissioned by	Oy Apotti Ab		
Title	PESTEL analysis tool to improve organization's cybersecurity		
Number of pages	93		

The purpose of this thesis was to create a PESTEL analysis tool for Oy Apotti Ab's cybersecurity management. PESTEL analysis is a framework that illustrates an organization's working state and the external factors that affect it from the political, economic, social, technological, environmental, and legal point of view. The thesis was commissioned by Oy Apotti Ab. Oy Apotti Ab develops an electronic client and patient record and an ERP system for social and health care organizations in Uusimaa region. The research focused on developing Oy Apotti Ab's cybersecurity management from the administrative point of view.

The purpose of the research was to create the questions for PESTEL analysis tool that would help Oy Apotti Ab to identify the external factors that affect the organization's cybersecurity. The research questions are: What external factors are affecting Oy Apotti Ab's cybersecurity? Which PESTEL analysis questions direct to find the external factors that affect Oy Apotti Ab's cybersecurity?

The method of the research was qualitative. The background information for the research was collected with a literature review and thematic interviews. The information was collected from international research, domestic cybersecurity guidelines and thematic interviews. Seven selected cybersecurity professionals from Oy Apotti Ab were interviewed in November 2022.

The results of the research provide widespread information about those external factors that affect Oy Apotti Ab's cybersecurity. Therefore, the results of the thesis research provide good quality information of the research subject. Based on the research results a PESTEL analysis tool was created for Oy Apotti Ab's cybersecurity management.

Keywords cybersecurity, information security, PESTEL analysis, information knowledge, knowledge management

SISÄLLYS

1 JOHDANTO 6

2 SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMÄT 8

2.1 Tietojärjestelmiin liittyvät lait ja määräykset 8
2.2 Tietojärjestelmien erityispiirteet 10
2.3 Tietojärjestelmät osana kriittistä infrastruktuuria 11
2.4 Digitalisaation vaikutus 12

3 TIETOTURVA JA KYBERTURVALLISUUS KÄSITTEINÄ 15

3.1 Tietoturva 15
3.2 Kyberturvallisuus 16
3.3 Kyberturvallisuuden nykytila Suomessa 18

4 SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN KYBERUHKAT 21

4.1 Suomeen kohdistuvat kyberuhkat 21
4.2 Sosiaali- ja terveydenhuollon kyberuhkat 22
4.3 Kybervaikuttamisen keinot 24
4.3.1 Tietojenkalastelu 25
4.3.2 Palvelunestohyökkäykset 26
4.3.3 Haittaohjelmat 27
4.3.4 Kiristyshaittaohjelmat 28

5 KYBERTURVALLISUUDEN HALLINTA JA KEHITTÄMINEN 30

5.1 Kyberturvallisuuden hallinta 30
5.2 Varautuminen 32
5.3 Yhteistyö ja tiedon jakamisen tärkeys 33
5.4 VAHTI 34
5.5 ISO 27001 36
5.6 Kybermittari 37
5.7 PESTEL-analyysi 38
5.7.1 Poliittinen analyysi 39
5.7.2 Ekonominen analyysi 40
5.7.3 Sosiaalinen analyysi 41

5.7.4 Teknologinen analyysi 42
5.7.5 Ekologinen analyysi 43
5.7.6 Lainsäädännöllinen analyysi 44
6 TUTKIMUKSEN TAUSTA 45
6.1 Toimeksiantaja 45
6.2 Tutkimuksen tausta ja nykytilanne 46
6.3 Tutkimuksen tarkoitus, tavoitteet ja tutkimuskysymykset 47
7 TUTKIMUSMENETELMÄ JA TOTEUTUS 49
7.1 Laadullinen tutkimusmenetelmä 49
7.2 Menetelmällinen toteutus 49
7.3 Tutkimuksen toteutus 50
7.4 Eettiset lähtökohdat 51
8 TUTKIMUSTULOKSET 53
8.1 Poliittiset muutostekijät 53
8.2 Ekonomiset muutostekijät 58
8.3 Sosiaaliset muutostekijät 62
8.4 Teknologiset muutostekijät 66
8.5 Ekologiset muutostekijät 72
8.6 Lainsäädännölliset muutostekijät 75
8.7 PESTEL-analyysityökalu Oy Apotti Ab:n kyberturvallisuuden tueksi 77
9 JOHTOPÄÄTÖKSET JA POHDINTA 80
9.1 Tulosten tarkastelu 80
9.2 Luotettavuuden tarkastelu 82
9.3 Jatkokehittämisaiheet 82
LÄHTEET 84

1 JOHDANTO

Covid-19-pandemia ja geopoliittiset muutokset Euroopan turvallisuustilanteessa ovat nostaneet korostetusti esille kyberturvallisuuden tärkeyden. Kansainvälisen politiikan ja valtasuhteiden muuttuminen on lisännyt kybervaikuttamista myös Suomessa (Pelttari 2022; Traficom 2022). Tällaisella vaikuttamisella tarkoitetaan kaikkea digitaaliseen ja verkottuneeseen ympäristöön tehtäviä vaikutusyrityksiä (Kyberturvallisuuden sanasto 2018, 21–24). Erityisesti kriittiseen infrastruktuuriin vaikuttaminen on yleistynyt.

Sosiaali- ja terveydenhuollon tietojärjestelmiin on viime vuosina tehty enenevissä määrin erilaisia kyberhyökkäyksiä, sillä rikollisuuden näkökulmasta niiden sisältämä tieto on perinteisiä luottokorttitietoja arvokkaampaa ja laadukkaampaa. Lisäksi asiakas- ja potilastietojärjestelmien sisältämä tieto on organisaatioille elintärkeää, ja sen vuoksi organisaatiot nähdään hyvinä kiristyskohteina. Haastetta lisää myös se, että kyberturvallisuuteen ei olla sosiaali- ja terveydenhuollon organisaatioissa panostettu riittävästi, vaan näihin organisaatioihin kyberhyökkäyksen tekeminen on helpompaa kuin esimerkiksi rahoitusalalla. (Lehto, Pöyhönen & Lehto 2019, 11–12; Kotipelto 2022.)

Kyberturvallisuuden ei tule olla vain organisaation toimialan tekninen tukitoimi, vaan siihen tulee panostaa laajamittaisesti. Kyberstrategiaa tulee kehittää pitkäjänteisesti organisaation liiketoiminnan tueksi. Organisaatioiden kyberturvallisuuden hallintaa ja kehitystä voidaan toteuttaa monella tapaa, esimerkiksi noudattamalla kansainvälisesti tunnistettuja standardeja. Yksi yleisimmin käytetty tietoturvastandardi on ISO 27001, jonka avulla organisaatio voi osoittaa tietoturvan hallinnanjärjestelmän laadun. Standardien mukainen toiminta yhtenäistää toimintamalleja, jolloin uusien työntekijöiden perehdyttäminen organisaatioon ja yhteistyö muiden organisaatioiden kanssa helpottuu ja tehostuu. (Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot 2020, 11–12; Mutanen, Tolonen & Vepsäläinen 2021, 7–8.)

Opinnäytetyössä keskityttiin kehittämään kyberturvallisuutta Oy Apotti Ab:ssa. Oy Apotti Ab tuottaa maailman ensimmäistä sosiaali- ja terveydenhuollon

yhdistävää tieto- ja toiminnanohjausjärjestelmää Uudenmaan alueella sosiaali- ja terveydenhuollon organisaatioille. Yritys on perustettu vuonna 2015 ja sen tarkoituksena on kehittää yhdenvertaisia sosiaali- ja terveydenhuollon palveluja asiakasorganisaatioiden ja kansalaisten käyttöön. Apotti-tietojärjestelmää käyttää noin 47 000 ammattihenkilöä ja järjestelmään on yhdistetty 139 integraatiota. Oy Apotti Ab:ssa työskentelee noin 540 työntekijää hallinnollisissa tehtävissä, tukipalveluissa ja järjestelmänkehityksessä. (Oy Apotti Ab 2022b; Oy Apotti Ab 2022e.)

Opinnäytetyön menetelmänä käytettiin kirjallisuuskatsausta ja kvalitatiivista tutkimusotetta. Kirjallisuuskatsauksessa tutkittiin kyberturvallisuuteen liittyviä trendejä ja suuntauksia sekä tutustuttiin kansallisen tason ohjeistuksiin. Kvalitatiivinen osuus toteutettiin teemahaastatteluina, joissa seitsemää Oy Apotti Ab:n tietoturvan ja kyberturvallisuuden parissa työskentelevää henkilöä haastateltiin PESTEL-rungon mukaisesti. PESTEL-analyysi on strategiatyökalu, jolla arvioidaan organisaation toimintaympäristöä ja siihen vaikuttavia muutosvoimia poliittisesta, ekonomisesta, sosiaalisesta, teknologisesta, ekologisesta ja lainsäädännöllisestä näkökulmasta (Vuorinen 2014, 220–222). PESTEL-analyysi valittiin Oy Apotti Ab:n toiveesta, sillä sen koettiin tuovan tarvittavaa tietoutta kyberturvallisuuden toimintaympäristöstä organisaation käyttöön laadukkaasti ja tehokkaasti.

Opinnäytetyössä keskityttiin Oy Apotti Ab:n kyberturvallisuuden toimintaympäristön tarkasteluun ja parantamiseen organisaation hallinnollisesta näkökulmasta, ei teknisen tai organisaation kehittämän tietojärjestelmän näkökulmasta. Kehittämistehtävä oli osa Oy Apotti Ab:n kyberturvallisuuden kehitysprojektia ja ISO 27001 -standardin vaatimusten täyttämistä. Opinnäytetyön lopputuotoksena tuotettiin PESTEL-analyysityökalu Oy Apotti Ab:n kyberturvallisuuden tueksi. Rakennettua PESTEL-analyysipohjaa on tarkoitus käyttää organisaation eri yksiköissä vähintään kerran vuodessa. Analyysissa saadun tiedon avulla on tarkoitus tunnistaa organisaation toimintaympäristössä tapahtuvia kyberturvallisuuteen vaikuttavia muutoksia ja sitä kautta saavuttaa entistä laadukkaampaa tietoon perustuvaa kyberturvallisuuden johtamista ja kehittämistä.

2 SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMÄT

2.1 Tietojärjestelmiin liittyvät lait ja määräykset

Sähköiset asiakas- ja potilastietojärjestelmät ovat oleellinen osa sosiaali- ja terveydenhuollon ammattilaisten päivittäistä työtä. Tietojärjestelmien avulla dokumentoidaan, tallennetaan ja ylläpidetään asiakas- ja potilasasiakirjoja. Tietojärjestelmien sisältämä tieto on arkaluontoista ja sen käyttöä ohjataan tiukalla lainsäädännöllä. Sosiaali- ja terveysministeriö vastaa eduskunnan säätämän lainsäädännön valmistelusta ja toimeenpanosta määrittelemällä asetukset, päätökset ja lainsäädännön tulkinnan. Terveyden ja hyvinvoinnin laitos, myöhemmin THL, tuottaa soveltavia ja tarkentavia ohjeistuksia sosiaali- ja terveysministeriön ohjeistuksen perusteella. THL myös ylläpitää ja muokkaa ohjeistuksia lakimuutosten osalta. (Sosiaali- ja terveysministeriö 2012, 11–14.) Sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira edistää ja valvoo tietojärjestelmiin liittyvien olennaisten vaatimusten toteuttamista (Valvira 2022a).

Tietojärjestelmän tulee täyttää sille asetetut vaatimukset ja sen tulee löytyä Valviran tietojärjestelmärekisteristä ennen kuin se voidaan ottaa käyttöön. Tietojärjestelmät luokitellaan luokkiin A1, A2, A3 ja B sen perusteella, millaista dataa järjestelmissä on ja miten sitä käytetään. Luokittelu määrittää ne vaatimukset, mitä järjestelmän tulee täyttää. Sosiaalihuollon asiakastietojärjestelmät ja terveydenhuollon potilastietojärjestelmät kuuluvat luokkaan A, sillä ne liittyvät suoraan tai välillisesti Kanta-palveluihin ja niissä käsitellään laajamittaisesti asiakas- ja potilastietoa. (Valvira 2022a.) Sosiaali- ja terveydenhuollon tietojärjestelmiä on Valviran (2022c) tietojärjestelmärekisterissä luokassa A yli kahdeksankymmentä ja luokassa B noin kolmesataakolmekymmentä kappaletta.

Valvira velvoittaa sekä tietojärjestelmätoimittajan että palveluntarjoajan ilmoittamaan mahdollisista poikkeamista tietoturvassa tai tietosuojassa (Valvira 2022b). Asiakas- ja potilastietojen tulee olla näkyvillä vain siltä osalta kuin mitä ammattihenkilön työtehtävän hoitaminen edellyttää. Asiakkaat ja potilaat voivat itse määritellä, antavatko he suostumuksen tiedoilleen näkyä rekisterirajan yli, esimerkiksi perusterveydenhuollon ja erikoissairaanhoidon rekisterien välillä. Jokaisella

ammattihenkilöllä on myös velvollisuus tehdä tietojärjestelmään vaadittavat kirjaukset ja merkinnät. Ammattihenkilöiden toimista jää jälki lokitietoihin, jotta tarvittaessa jälkikäteen voidaan tarkastella, kuka on tietoja käynyt katsomassa ja onko sille ollut perustetta. (Sosiaali- ja terveysministeriö 2019, 14–15, 17.)

Tietojärjestelmien tulee täyttää käyttötarkoituksensa mukaiset ajantasaiset vaatimukset. Säädettävät lait ja lakimuutokset vaikuttavat sekä palveluntuottajiin että tietojärjestelmätoimittajiin. Esimerkiksi marraskuussa 2021 voimaan tullut asiakastietolaki (Laki Sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 784/2021) toi uudistuksia, joiden tarkoituksena on tukea sosiaali- ja terveydenhuollon palvelujen muutosta kohti parempaa asiakas- ja potilasturvallisuutta sekä parantaa hoitoa ja palveluja. Uudistettu laki mahdollistaa aiempaa paremmin asiakas- ja potilastietojen liikkumisen eri palveluntarjoajien välillä, jos henkilö on tähän luvan antanut. Uudistetut Kanta-informointiin ja luovutuslupaan liittyvät muutokset astuivat voimaan siirtymäajan päättyessä 1.1.2023.

Uudistettu asiakastietolaki (Laki Sosiaali- ja terveydenhuollon asiakastietojen käsittelystä 784/2021) velvoitti tietojärjestelmätoimittajia ja palveluntarjoajia dokumentoimaan tietoturvasuunnitelman, joka oli vaatimuksiltaan laajempi kuin aikaisemmin vaadittu omavalvontasuunnitelma (Valvira 2015). Lain vaatimuksiin perustuen THL on julkaissut määräyksen tietoturvasuunnitelmaan sisällytettävistä vaatimuksista (THL 2021a) ja määräyksen sosiaali- ja terveydenhuollon tietojärjestelmien olennaisista toiminnallisista vaatimuksista ja tietoturvavaatimuksista (THL 2021b). Määräyksissä ohjeistetaan sekä järjestelmätoimittajaa että palveluntarjoajaa toteuttamaan tietojärjestelmän rakentaminen ja käyttö tietoturvallisesti koulutetun henkilökunnan avulla ja kiinnittämään huomio siihen, miten tietojärjestelmän käytön jatkuvuus ja ylläpito on turvattu. Määräysten tarkoitus on kehittää tietojärjestelmien ja organisaatioiden tieto- ja kyberturvallisuutta.

Lait uudistuvat nopeasti kehittyvän digitalisaation ja muiden esiin nousseiden muutostarpeiden vuoksi. Asiakastietolaista on jo suunnitteilla uusi versio (HE 246/2022), jonka tavoitteena on koota yhteen säädökset, jotka koskevat tietosuojaa, salassapitoa, tiedonsaantioikeuksia ja asiakastietojen luovutusta sekä asiakirjojen käsittelyä. Lisäksi laissa säädetään tarkennetusti valtakunnallisia

tietojärjestelmiä ja tiedonhallinnan ohjausta koskevia määräyksiä. Uudistuneen lain on tarkoitus vastata perustuslain ja Euroopan yleisen tietosuoja-asetuksen vaatimuksiin. Tavoitteena on, että nykyisen pirstaloituneen ja osin vanhentuneen asiakastietolain korvaisi jatkossa laki, joka muodostaa selkeän, yhtenäisen ja kattavan kokonaisuuden, jolloin sosiaali- ja terveyspalvelut muodostaisivat asiakkaalle turvallisen ja toimivan kokonaisuuden. Lakia valmistellaan sosiaali- ja terveysministeriössä ja sen on tarkoitus astua voimaan vuoden 2024 alussa. (Valtioneuvosto 2022a.)

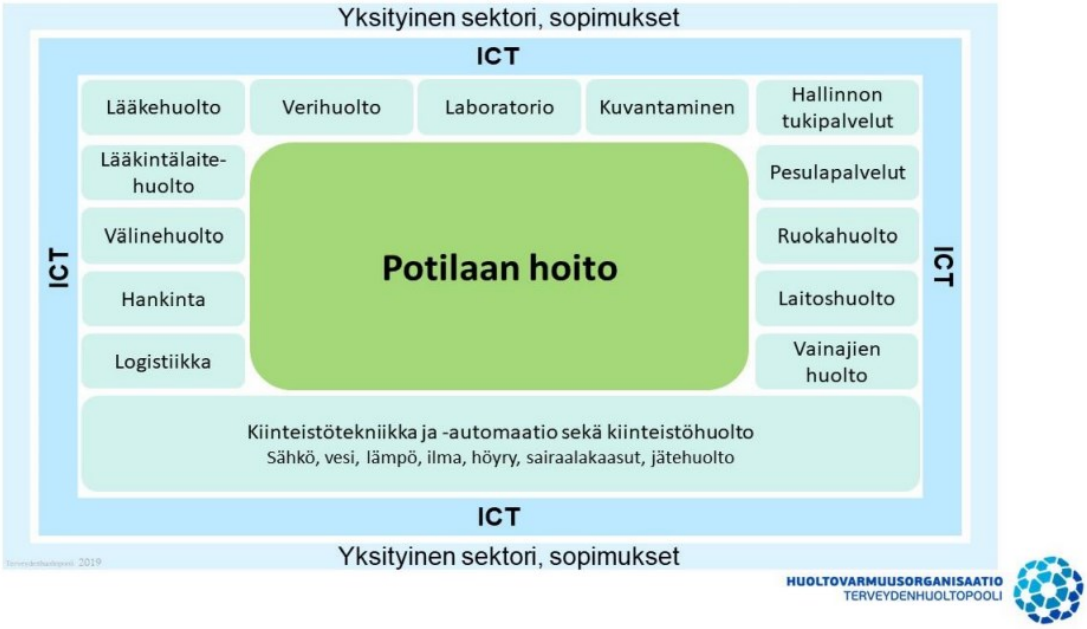
Lähitulevaisuuden suurena lainmääräämänä muutoksena tulee Kanta-palvelun laajeneminen sosiaalihuollon puolelle. Jokaisen julkisen ja yksityisen palvelunjärjestäjän on liityttävä Kantaan, jos he käsittelevät asiakastietoja tietojärjestelmien kautta. Tämä tuottaa runsaasti työtä ja investointitarvetta sekä palveluntarjoajille että järjestelmätoimittajille. Sosiaalihuollon asiakaskirjojen tallentamisen velvollisuus etenee palvelutehtävittäin siten, että vuonna 2026 kaikkien sosiaalihuollon palvelutehtävien on täytynyt liittyä Kanta-verkostoon. (Kanta 2022a; Kanta 2022b.) Asiakas- ja potilastietojärjestelmiin, niiden toimittajiin ja palveluntarjoajiin vaikuttavat myös monet muut lait ja määräykset, kuten esimerkiksi laki potilaan asemasta ja oikeuksista (785/1992), Lääkelaki (395/1987) ja Terveyden ja hyvinvoinnin laitoksen määräykset (THL 2022).

2.2 Tietojärjestelmien erityispiirteet

Sosiaali- ja terveydenhuollon organisaatiot ovat monimuotoisia ja kompleksisia kokonaisuuksia. Asiakkaiden ja potilaiden hoitaminen vaatii monialaisten ammattihenkilöryhmien tiivistä yhteistyötä, jossa kaikki tekevät osaltaan aikakriittistä ja tietosensitiivistä työtä käyttäen hyväkseen ja tiedon tallentamiseen erityisiä tietojärjestelmiä. Tietojärjestelmäarkkitehtuuri koostuu paikallisista ja alueellisista järjestelmistä, joiden avulla päivittäistä työtä toteutetaan sekä kansallisista järjestelmistä, joissa tieto varastoidaan ja joista tietoa jaetaan. (Sosiaali- ja terveysministeriö 2019, 14–18.)

Sosiaalihuollossa tietojärjestelmällä tulee kyetä tehdä viranomaispäätöksiä, maksusuorituksia ja maksusitoumuksia. Lisäksi asiakkaiden ja potilaiden hoitamiseen

ja henkilökunnan turvaamiseen tarvitaan valvonta- ja päällekarkausjärjestelmiä. Sairaaloissa potilaan hoitoon tarvitaan lukuisia integraatioita potilaan operationaaliseen hoitoon. Näitä integraatioita ovat muun muassa välinehuolto, lääkehuolto, veripalvelut ja kuvantamispalvelut. Kuviossa 1 havainnollistetaan tarvittavien toimintojen kokonaisuutta sairaalaympäristössä. (Sosiaali- ja terveysministeriö 2019, 14–18.) Asiakkaan ja potilaan hoitamiseen eivät siis riitä pelkästään yksittäiset asiakas- ja potilastietojärjestelmät, vaan tarvitaan enemminkin verkostoitunut järjestelmien kokonaisuus. Tämä vaadittavien järjestelmien monimuotoisuus lisää haasteita kyberturvallisuuden toimintaympäristössä sekä järjestelmien toimittajien että palveluntarjoajien näkökulmasta.



Kuvio 1. Terveydenhuollon toimintaympäristö (Huoltovarmuuskeskus 2021, 11)

2.3 Tietojärjestelmät osana kriittistä infrastruktuuria

Sosiaali- ja terveydenhuollon tietojärjestelmien toiminnan turvaaminen on osa yhteiskunnan huoltovarmuuden varmistamista myös poikkeusoloissa. Häiriötilanteissa korostuu kriisipalveluiden tarve, jolloin sekä sosiaali- että terveydenhuollon asiakkuuksia syntyy enemmän. Julkisen hallinnon tietoturvakriteeristössä (Julkri), joka perustuu lakiin julkisen hallinnon tiedonhallinnasta (906/2019), määritellään asiakas- ja potilastietojärjestelmien saatavuuden taso tärkeäksi, mikä tarkoittaa sitä, että tiedon saatavuuden osalta voidaan hyväksyä enintään tuntien mittaisia häiriöitä (Julkisen hallinnon tietoturvallisuuden arviointikriteeristä (Julkri):

Suositus ja kriteeristö 2022, 20). Tietojärjestelmien tulee olla turvattuina häiriö- ja riskiarvioinnin perusteella suunnitellun varautumisjärjestelyn ja jatkuvuussuunnitelman mukaisesti. Asiakas- ja potilastiedon tulee olla saatavilla käytettäväksi missä tahansa olosuhteissa ja tämän vuoksi tietojärjestelmien sisältämää tietoa ei saa säilyttää ulkomailla. (Turvallisuuskomitea 2017, 22, 69.)

Mutanen, Tolonen & Vepsäläinen (2021, 24) toteavat, että kompleksisten toimintaympäristöjen ymmärtäminen ja varsinkin kriittisten palveluiden tunnistaminen ovat avainasemassa sosiaali- ja terveydenhuollon palveluiden jatkuvuuden hallinnalle ja kehitykselle. Organisaatioiden tulee tunnistaa kriittiset palvelut, niiden tuottajat ja mahdolliset alituottajat. Palveluntuottajana tai järjestelmätoimittajina voivat toimia myös kolmannet osapuolet tai ainakin kriittiset toiminnat voivat olla riippuvaisia kolmansista osapuolista. Tämän vuoksi on tärkeää, että toimittajahallinta on ymmärretty keskeiseksi osaksi kriittisten toimintojen luokittelun kokonaisuutta. Kriittisen järjestelmän, laitteen tai toiminnon tunnistamiseksi täytyy selvittää sosiaali- ja terveydenhuollon yksiköiden toimintaprosessit. Tavoite on, että ihminen pystyy saamaan missä ja milloin tahansa oikeaa hoitoa ja apua mahdollisimman vähällä haitalla, eli asiakas- ja potilasturvallisuus tulee olla taattuna. Itse tietoturvallisuudella ei ole nähtävää itseisarvoa kriittisten toimintojen jatkuvuuden suunnittelussa ja toteutuksessa, vaan sen tulee enemminkin tukea sosiaali- ja terveydenhuollon palveluita ja varmistaa työssä tarvittava tietoturvallisuus. (Mutanen, Tolonen & Vepsäläinen 2021, 11–14.)

2.4 Digitalisaation vaikutus

Digitalisaatiolle ei ole yksiselitteistä tai vakiintunutta määritelmää, mutta sen voidaan ajatella olevan erilaisten digitaalisten teknologioiden hyödyntämistä ja käyttöä toimintojen toteuttamisessa, kehittämisessä ja uudistamisessa (Koivisto 2021, 6). Informaatioteknologia on kehittynyt sosiaali- ja terveydenhuollon alalla nopeasti 2000-luvulta lähtien. Tietojärjestelmät ja niihin integroitavat lääkinnälliset laitteet ovat kehittyneet ja kehityksen myötä datan määrä ja käytettävyys ovat kasvaneet. Teknologian kehittymisen myötä tiedon käsittely on nopeutunut ja tietojärjestelmiä ja -verkkoja hyödynnetään entistä monipuolisemmin myös asiakas- ja potilaskontakteissa. Laitteet tallentavat ja ihmiset kirjaavat suuria määriä tietoa

järjestelmiin, joista se on varsinkin rakenteisessa muodossa tallennettuna helposti käytettävissä. Tiedon arvo on tunnistettu organisaatioissa ja tietoa pyritään käyttämään hyödyksi sekä yksilön että kansanterveyden hyväksi. (Koivisto 2021, 6.)

Digitalisaation lisäämä tietojärjestelmien verkostoituminen tekee kyberturvallisuuden hallinnasta haastavampaa. Tutkimuksissa on tunnistettu, että organisaatioiden ja laitevalmistajien panostus kyberturvallisuuteen ei ole välttämättä riittävää. Varsinkin lääkinnällisten laitteiden, kuten sydämentahdistimien ja insuliinipumppujen kyberturvallisuus on herättänyt huolta eri tahoissa (Williams & Woodward 2015, 307; Zhang, Qiu, Tsai, Hassan & Almari 2017, 88–92; Coventry & Branley 2018, 48–49; Weber & Kleine 2020, 147; Kybersää lokakuu 2022). Huoleen on reagoitu ja EU:n tasolla lääkinnällisten laitteiden tietoturvaan on jo asetettu vaatimuksia. Huoltovarmuuskeskuksen Kyber-Terveys-hanke tuotti listan tietoturva- ja tietosuojavaatimuksista sosiaali- ja terveydenhuollon hankinnoissa. (Lehto, Pöyhönen & Lehto 2019, 15.)

Digitalisaation vaikutus sosiaali- ja terveydenhuollon palveluihin voi olla täydellinen tai osittainen. Täydellisellä digitalisaatiolla tarkoitetaan tilannetta, jossa palveluun tai toimintoon ei liity lainkaan vuorovaikutusta ihmisten välillä, vaan palvelu on toteutettu täysin digitaalisesti, kuten chatbottien, digitaalisten oirearvioiden tai sosiaalihuollon hakemusten ja ilmoitusten kautta. Toisaalta digitalisaatio voi olla osittainen, jolloin se toimii apuna asiakkaan tai potilaan ja ammattihenkilön välissä, kuten etävastaanotolla. (Koivisto 2021, 6.) Esimerkiksi Helsingin ja Uudenmaan sairaanhoitopiiri (HUS) on mahdollistanut potilastietojärjestelmänsä kautta toteutettavat etäpäivystyskäynnit yhteispäivystyksissä (HUS 2022).

Digitalisaatio ja sen vauhdikas kehittyminen tulee vaatimaan sekä sosiaali- ja terveydenhuollon ammattilaisilta että kansalaisilta uusien taitojen omaksumista. Hege, Tolks, Kuhn & Shiozawa (2020, 1–2) ja Koivisto ym. (2020, 11) kirjoittavat Covid-19-pandemian laukaisemasta digitalisaation kehityksestä. Sosiaali- ja terveydenhuollon alalle kehitetään jatkuvasti uusia applikaatioita ja tekoälyllä pyritään ratkaisemaan esiin nousseita haasteita. Kehitys koetaan teknologisesti pääsääntöisesti hyväksi, mutta haasteeksi on noussut se, ettei kehitettyjä uusia

digitaalisia palveluita pääse harjoittelemaan. Sama huoli nostettiin esiin Valtioneuvoston (2019) tekemässä selvityksessä. Huomiota kiinnitettiin myös kansalaisten yhdenvertaisuuteen ja niihin haasteisiin, joita digitalisaatio aiheuttaa. Digitalisaatio ei saa syrjäyttää ketään ja palvelut tulevat olla tasavertaisesti kaikkien saavutettavissa sekä teknisesti että kognitiivisesti. (Valtioneuvosto 2019.)

3 TIETOTURVA JA KYBERTURVALLISUUS KÄSITTEINÄ

3.1 Tietoturva

Tietotekniikan ja tietoaineistojen tulee olla turvallisia, toimintakykyisiä ja käytettäviä olosuhteista riippumatta. Tietoturvalla pyritään erilaisin hallinnollisin ja teknisin toiminnoin varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus. (Kyberturvallisuuskeskus 2022f.) Luottamuksellisuudella tarkoitetaan sitä, että tiedot on rajattu saataviksi vain niiden käyttöön oikeutetuille ihmisille eikä niihin ole ulkopuolisille pääsyä. Tiedon eheydellä varmistetaan, että tieto on yhdenpitävää alkuperäisen tiedon kanssa ja sitä voi muokata vain ne henkilöt, joilla siihen on oikeus ja tarve. Tiedon tulee olla käytettävää, eli tiedon tulee olla saatavissa ja hyödynnettävissä haluttuna aikana. Tietoturvallisuuden voidaan katsoa olevan osa organisaatioiden johtamistoimintaa, jonka tavoitteet ja kehittäminen tulee sisällyttää liiketoimintamalliin. (VAHTI 2/2011, 13; Kyberturvallisuuden sanasto 2018, 15; Kyberturvallisuuskeskus 2022f.)

Tietoturva voidaan jakaa eri osa-alueisiin:

- hallinnollinen tietoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus
- käyttöturvallisuus (VAHTI 7/2003, 29).

Hallinnollisen tietoturvallisuuden perustana on organisaation tietoturvapolitiikka, joka määrittelee tietoturvallisuuden periaatteet ja toimintatavat. Hallinnollinen tietoturva ei ole vain organisaation sisäistä toimintaa, vaan siihen kuuluu oleellisena osana suhteiden ylläpitäminen asiakkaisiin ja muihin sidosryhmiin. Organisaation tekemät laite- tai palveluvalinnat ovat osa hallinnollista tietoturvallisuutta.

Henkilöstöturvallisuus sisältää henkilöstöön liittyvien riskien hallinnan, joita ovat esimerkiksi henkilön soveltuvuus tehtävään, henkilöstön tietoturvataitojen ylläpitäminen ja toimintatapojen valvominen. Yhtenä suurena henkilöstöturvallisuushaasteena ja mahdollisena tietoturvauhkana ovat avainhenkilöriippuvuudet, joiden syntymisen välttämiseen organisaatioiden tulisi panostaa. Fyysisellä turvallisuudella tarkoitetaan organisaation fyysisten toimitilojen suojaamista sekä tuhoutumiselta että tilaan kuulumattomilta henkilöiltä. Tietoturvaa voidaan toteuttaa huolehtimalla asiakirjojen turvallisella säilytyksellä ja kulunvalvonnalla tiloihin, joissa tietoa käsitellään. (VAHTI 07/2003, 29–35; Kyberturvallisuuden sanasto 2018, 15–20.)

Tietoliikenneturvallisuus pitää sisällään mm. tietoliikennelaitteiston kokoonpanon, verkonhallinnan, käytönvalvonnan ja tietoliikenteen testaamisen ja hyväksymisen. Teknisesti tietoturvaa luodaan ja kehitetään tietojen salauksella, varmuuskopioinnilla sekä palomuurin, virustorjuntaohjelmien ja varmenteiden käytöllä. Laitteistoturvallisuudella pidetään yllä käytettävyyttä, toimintaa ja laadunvarmistusta. Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmien, sovellus- ja tietoliikenneohjelmistojen turvaamista sekä pääsynvalvontaa ja lokimenettelyjä. Oleellinen osa digitaalista tietoturvaa on pääsynhallinta, jolla varmistetaan, että käyttäjät, laitteet ja sovellukset pääsevät käyttämään tietojärjestelmien sisältämää tietoa rooliensa mukaisesti. Valtuutettujen henkilöiden tulee myös tietoturvan määritelmän mukaisesti kyetä todentamaan käyttöoikeus tietojen käyttöön. Käyttöturvallisuus kattaa käyttöympäristöön, tietojenkäsittelyyn ja varsinkin sen jatkuvuuteen liittyvät turvallisuustoimenpiteet. Tietoturvallisuudella tarkoitetaan sitä, että tietoturvariskit ovat tiedostettu ja hallinnassa. (VAHTI 07/2003, 35–39; Kyberturvallisuuden sanasto 2018, 15–20.)

3.2 Kyberturvallisuus

Kyberturvallisuus on sisällöltään vakiintumaton termi, mutta sillä tarkoitetaan digitaalisen ja verkottuneen toimintaympäristön turvallisuutta. Kyberturvallisuuden tärkeimpänä tavoitteena on tietoturvan toteutuminen. Kyberturvallisuus tulee kuitenkin nähdä tietoturvaa laajempana kokonaisuutena. Kyberturvallisuuden käsitteessä ei tarkastella vain tietoteknisiä järjestelmiä ja niiden hallintaa, vaan

tarkoituksena on huomioida erilaisten järjestelmien luomia verkostoja ja niissä esiintyviä häiriöitä ja vaikutuksia. Kyberturvallisuutta toteutetaan toimenpiteillä, joiden tarkoituksena on ennakoida, sietää ja ratkaista haitallisia kyberympäristöön liittyviä tapahtumia tai kehityskulkuja sekä kyberuhkia ja niiden mahdollisia vaikutuksia. Kyberturvallisuuden osina voidaan pitää jatkuvuuden hallintaa ja kriisivarautumista. (Suomen kyberturvallisuusstrategia 2013, 13; Kyberturvallisuuden sanasto 2018, 21–24; Kinnunen, Seppo & Rousku 2021, 27–28.)

Kyberturvallisuuden oleellisena osana on kyberympäristön kokonaiskuvan hahmottaminen, jossa pyritään havaintojen, arviointien, mittarien ja analyysien avulla saavuttamaan ymmärrys kybertoimintaympäristöstä ja siihen vaikuttavista tekijöistä. Tavoitteena on saavuttaa tilanne, jossa kybertoimintaympäristöstä ei aiheudu haittaa tai vaaraa informaation käsittelystä riippuvaisille toiminnoille tai toimivuudelle. Kybertoimintaympäristön luottamus perustuu siihen, että eri toimijat toteuttavat tarkoituksenmukaisia ja riittäviä tietoturvallisuusmenetelmiä. (Suomen kyberturvallisuusstrategia 2013, 13; Kyberturvallisuuden sanasto 2018, 21–24; Kinnunen, Seppo & Rousku 2021, 27–28.) Kyberturvallisuutta tulee toteuttaa taktisella, operatiivisella ja strategisella tasolla. Tarkoituksena on saavuttaa tila, jossa kybertoimintaympäristöön voi luottaa ja sen toiminta on turvattu. (Kyberturvallisuuden sanasto 2018, 21–24.)

Kyberturvallisuudesta ja toteutettavasta kyberstrategiasta vastaa organisaation johto. Kyberstrategian kehittämistä ohjaa liiketoimintaprosessi ja toiminnan tehostaminen. Kyberstrategia tulisi kuitenkin laatia yhdessä asiantuntijoiden kanssa, jotta strategian suunnittelussa päästään kyberturvallisuuden perusasioita syvemmälle. Kyberstrategiassa paneudutaan kyberturvallisuuden johtamisen suunnitteluun, koko organisaation ajattelutavan muutokseen, kybertilannekuvan luomiseen sekä optimoituun resurssien käyttöön hyökkäysten ennaltaehkäisyssä ja mahdolliseen toimintaan hyökkäyksen aikana ja sen jälkeen. Organisaation johdon luoman kyberstrategian pohjalta tekniset asiantuntijat ja hallinnollisen tietoturvan edustajat soveltavat yksityiskohtaisemmin toimintaa. Kyberstrategian onnistumisen kannalta on oleellista, että johdon ja tietoturva-ammattilaisten lisäksi koko organisaatio on sitoutettu kyberstrategian toteuttamiseen. Täydellistä kyberturvallisuutta ei voida saavuttaa, vaan strategian tulee perustua

kokonaistilannekuvan ymmärtämiseen ja löytää siten tasapaino uhkien ja mahdollisuuksien suhteen. (Limnéll, Majewski & Salminen 2014, 157–160, 171.)

3.3 Kyberturvallisuuden nykytila Suomessa

Teknologiayrityksen Cisco Systemsin entinen toimitusjohtaja John Chambers on maininnut, että maailmassa on kahdenlaisia organisaatioita: niitä, joiden järjestelmät on hakkeroitu ja niitä, jotka eivät tiedä, että heidän järjestelmänsä on hakkeroitu (Cisco Press 2016). Kyberrikollisuus on laaja-alaista, monimuotoista ja se sisältää myös informaatiovaikuttamista. Kyberrikolliset pyrkivät vaikuttamaan tietojärjestelmiin joko muokatakseen tietoa, varastaakseen sitä tai estääkseen palvelun toiminnan. Yhä useammin kyberhyökkäyksen taustalla on taloudelliset motiivit tai halu horjuttaa yhteiskuntajärjestystä. Tyypillisimpiä kyberuhkia ovat erilaiset haitta- tai kiristysohjelmat, palvelunestohyökkäykset ja tietojenkalastelu. Toimijoina voi olla yksittäiset henkilöt, järjestäytyneet rikollisliigat, tai valtiolliset toimijat tai heidän palkkaamat alihankkijat. (Kinnunen, Seppo & Rousku 2021, 28.)

Suomessa toimivien organisaatioiden kyberturvallisuustilan arvioidaan olevan Euroopan keskitasoa vahvempaa, mutta kyberturvallisuushaasteita on tunnistettu ja Suomen kyberturvallisuustilan todetaan olevan heikompi kuin muissa Pohjoismaissa. Varsinkin tietovuodot ovat aiheuttaneet eri kokoisille organisaatioille kyberturvallisuutta uhkaavia haasteita. (ETLA Muistio 2020, 6–7.) Organisaatiot itse ovat erityisen huolestuneita kiristyshaittaohjelmahyökkäyksistä, jotka onnistuessaan voivat vaikuttaa jopa koko yritystoiminnan loppumiseen (Limnéll 2022).

Yhtenä suurena koko kyberturvallisuusalan haasteena, joka ei rajoitu vain Suomen rajojen sisäpuolelle, on kysynnän ja tarjonnan välinen ristiriita. Kyberturvallisuusammattilaisista on suuri pula. Kyberturvallisuusalan kattojärjestön FISC:in mukaan kyberturvallisuusammattilaisia tarvitaan vuoteen 2025 mennessä 15 000 lisää. Tähän on syynä se, että kyberturvallisuus ei kosketa vain IT-alaa, vaan se on levittäytynyt koskemaan jokaisen ihmisen elämää ja varsinkin heidän kokemaa turvallisuuden tunnetta. Organisaatioiden tarve ei ole enää löytää vain ohjelmoijia, vaan tulevaisuuden laaja-alainen digitalisaation kehittyminen aiheuttaa

kyberturvallisuuden ja datan osaajille entistä enemmän ja laaja-alaisempaa kysyntää. Osaavien ammattilaisten ammattitaidon kehittyminen vaadittavalle tasolle tulee kuitenkin kestämään vielä vuosia. Yleisradion (2022) julkaisemassa artikkelissa Jyväskylän yliopiston kyberturvallisuuden työelämän professori Martti Lehto kertoo toimittamansa tutkimuksen tuloksista, joiden mukaan korkeakoulujen koulutus ei vastaa täysin työelämän tarpeisiin. Kouluttamisen osalta haasteena on löytää hyviä opettajia ja vaikka kyberturvallisuusosaajia tarvitaan runsaasti, on harjoittelupaikkojen löytäminen haastavaa. Lyhyellä aikavälillä pulaa tulee olemaan teknisistä osaajista ja pitkällä aikavälillä osaajatarve monipuolistuu muun muassa hallinnollisiin osaajiin. (Limnéll 2022; YLE 2022.). Ongelmaa pyritään ratkaisemaan koulutuksen lisärahoituksella. Jyväskylän yliopisto ja Jyväskylän ammattikorkeakoulu ovat saaneet opetus- ja kulttuuriministeriön myöntämän yli kolmen miljoonan euron rahoituksen kyberturvallisuuden koulutuksen kehittämiseksi. (Virranniemi 2022.)

Kyberturvallisuuskeskuksen julkaisemassa Kybersää elokuu 2022-katsauksessa kirjoitetaan organisaatioiden kyberturvallisuuden kehittämisen haasteista. Kyberturvallisuuden kehittämisen, toteuttamisen ja parantamisen haasteena ei ole pelkästään osaajapula, vaan organisaatioiden työkulttuuriin, toimintatapoihin ja prosesseihin tarvitaan myös kehitystä. Osaamisen on todettu henkilöityvän helposti, jolloin se muodostaa organisaation kyberturvallisuudelle ja jatkuvuudelle riskin. Organisaatioiden johdolla onkin haaste tunnistaa se kyberturvallisuusosaaminen, mitä tulevaisuudessa tarvitaan, varmistaa se, että osaaminen pysyy organisaation sisällä ja välttää avainhenkilöriippuvuuksien syntyä. Organisaatioiden tulisi myös kehittää läpinäkyvää ja koko organisaation läpi ulottuvaa kyberkulttuuria ja varmistaa siten, että jokainen työntekijä ymmärtää olevansa suuressa roolissa tietoturvan ja kyberturvallisuuden kehittämisessä ja ylläpidossa. (Kybersää elokuu 2022.)

Suomessa ajantasaiseen kyberturvallisuuden tilannetietouteen ja tiedottamiseen on panostettu kansallisella tasolla. Huoltovarmuuskeskus (2022a) huolehtii varautumisesta kyberturvallisuuden häiriöihin ja Kyberturvallisuuskeskus (2022g) kehittää ja valvoo viestintäverkkojen ja -palveluiden turvallisuutta sekä tuottaa kyberturvallisuuden ajantasaista tilannekuvaa (kuvio 2). Kyberturvallisuuskeskus

julkaisee kuukausittain kybersään koosteen, jossa kerrotaan merkittävimmät kyberturvapoikkeamat- ja ilmiöt. Koosteet ovat julkisesti saatavilla.

Kuvio 2. Kybersää marraskuu 2022 (Kyberturvallisuuskeskus 2022)

4 SOSIAALI- JA TERVEYDENHUOLLON TIETOJÄRJESTELMIEN KYBERUHKAT

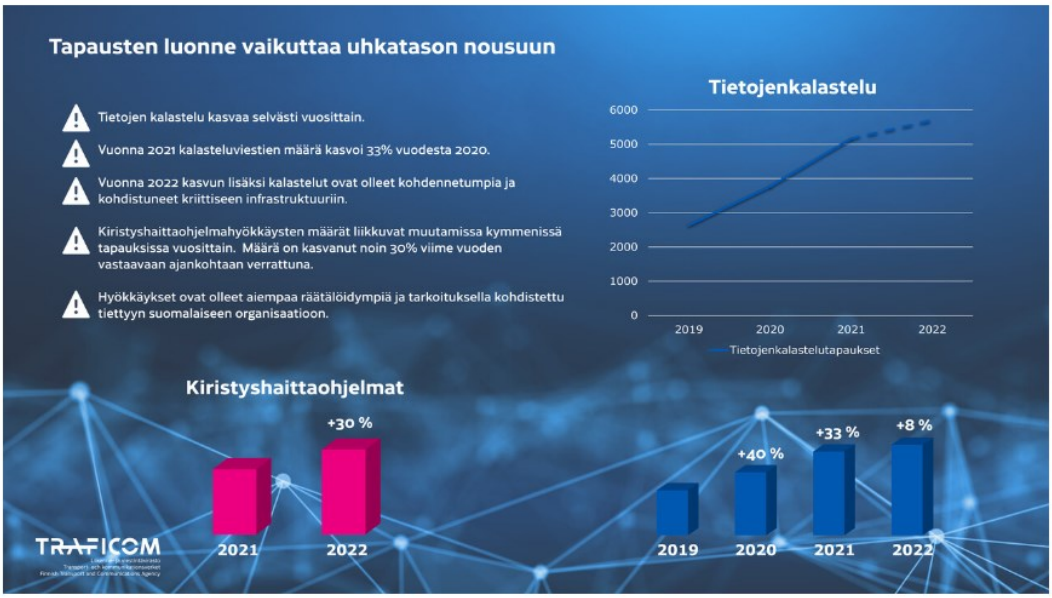
4.1 Suomeen kohdistuvat kyberuhkat

Kyberhyökkäysten määrä on lisääntynyt maailmanlaajuisesti viime vuosien aikana. Traficomin (2022) saamien tietojen mukaan suomalaisiin organisaatioihin kohdistuu erityisesti haittaohjelmia, tietojenkalasteluja ja palvelunestohyökkäyksiä, kuten kuviosta 3 on havaittavissa. Kybervaikuttamisen toimintatavat ovat muuttuneet selkeästi räätälöidymmiksi, sillä on huomattavissa, että vaikuttamista halutaan kohdistaa yksittäisiin, ennalta valittuihin, organisaatioihin aikaisemman hakuammunnan sijaan. Vuoden 2022 aikana kyberrikollisten kohteena on ollut entistä enemmän kriittinen infrastruktuuri. (Traficom 2022.)

Siinä missä Traficom (2022) pidättäytyy mainitsemasta suoraan Venäjän osallisuutta kasvavaan kyber- ja informaatiovaikuttamiseen sekä kybervakoiluun, kirjoittaa Suojelupoliisin päällikkö Antti Pelttari (2022) tästä avoimemmin. Hänen mukaansa koko EU:n alueella ovat lisääntyneet erilaiset kyberhyökkäykset kesän 2022 kuluessa, kun Venäjän eteneminen Ukrainan alueella hidastui. Venäjän hyökkäyssodan aiheuttamat pakotteet vaikuttavat Suomessa eniten energian hintaan, ja tätä voidaan olettaa Venäjän käyttävän hyväkseen kohdennetussa informaatiovaikuttamisessa. Pelttari (2022) varoittaa myös kohdennetusta kybervakoilusta, jota Venäjän oletetaan kohdistavan suomalaisiin organisaatioihin tarkoituksenaan kerätä tietoa ja kiertää sodan vuoksi asetettuja pakotteita. Pakotteet ja taloudellinen tilanne Venäjällä saattavat lisätä myös taloudellista hyötyä tavoittelevia kyberiskuja.

Pelttarin (2022) mukaan suurin osa Suomeen tehdyistä kyberiskuista on verkkopalveluihin kohdistuvia palvelunestohyökkäyksiä, sillä näiden toteuttaminen on helppoa. Suomessa yhteiskunta toimii vahvasti digitaalisten palveluiden ympärillä ja tieto on totuttu saamaan käyttöön reaaliaikaisesti. Pelttari (2022) mainitseekin, että organisaatioiden on hyvä tiedostaa kohonnut hyökkäysten uhka, vaikka koko yhteiskunnan lamauttavaa palvelunestohyökkäystä tuskin pystytään toteuttamaan. On tärkeää huomioida, etteivät Suomeen kohdistuvat kyberuhkat tule vain

Venäjältä. Eurooppaan ja Suomeen kohdistuu myös muiden tahojen harjoittamaa kybervaikuttamista ja -toimintaa. Näistä hyvänä esimerkkinä Pelttari (2022) mainitsee Kiinan, jonka tiedetään kohdistavan länsimaihin runsaasti erilaista kybertoimintaa.



Kuvio 3. Kyberhyökkäysten määrän kasvu (Traficom 2022)

4.2 Sosiaali- ja terveydenhuollon kyberuhkat

Kyberhyökkäyksiä toteutetaan sosiaali- ja terveydenhuollon organisaatioihin monista syistä. Yksi yleisimmistä tekijöistä on rahallisen hyödyn tavoittelu. Sosiaali- ja terveydenhuollon tietojärjestelmien sisältämä tieto on perinteisiä luottokorttitietoja arvokkaampaa, sillä tietojen myynnistä voi pyytää huomattavasti suurempaa hintaa verrattuna perinteisiin luottokorttitietoihin. Varastettuja tietoja on käytetty hyväksi esimerkiksi lääkeainevarkauksien mahdollistamiseen, jolloin rahallinen hyöty on saatu myymällä lääkeaineita pimeässä verkossa. Asiakas- ja potilastietoja on käytetty myös pankkitilien avaamiseen, lainanottamiseen ja passien hankintaan. Myös kiristystilanteissa tiedot ovat osoittautuneet arvokkaaksi, sillä asiakas- ja potilastietojärjestelmät ovat sosiaali- ja terveydenhuollon organisaatioiden toiminnalle elintärkeitä ja sen vuoksi organisaatiot ovat valmiita maksamaan lunnaita tietojen palauttamiseksi. Digitalisaatio on vaikuttanut siihen, että onnistunut yksittäinen kyberhyökkäys voi vaikuttaa huomattavaan määrään ihmisiä. Lisäksi

sosiaali- ja terveydenhuollon organisaatiot ovat toistaiseksi resursoineet huonosti kyberturvallisuuteen, joten kybervaikuttaminen on helpompaa kuin esimerkiksi rahoitusalalla. (Coventry & Branley 2018, 49; Lehto, Pöyhönen & Lehto 2019, 11–12.)

Rahallisen hyödyn lisäksi terveystietoihin on murtauduttu myös poliittisista syistä. Esimerkiksi Maailman antidopingjärjestö WADA:n tietokantaan murtauduttiin ja valikoitujen urheilijoiden terveystietoja vuodettiin julkisuuteen tarkoituksena mustamaalata tiettyjä urheilijoita disinformaation keinoin (BBC 2016). Terveydenhuollon palveluiden näkyvyyttä on käytetty poliittisesti hyväksi myös esimerkiksi Isossa-Britanniassa, kun NHS:n (National Health Service) verkkosivuille murtauduttiin ja sivuilla esitettiin kuvia Syyrian sodan uhreista (Sengupta 2017).

Sosiaali- ja terveydenhuollon palvelujen verkottuminen, applikaatiot ja lääkelaiteliitännät ovat lisänneet palvelujen yksilöllisyyttä, laatua ja vähentänyt hoitovirheitä. Varsinkin terveydenhuollon alalla teknologia kehittyy ja esimerkiksi pitkäaikaissairaiden ihmisten hoitoon on kehitetty lääkinnällisiä laitteita, jotka on liitetty sairaaloiden tietojärjestelmiin. Kun laitteiden ja tietojärjestelmien verkottuminen lisääntyy, lisääntyvät myös mahdolliset väylät kyberuhkille. Yksikin laite saattaa avata väylän palomuurien ohitse sairaalan tietoverkkoihin. Lääkinnälliset laitteet, kuten esimerkiksi insuliinipumput ja sydämentahdistimet, voivat mahdollistaa väylän sille, että potilaan arkaluontoiseen tietoon päästään käsiksi ja sitä voidaan käyttää identiteettivarkauteen. Laitteeseen voidaan myös asentaa haittaohjelma tai virus, joka vaikuttaa laitteen toimintaan, laitetta voidaan manipuloida toimimaan väärin tai lopettamaan toimintansa, jolloin ihmisen henki voi vaarantua. (Williams & Woodward 2015, 307; Coventry & Branley 2018, 48–49; Weber & Kleine 2020,147.) Toistaiseksi ei ole tiedossa, että tämänkaltaista toimintaa olisi toteutettu rikollisena toimintana, mutta Michiganin yliopiston tutkijaryhmä on demonstroinut miten helposti murtautuminen implantteihin, kuten sydämentahdistimeen, onnistuu (Williams & Woodward 2015, 307).

Tulee muistaa, että kaikki kyberuhkat eivät tapahdu suoraan tietojärjestelmissä, verkkoon liitetyissä laitteissa tai sairaalaympäristössä. Sosiaali- ja terveydenhuollossa palveluita tarjotaan usein asiakkaan tai potilaan kotona ja tämä tuo uusia

haasteita kyberturvallisuudelle, koska palveluntarjoajan perinteinen tietoturva ja kyberturva ei ulotu näihin ympäristöihin. Kyberturvallisuusuhkia on tunnistettu tulevan siitä, että ihmiset ovat tehneet virheitä konfiguroinnissa eikä kaikkia tietoturvaan liittyviä asioita ole huomioitu oikealla tavalla tai RFID-siruja, joita käytetään esimerkiksi kulkuluvissa, on kopioitu. (Coventry & Branley 2018, 48–49; Sosiaali- ja terveysministeriö 2019, 20.) Sosiaali- ja terveydenhuollon alan kyberuhkat eivät ole vain ihmislähtöisiä. Myös ympäristötuhot tai maailman poliittinen tilanne saattavat vaikuttaa esimerkiksi sähkön saantiin tai tietoverkkojen toimintaan (Sosiaali- ja terveysministeriö 2019, 20).

Sosiaali- ja terveydenhuolto ovat vahvasti riippuvaisia toimivista tietojärjestelmistä ja niihin liitetyistä palveluista. Näitä palveluita ovat yksittäisten operatiivisten tietojärjestelmien lisäksi muun muassa Kanta-palvelut, joiden toimintaan vaikuttivat loppuvuodesta 2022 tapahtuneet Kelan palveluihin kohdistetut palvelunestohyökkäykset (Melanen 2022). Kriittisen infrastruktuurin palveluiden laadukas ja jatkuvasti kehittyvä suojaus kaikkia uhkia vastaan on elintärkeää. Sosiaali- ja terveydenhuollon tietojärjestelmätoimittajien ja palveluntarjoajien tulee tehdä jatkuvaa ja tiivistä yhteistyötä kyberturvallisuuden parantamiseksi kehittämällä varautumista, toiminnan jatkuvuutta, tietoturvaa ja tietosuojaa. (Sosiaali- ja terveysministeriö 2019, 14,17; Kinnunen, Seppo & Rousku 2021, 28.)

4.3 Kybervaikuttamisen keinot

Euroopan unionin kyberturvallisuusviraston (Enisa) julkaiseman Enisa Threat Landscape 2022 -raportin (ENISA 2022, 4) mukaan 07/21–06/22 välisenä aikana Euroopan yleisimmät kyberuhkat olivat

- kiristyshaittaohjelmat (ransomware)
- haittaohjelmat (malware)
- sosiaalinen vaikuttaminen (social engineering threats)
- tietoon kohdistuvat uhkat (threat against data)
- palvelunestohyökkäykset (threat against availability: Denial of Service)
- internettiin kohdistetut hyökkäykset (threat against availability: Internet threats)

- valeuutisointi, väärän tiedon levittäminen (disinformation/ misinformation)
- toimitusketjuihin vaikuttavat hyökkäykset (supply chain attacks).

Euroopassa sosiaali- ja terveydenhuoltoon kohdistui 06/21–07/22 välisenä aikana lähes yhtä paljon hyökkäyksiä kuin rahoitusalalle. Hyökkäyksissä onnistuttiin tekemään tietomurtoja siten, että arkaluontoista asiakas- ja potilastietoa päätyi rikollisten haltuun ja toisaalta onnistuttiin palvelunestohyökkäyksillä estämään muun muassa ajanvarauksien tekeminen sosiaali- ja terveydenhuollon organisaatioihin. Terveydenhuoltoon suunnattiin runsaasti verkkosovelluksiin kohdistuvia hyökkäyksiä ja muita järjestelmiin luvattomasti tunkeutumisia. Nämä yhdessä luokittelemattomien uhkien kanssa kattoivat 76 % sosiaali- ja terveydenhuollon alalle kohdistuvista rikkomuksista. Huomioitavaa on, että kybervaikuttamista todettiin tapahtuneen runsaasti myös organisaatioista sisälähtöisesti. Covid-19-pandemiaan ja varsinkin rokotteisiin liittyvä valeuutisointi jatkui vuonna 2022 runsaana. Lisäksi onnistuneet haitta- ja kiristyshaittaohjelmahyökkäykset OT-järjestelmiin vaikuttivat välillisesti myös terveydenhuollon palveluihin. (ENISA 2022, 14, 17, 33, 64, 85.)

4.3.1 Tietojenkalastelu

Tietojenkalasteluyritykset ovat yleistyneet viime vuosina rajusti niin Suomessa kuin ulkomaillakin, ja osansa siitä saa myös sosiaali- ja terveydenhuollon ala (ETLA Muistio 2020, 4). Tietojen kalastelun tavoitteena on saada tietoon käyttäjätunnus- ja salasanapareja tai muita tärkeitä tietoja. Iso osa tietojenkalastelusta toteutetaan lähettämällä sähköposti tai tekstiviesti, jossa oleva huijaustarkoitukseen luotu linkki ohjaa linkin sivuille kirjoitetut tunnistetiedot suoraan tietojenkalastelijalle. Tietojenkalasteluviestit ovat kehittyneet uskottavan oloisiksi ja tämän vuoksi rikolliset onnistuvat entistä useammin saamaan haluamansa tiedot. Viime aikoina tietojenkalastelua on tapahtunut erityisesti Microsoft Office 365 -ympäristössä. Tietojenkalastelun motiiveja on monia: voidaan haluta seurata laskutusliikennettä, jolloin hyöty on taloudellista tai voidaan haluta aiheuttaa mainehaittoja, jolloin vaikutus on enemminkin poliittinen. (Traficomin julkaisuja 2/2020, 4.)

IBM Security (Zaboeva 2020) onnistui havaitsemaan ja paljastamaan syyskuussa 2020 aloitetun laajan kansainvälisen tietojenkalasteluyrityksen, jossa pyrittiin vaikuttamaan koronarokotteisiin. Tietojenkalastelua yritettiin toteuttaa sähköpostin välityksellä lähettämällä viestejä organisaatioihin, jotka olivat vastuussa Covid-19-rokotteiden kylmäketjusta. Myös muita koronaan liittyviä vaikutusyrityksiä on toteutettu, kuten esimerkiksi Euroopan lääkevirastoon onnistuttiin murtautumaan ja pääsemään käsiksi Pfizerin koronarokotteen tietoihin (Security Week 2020). Potilastietueisiin kohdistunutta tietojenkalastelua on toteutettu onnistuneesti varsinkin Yhdysvalloissa. UConn Health sairaalan 326 000 potilaan tietoihin päästiin murtautumaan sähköpostitilien hakkeroinnin kautta (Davis 2019) ja Charleston Area Medication Centerin järjestelmään kohdistetun onnistuneen sähköpostin kautta toteutetun tietojenkalasteluyrityksen kautta rikolliset pääsivät käsiksi 54 000 potilastietueeseen (Adams 2022).

4.3.2 Palvelunestohyökkäykset

Palvelunestohyökkäyksen tarkoitus on lamaannuttaa joku palvelu tai tietojärjestelmä kuormittamalla verkkoa ylimääräisellä tietoliikenteellä. Hyökkäykset pyrkivät löytämään mahdollisia heikkouksia organisaatioiden tietojärjestelmistä ja sellaisen löydettyään, ne pyrkivät käyttämään sitä hyväkseen. Tyypillisesti tämänkaltaiset hyökkäykset kestävät niin kauan, kunnes hyökkäys saadaan torjuttua, mutta hyökkääjä saattaa keskittää seuraavan palvelunestohyökkäyksen organisaation toiseen osaan. Palvelunestohyökkäykset ovat usein kansainvälisiä ja automatisoituja. Organisaatioiden tulisi tunnistaa palvelunestohyökkäykset sekä ilmiönä että teknisesti, jotta näitä vastaan suojautuminen olisi tehokasta (Traficomin julkaisuja 2/2020, 8). Usein organisaation heikkous löytyy ihmisten toiminnasta, sillä käyttäjätunnuksia ja salasanoja, joiden avulla organisaation järjestelmään päästään sisään toteuttamaan hyökkäys, onnistutaan keräämään sähköpostin välityksellä. Tämän vuoksi palvelunestohyökkäysten ehkäisynä organisaatioissa tulee panostaa henkilöstön koulutukseen. Palvelunestohyökkäyksiin voi varautua myös riittävällä tietoliikennekapasiteetilla ja esimerkiksi teleoperaattoreiden tarjoamilla palveluilla, joilla haitallinen liikenne siivotaan pois. (Traficomin julkaisuja 2/2020, 8; Kyberturvallisuuskeskus 2022e.)

Hyökkäyksiä tekeviä tahoja on monia, aina yksittäisistä henkilöistä valtiollisiin toimijoihin. Kyberturvallisuuskeskuksen (2022e) mukaan Suomessa tapahtuu vuosittain yli 10 000 palvelunestohyökkäystä eri organisaatioiden verkkosivuille. Palvelunestohyökkäysten yleisyys johtuu siitä, että niitä on verrattain helppo toteuttaa ja palvelun voi ostaa ulkoiselta taholta. Helsingin ja Uudenmaan sairaanhoitopiirin verkkopalveluihin toteutettiin noin viikon kestävä palvelunestohyökkäys syksyllä 2021 (HUS 2021). Useissa sairaanhoitopiirin ylläpitämissä verkkopalveluissa, kuten hus.fi-verkkosivuilla, Terveyskylän palveluissa sekä koronarokotus- ja näytteenoton ajanvarauksissa oli ajoittaisia käyttökatkoksia. Itse sairaanhoitopiirin käyttämän potilastietojärjestelmän toiminta ei vaarantunut. Kanta-palvelun toiminnassa oli häiriöitä joulukuussa 2022, kun palvelunestohyökkäys kohdistui koko Kelan palveluihin (Melanen 2022). ENISA (2022, 108) raportoi toukokuussa 2022 palvelunestohyökkäyksestä Italian julkiseen hallintoon, sisältäen terveyspalveluiden instituutin. Hyökkäyksen tekijöinä olivat Venäjän hakkerit, joiden tarkoitus oli kohdistaa palvelunestohyökkäyksiä Naton jäsenmaihin.

4.3.3 Haittaohjelmat

Haittaohjelmien tarkoituksena on kirjaimellisesti tuottaa haittaa verkkosivuille ja tietojärjestelmiin. Haittaohjelmat leviävät saastuneiden sähköpostin liitetiedostojen, verkkosivujen ja haavoittuvien palvelimien välityksellä. Tyypillisesti tämän kaltaiset kybervaikuttamiset kohdennetaan tahoille, jotka nähdään houkuttelevina ja rahakkaina. Nämä ovat yleensä suuria organisaatioita, joilla on runsas käyttäjä- ja asiakasmäärä. Hyökkäyksessä haittaohjelma on päässyt jo leviämään organisaation verkkoon, ja ohjelman käynnistyttyä ongelmat näkyvät toiminnan hitautena tai muina organisaation toimintaa haittaavina toimintoina. Ne voivat lamauttaa toiminnan lähes kokonaan. (Traficomin julkaisuja 2/2020, 6; Kyberturvallisuuskeskus 2022a.)

Kyberturvallisuuskeskus tuottaa vuosineljänneksittäin julkaisun yleisimmistä haittaohjelmista, joita sen Autoreporter-järjestelmä on tunnistanut. Vuoden 2022 kolmannen neljänneksen yleisimmät havainnot tulivat Hummer-piilohallintaohjelmasta, joka on suunniteltu Android-käyttöjärjestelmälle. Se pyrkii korottamaan itselleen pääkäyttäjäoikeudet, jonka jälkeen se vaikeuttaa laitteen käyttöä

esimerkiksi jatkuvalla mainosviestinnällä tai aikuisviihteellä. (Kyberturvallisuuskeskus 2022a.)

Monessa sosiaali- ja terveydenhuollon organisaatiossa käytetään viestintäpalvelu Teamsia. Talvella 2022 uutisoitiin, että haittaohjelmia on onnistuttu levittämään myös Teams-keskustelujen välityksellä (Laakso 2022). Erilaisia puhelimia ja älylaitteita pyritään altistamaan haittaohjelmille. Android-käyttöjärjestelmälle tarkoitettu Google Playsta löytyvä sovellus paljastui olevan todellisuudessa haittaohjelma (Kullas 2022). Lahden kaupungin tietoverkossa yli tuhanteen koneeseen levinnyt haittaohjelma lähti yksittäisen työaseman luvattomasta yhteydestä (Ahjopalo 2019). Haittaohjelman vuoksi tietoliikenneyhteydet Lahden kaupungin ja Päijät-Hämeen hyvinvointiyhtymän välillä oli katkaistava, jotta haittaohjelman leviäminen saatiin loppumaan. Tämä vaikutti suuresti terveydenhuollon potilaisiin muun muassa sähköisten reseptien ja laboratoriotulosten osalta. Yhdysvalloissa US Department of Veterans Affairs järjestön verkkoon päässyt haittaohjelma vaikutti yli 50 000 lääkinnälliseen laitteeseen (Williams & Woodward 2015, 307).

4.3.4 Kiristyshaittaohjelmat

Kiristyshaittaohjelmat ovat haittaohjelmia, joissa tarkoituksena on päästä käsiksi organisaation dataan, salata tieto salausalgoritmilla ja vaatia tämän jälkeen lunnaita tietojen palauttamista vastaan. Kiristämistä voidaan toteuttaa myös varastamalla ja uhkaamalla julkaista tiedot, ellei kiristäjän vaatimuksiin suostuta. Tämän kaltaisten kyberhyökkäysten määrä on kasvussa Suomessa. Vuodesta 2020 vuoteen 2021 määrä kasvoi noin 105 %. Hyökkääjät pääsevät organisaation tietoihin hyödyntämällä tietorakenteen heikkouksia tai ihmisen virheestä, esimerkiksi saastuneen sähköpostin linkin tai liitteen avaamisen välityksellä. Kiristyshaittaohjelmilla haetaan pääasiallisesti taloudellista hyötyä ja kohteeksi valikoituu usein organisaatiot, joilla kyberturvallisuuteen varautuminen on heikkoa. Ongelmallista on, että vaikka organisaatio maksaisikin lunnaat, hyökkäys ja kiristys saattavat jatkua siitä huolimatta. (Traficomin julkaisuja 12/2022.)

Psykoterapiakeskus Vastaamon tietomurto 2018–2019 oli kansainvälisestikin historiallinen tietoturvaloukkaustapaus. Tietomurtautuja pääsi käsiksi

potilastietoihin hyödyntäen organisaation tietorakenteen heikkouksia, jonka jälkeen potilastiedot varastettiin ja ne uhattiin julkaista verkossa, ellei kiristäjän lunnasvaatimuksiin suostuttaisi. Tapaus osoitti sen, että kiristäjillä ei ole moraalisia ja eettisiä säännöksiä. Vastaamon tietomurrossa verkkoon levisi tietoja psykoterapiassa käyneiden ihmisten potilastietomerkinnöistä sekä heidän henkilöturvatunnuksiansa. Tietovuotoon liittyvänä lieveilmiönä henkilöiden henkilötietoja on alettu käyttämään tilauspetoksissa ja identiteettivarkauksissa. (Sosiaali- ja terveysministeriö 2017, 19; Kyberturvallisuuskeskuksen viikkokatsaus – 44/2022.)

Toukokuussa 2017 WannaCry-niminen kiristyshaittaohjelma vaikutti vähintään 200 000 tietotekniseen laitteeseen ainakin sadassa eri maassa vaatien uhreilta bitcoinlunnaita. Isossa-Britanniassa vaikutuksen kohteena oli NHS, vaikkakaan sitä ei ollut siihen varsinaisesti kohdennettu. Viidenkymmenen brittiläisen sairaalan tietojärjestelmät lakkasivat toimimasta ja potilaiden hoito viivästyi, kun MRI-laitteet tai verivalmisteiden säilytykseen käytetyt jääkaapit eivät toimineet (National Audit Office 2017, 4; Coventry & Branley 2018, 50.) Kyseinen WannaCry-kiristyshaittaohjelma löytyi myös muun muassa Turun yliopistollisen keskussairaalan eräästä kuvantamislaitteesta (Sosiaali- ja terveysministeriö 2019, 19). ENISA (2022, 45) raportoi ainakin kesäkuusta 2021 lähtien aktiivisena olleesta RaaS-palveluntuottajasta (ransomware-as-a-service) Hivestä, jonka avulla toteutettiin isku Costa Rican julkiseen terveydenhuoltoon. RaaS-palveluiden tarjoajat myyvät kehittämäänsä haittaohjelmaa, jolloin palvelunostajalla ei tarvitse olla tietoteknistä osaamista kiristyshaittaohjelman kehittämiseen ja siten kiristyshaittaohjelmien kautta tehtävien kyberhyökkäysten toteuttaminen helpottuu.

5 KYBERTURVALLISUUDEN HALLINTA JA KEHITTÄMINEN

5.1 Kyberturvallisuuden hallinta

Organisaatioiden kyberturvallisuuden vaatimukset on määritelty EU:n ja kansallisen tason lainsäädännössä, asiakkaiden kanssa tehdyissä sopimuksissa ja muissa suosituksissa ja ohjeissa, kuten kuvio 4 osoittaa. Sopimukset ja lait velvoittavat organisaatioita huolehtimaan tietoturvallisuuden tasosta, eikä näitä vaatimuksia voi jättää täyttämättä. (VAHTI 3/2012, 11–12.) Lainsäädäntö velvoittaa organisaatioita enenevissä määrin määrittelemään prosesseja ja nimeämään toiminnoille vastuutahoja, mikä vaikuttaa suoraan organisaatioiden kyberturvallisuutta parantavasti. Suurin vastuu organisaatioiden kyberturvasta on johdolla, jonka tehtävänä on määritellä kyberstrategia. Kyberstrategian tarkoituksena on ohjata organisaation tietoturvan ja kyberturvan toteuttamista. Strategiaa laatiessa tulee huomioida lakien ja sopimusten määrittelemät reunaehdot. (Kyberturvallisuuskeskus 2022d.)

Kuvio 4. Organisaation tietoturvallisuuteen vaikuttavat tekijät (VAHTI 3/2012, 12)

Huoltovarmuuskeskuksen (2020, 10–11) toteuttamassa organisaatioiden kyberturvallisuuden tilaa tutkivassa kartoituksessa nousi esiin haasteita kyberturvallisuusstrategian, kyberturvallisuusriskienhallinnan ja riskienhallintastrategian riittävässä määrittelyssä. Useassa organisaatiossa kyberturvallisuudesta

huolehtiminen nähdään edelleen teknisenä tukitoimena, vaikka se pitäisi ymmärtää pitkäjänteisenä kehitystyönä ja tärkeänä osana organisaation liiketoimintaa. Organisaation tehokkaaseen ja turvalliseen toimintamalliin pääseminen vaatii kyberturvallisuuden tavoitetilan määrittelyn ja sen toteuttamiseksi laaditun strategian. Strategian tulisi olla määritelty niin, että se ohjaa riittävästi kyberturvallisuuden vastuuhenkilöiden toimintaa kehittämisessä, valinnoissa ja investoinneissa. (Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot 2020, 10–11.)

Kyberturvallisuuden strateginen määrittely ja johtaminen ei ole yksinkertaista, sillä organisaation toimintaympäristö muuttuu jatkuvasti. Toimintaympäristön hahmottamiseen, strategian suunnitteluun ja kyberturvallisuuden kehittämisen käytännön tueksi on kehitetty erilaisia työkaluja. Työkalujen käyttö luo strategiselle johtamiselle tietopohjan, jolloin toimintaympäristössä tapahtuvat muutokset voidaan ottaa laajemmin huomioon. Toimintaympäristön muutosten vaikutusten ennakoimiseen voidaan käyttää strategiatyökaluja, kuten SWOT- tai PESTEL-analyysi (Vuorinen 2014, 220–222, 249–253). Näin organisaatiot kykenevät ennakoimaan tulevaa ja ovat siten valmistautuneita toimimaan paremmin ja tehokkaammin. Organisaatiot voivat myös ottaa strategiseksi tavoitteeksi osoittaa tietoturvatasonsa käyttämällä kansainvälisesti tunnistettuja tietoturvastandardeja, kuten ISO 27001, jolloin organisaation ulkopuolelle ja yhteistyötahoille välittyy viesti organisaation kyberturvallisuuden tilasta. (Mutanen, Tolonen & Vepsäläinen 2021, 7–8.)

Kyberturvallisuuden käytännön parantamiseen on kehitetty kansallisella tasolla ohjeistuksia ja mittareita, kuten VAHTI-ohjeet (Suomidigi 2022) ja Kybermittari (Kyberturvallisuuskeskus 2022c). Näiden työkalujen ja ohjeiden avulla organisaatiot voivat kehittää käytännön kyberturvallisuutta ja mitata kyberturvallisuuden kypsyystasoa. Oman organisaation toimintaympäristön ymmärtämisen ja kyberturvallisuuden kehittämisen tukena organisaatiot voivat osallistua ulkopuolisten tahojen kuten Huoltovarmuuskeskuksen Digipoolien (Huoltovarmuuskeskus 2022b) tai Kyberturvallisuuskeskuksen ISAC-tiedonjakoryhmien toimintaan (Kyberturvallisuuskeskus 2022b).

5.2 Varautuminen

Kyberturvallisuuskeskuksen (2022d) julkaiseman johdolle ja asiantuntijoille suunnatun ohjeistuksen mukaan organisaatioiden tulisi tarkastella mahdollisten kyberuhkien vaikutuksia omaan toimintaansa kokonaisvaltaisesti. Organisaation johdolla tulisi olla ajantasainen ymmärrys yrityksen digitaalisista palveluista ja niiden suojaustoimenpiteistä sekä toimintaympäristöstä ja siihen vaikuttavista muuttuvista tekijöistä. Varautumisen tärkeimpänä tarkoituksena on kyberuhkatilanteeseen reagoinnin sijasta ennakointi. Painopisteenä kyberturvallisuuden varautumisessa ovat kyberturvallisuuden suunnittelu, hiljaisten signaalien havainnointi sekä erilaisten ennakointimenetelmien, tutkimustiedon, innovaatioiden ja erilaisten analyysien hyväksikäyttö. Varautumisen yhtenä osa-alueena on toimintaympäristön muutostrendien ajantasainen seuranta ja mahdollisten skenaarioiden läpi käyminen oman organisaation näkökulmasta. Organisaatiot voivat käyttää hyödykseen myös erilaisia sisäisiä ja ulkoisia auditointeja tai asiantuntija-arviointeja kyberturvallisuuden varautumisen tukena. Arviointiprosessin tulee olla osa varautumissuunnitelmaa, jotta sen vaikuttavuutta ja laatua voidaan arvioida luotettavasti. (Turvallisuuskomitea 2022a.)

Kyberturvallisuuskeskus (2022d) ohjeistaa edelleen, että varautumisen tärkeänä toimenpiteenä on varata riittävät resurssit kyberturvallisuuden varmistamiseksi ja toteuttamiseksi. Tietoturvatyön tulee olla jatkuvaa ja laadukasta sekä organisaation sisällä että yhteistyötahojen välillä. Organisaatioiden tulee varmistaa, että toiminta voi jatkua normaalitilanteen häiriötilanteissa ja poikkeusoloissa. Tämän vuoksi on tärkeää tiedostaa ja määritellä liiketoiminnan kannalta kriittiset toiminnot ja luoda suunnitelma näiden suojaamiseksi. Organisaation johdon, palveluista vastaavien asiantuntijoiden ja kumppaneiden tulisi muodostaa yhdessä dokumentoitu prosessi, jossa on kuvaus siitä, miten toimitaan mahdollisessa hyökkäystilanteessa, hyökkäyksen jatkuessa ja hyökkäyksen jälkeen. Varmuuskopioinnin tärkeys korostuu häiriötilanteessa, mutta prosesseissa tulee olla pohdittu ja kuvattu myös se, milloin ja mihin ympäristöön varmuuskopioitu tieto voidaan palauttaa ja kuka tekee asiasta päätöksen. Prosessikuvauksissa tulee ottaa huomioon, miten viestintä toteutetaan ja miten tarvittavaan henkilökuntaan saadaan

yhteys minä vuorokauden aikana tahansa. Varautumisen prosessia on kuvattu kuviossa 5. (Kyberturvallisuuskeskus 2022d; Turvallisuuskomitea 2022b.)

Kuvio 5. Ennakointi ja varautuminen (Turvallisuuskomitea 2022b)

5.3 Yhteistyö ja tiedon jakamisen tärkeys

TIETO22-harjoituksessa, jossa harjoiteltiin monien suurien, kriittiselle infrastruktuurille tärkeiden ja yhteiskunnan toimivuuden kannalta oleellisten, organisaatioiden ja eri viranomaisten, kuten Kyberturvallisuuskeskuksen, Puolustusvoimien ja poliisin välistä yhteistyötoimintaa laajojen kyberhäiriöiden varalta, on nostettu esiin tiedon tehokkaan ja tarkoituksenmukaisen jakamisen tärkeys (Huoltovarmuuskeskus 2021; Pispa 2022). Pispan (2022) mukaan haasteena on ollut, että organisaatiot suhtautuvat varovaisesti turvallisuusuhkiin liittyvään sensitiiviseen tietoon ja sen jakamiseen. Yhteistyöharjoituksia toteutetaan säännöllisesti ja niiden nähdään kuitenkin lisänneen organisaatioiden välisiä kontakteja ja näin ollen luottamus verkoston toimintaan on lisääntynyt. On ymmärretty, että tieto auttaa usein myös muita organisaatioita varautumaan ja suojautumaan. Varsinkin TIETO-harjoitusten kaltaisissa laaja-alaisissa kyberhäiriötilanteissa yhteistyö auttaa huomaamaan ja löytämään kehityskohteet ja -mahdollisuudet. (Huoltovarmuuskeskus 2021; Pispa 2022.)

Suurharjoitusten lisäksi Huoltovarmuuskeskuksen alaisuudessa toimii pooleja, jotka vastaavat toimiala- ja toimipaikkakohtaisesta operatiivisesta varautumisesta yhteistyössä elinkeinoelämän kanssa. Poolit toimivat Huoltovarmuuskeskuksen ja toimialajärjestöjen välisten sopimusten mukaisesti. Poolien tehtävänä

on alan organisaatioiden yhteistyönä seurata, selvittää ja huolehtia organisaation huoltovarmuudesta. Pooleissa tehdään myös selvityksiä ja esityksiä varmuus- ja turvavarastoinnin tarpeesta. Oleellisena osana poolien toimintaa on järjestää tiedotus-, koulutus- ja harjoitustilaisuuksia, osallistua niihin ja toimia poolin antamien ohjeiden mukaisesti. (Huoltovarmuuskeskus 2022b.)

Organisaation omien tietoturvafoorumeiden, Huoltovarmuuskeskuksen poolien ja muiden yhteistyöväylien lisäksi on olemassa ISAC-tiedonvaihtoryhmiä (Information Sharing and Analysis Centre), joita Kyberturvallisuuskeskus ylläpitää. Nämä ovat kyberturvallisuuden yhteistyöelimiä, joissa voidaan käsitellä luottamuksellisesti kyberturvallisuuteen liittyviä uhkia, ilmiöitä ja jakaa hyviä käytänteitä. ISAC:n pääasiallinen tarkoitus on jakaa tietoa ja kokemuksia, jolloin organisaatiot voivat ottaa toisiltaan oppia kyberturvallisuuden parantamiseksi. Ryhmissä kehitetään myös oman toimialan riskianalyyseja, toteutetaan tutkimuksia ja luodaan ohjeistuksia. ISAC on organisaatioille kustannustehokas tapa lisätä ymmärrystä kyberuhkista ja saada tarvittaessa muilta alan toimijoilta asiantuntemusta, analyysiresursseja ja tietolähteitä häiriötilanteen tapahtuessa. (Mutanen, Tolonen & Vepsäläinen 2021, 23; Kyberturvallisuuskeskus 2022b: Kyberturvallisuuskeskus 2022d.)

5.4 VAHTI

VAHTI-verkosto on Digi- ja väestötietoviraston hallinnoima verkosto, jonka tarkoituksena on kerätä yhteen organisaatioiden johto ja digitaalisen turvallisuuden asiantuntijat. VAHTI on jaettu kolmeen eri kokonaisuuteen:

- VAHTI-johtoryhmä
- VAHTI-työryhmät
- VAHTI valtiohallinnon tietoturvan vastuuhenkilöiden verkosto, joka edistää valtiohallinnon tietoturvaa.

Verkostot toteuttavat ja koordinoivat yhdessä laaja-alaisella valmistelulla ja kansallisen tason yhteistyöllä digiturvallisuutta. Verkoston tavoitteena on ylläpitää luottamusta julkiseen hallintoon, turvata yhteiskunnalle elintärkeitä ja oleellisia

toimintoja sekä luoda digiturvallisempaa yhteiskuntaa. (Digi- ja väestötietovirasto 2022.)

VAHTI-johtoryhmään kuuluu julkisen hallinnon organisaatioita, jotka ovat kansallisella tasolla vastuussa digitaalisesta turvallisuudesta ja keskeisten palveluiden tuottamisesta. VAHTI-johtoryhmän tarkoituksena on koordinoida eri tahojen yhteistyötä ja siten kehittää ja sovittaa yhteen toimintatapoja digitaalisen turvallisuuden parantamiseksi. Johtoryhmä tuottaa VAHTI-ohjeita ja parhaita käytänteitä digiturvallisuuden eri osa-alueiden kehittämiseksi. VAHTI-johtoryhmään kuuluvat muun muassa Helsingin ja Uudenmaan sairaanhoitopiiri HUS ja Huoltovarmuuskeskus. (Digi- ja väestötietovirasto 2022; Suomidigi 2022.)

VAHTI-työryhmät tuottavat käytäntöjä, työkaluja ja mallipohjia organisaatioiden käyttöön. Työryhmiin voi hakeutua oman esihenkilön luvalla. Työryhmiin kuulumisen hyötynä on verkostoituminen muiden alan asiantuntijoiden kanssa ja mahdollisuus keskustella ajankohtaisista aiheista. VAHTI-työryhmiä ovat:

- toiminnan jatkuvuuden ja varautumisen kehittäminen
- ICT-palveluiden digitaalisen turvallisuuden kehittäminen
- tietosuojan kehittäminen
- digiturvaosaamisen kehittäminen
- riskien hallinnan kehittäminen. (Digi- ja väestötietovirasto 2022.)

VAHTI-verkoston tärkein ja kansalaisille näkyvin toiminta on tuotetut VAHTI-ohjeet, jotka löytyvät Suomidigin verkkosivuilta vapaasti luettavaksi ja hyväksi käytettäväksi. VAHTI-ohjeistus on maailman mittakaavassa yksi kattavimmista yleisistä tietoturvaohjeistuksista. VAHTI-ohjeissa digitaalinen turvallisuus on tarkastelun kohteena monelta eri näkökulmalta kuten fyysinen turvallisuus, henkilöstöturvallisuus, tietoliikenneturvallisuus ja hallinnollinen turvallisuus, joka sisältää johdon määrittelemät periaatteet, resurssit ja vastuunjaon. VAHTI-ohjeistuksia käytetään laajasti hyödyksi myös kansainvälisessä tietoturva- ja yhteistyössä, elinkeinoelämässä, erilaisissa organisaatioissa sekä kunnissa opetus- ja kansalaistoiminnassa. (Suomidigi 2022; Valtionvarainministeriö 2022.)

5.5 ISO 27001

Organisaatioiden kyberturvallisuuden hallintaa ja kehitystä voidaan toteuttaa noudattamalla kansainvälisesti tunnistettuja standardeja. Standardien noudattaminen osoittaa, että tietoturvallisuutta ja tietosuojaa hallitaan laadukkaasti. Standardien mukainen toiminta yhtenäistää toimintamalleja, jolloin uusien työntekijöiden perehdyttäminen organisaatioon ja yhteistyö muiden organisaatioiden kanssa helpottuu ja tehostuu. (Mutanen, Tolonen & Vepsäläinen 2021, 7–8.)

Mutanen, Tolonen & Vepsäläinen (2021, 7–8) ja Vepsäläinen & Tolonen (2021, 1–8) toteavat, että ISO 27001 -standardin mukainen tietoturvallisuuden hallintajärjestelmä pitää sisällään koko organisaation toiminnan tukien sitä strategisten tavoitteiden saavuttamisessa. Standardissa tärkeässä roolissa ovat johdon sitouttaminen tietoturvaan, laadukkaan tietoturvapolitiikan ja kulttuurin luominen organisaatioon sekä riskienhallinnan prosessien dokumentointi. Standardin vaatimalla systemaattisella lähestymistavalla organisaatio kykenee hallitsemaan tietoturvallisuutta ja siten saavuttamaan tavoitteet, joihin halutaan päästä. Organisaation johdon roolin lisäksi standardissa painotetaan koko organisaation henkilöstön tietoturvaosaamista ja tarvittavien tietoturvaan liittyvien roolien ja vastuiden selkeyttämistä. Toimintaympäristön tiedostaminen ja analysointi sekä tietoturvallisuuteen sitoutunut henkilöstö ovat avainasemassa toimivan tietoturvakulttuurin luomiseksi. Täydellistä tietoturvaa ei voida saavuttaa, vaan se on parhaimmillaankin laadukasta riskien hallintaa. Vepsäläisen & Tolosen (2021, 8) mukaan organisaatioissa tulisi panostaa tietoturvan jatkuvaan parantamiseen ja suorituskyvyn arviointiin seurannalla, mittareilla ja sisäisillä auditoinneilla. Toimintaympäristön analysointi tulisi toteuttaa vähintään vuosittain, jotta organisaatio pystyy määrittelemään muuttuneet, organisaatiosta riippumattomat, muutostekijät ja -ajurit. (Mutanen, Tolonen & Vepsäläinen 2021 7–8; Vepsäläinen & Tolonen 2021, 1–8.)

Vepsäläisen & Tolosen (2021, 3) mukaan ISO 27001 -standardi on yksi yleisimmistä standardeista, joita sosiaali- ja terveydenhuollon organisaatiot käyttävät tietoturvallisuuden hallintajärjestelmän viitekehyksenä. Sosiaali- ja terveydenhuollon perimmäisinä tietoturvavaatimuksina on, että asiakkaalle ja potilaalle on

kirjattu tietoja oikealle henkilölle oikealla tavalla, eikä tietoa ole muutettu luvattomasti tai tahattomasti. Tiedon tulee olla saatavilla asiakkaan ja potilaan hoidossa oikea-aikaisesti silloin kun sitä tarvitaan, ja sitä pitää päästä käsittelemään vain ne ammattihenkilöt, jotka hoitavat asiakkaan tai potilaan asioita, ja vain niiltä osin, kun se on tarpeellista. (Vepsäläinen & Tolonen, 2021, 3.)

5.6 Kybermittari

Kyberturvallisuuskeskus yhteistyössä Huoltovarmuuskeskuksen, kriittisen infrastruktuurin organisaatioiden ja muiden asiantuntijoiden kanssa on luonut organisaatioiden käyttöön Kybermittarin (Kyberturvallisuuskeskus 2022c). Tämä kansallisella tasolla kehitetty kyberturvallisuuden mittari mahdollistaa yhtämittaisen vertailun ja luo yhteisen kielen kyberturvallisuuden mittaamiseen ja kehittämiseen. Kybermittari on suunnattu huoltovarmuuskriittisille organisaatioille ja yhteisöille, mutta se on vapaasti löydettävissä ja otettavissa käyttöön Kyberturvallisuuskeskuksen verkkosivuilta myös muille organisaatioille. Mittarin avulla organisaatioiden johto ja tietoturva-ammattilaiset voivat arvioida kyberturvallisuuden tämänhetkistä kypsyystasoa ja kehittämiskohteita eri osa-alueilla. (Mutanen, Tolonen & Vepsäläinen 2021, 9–10; Kyberturvallisuuskeskus 2022c.) Kybermittari perustuu kansainvälisesti käytettyihin NIST Cybersecurity Framework (NIST 2022) ja Cybersecurity Capability Maturity Model (C2M2 2022) -malleihin.

Kybermittarin tarkoituksena on mitata työpajojen, itsearvioinnin ja haastattelujen avulla organisaation toimintamalleja, prosesseja ja tekniikoita. Tulosten perusteella voidaan arvioida organisaation käyttämien investointien vaikutusta kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Mittarin käytöllä pyritään luomaan johdon ja asiantuntijoiden käyttöön ymmärrettävä kuvaus niistä kyberturvallisuusriskeistä, joita organisaatio pystyy hallitsemaan ja arvioimaan, onko kaikki toiminnan kannalta oleelliset riskit varmasti tunnistettu. Kybermittarin rakenne koostuu yhdestätoista eri kyberturvallisuuden osiosta, osioille osoitetuista tavoitteista ja tavoitteiden täyttymistä mittaavista käytännöistä. Kybermittarin rakenne on esitetty kuviossa 6. Kybermittari toimii ohjaavasti, sillä se kertoo saavutetun kypsyystason ja osoittaa kehitysalueet, joita tarvitaan seuraavalle tasolle

siirtymiseen. (Mutanen, Tolonen & Vepsäläinen 2021, 10; Kyberturvallisuuskeskus 2022c.)

Kuvio 6. Kybermittarin rakenne (Mutanen, Tolonen & Vepsäläinen 2021, 10)

Ohjastusta mittarin käyttöön saa Kybermittari-tapahtumista, joita järjestetään Kyberturvallisuuskeskuksen toimesta tai palveluita voi ostaa organisaatioilta, jotka ovat perehtyneet Kybermittarin käyttöön. Organisaatiot voivat myös jakaa Kybermittarilla saadut tulokset Kyberturvallisuuskeskukselle, joka anonymisoi ja analysoi tulokset. Kyberturvallisuuskeskus hyödyntää tuloksia lakisääteisten tehtävien toteutukseen. Tulosten perusteella organisaatioille tarjotaan oman toimialan vertailutietoa muilta organisaatioilta sekä suosituksia kyberturvallisuuden edistämiseksi. (Kyberturvallisuuskeskus 2022c.)

5.7 PESTEL-analyysi

PESTEL-analyysi on strategiatyökalu, jolla arvioidaan organisaation toimintaympäristöä ja siihen vaikuttavia muutosvoimia. PESTEL-analyysiä voidaan joustavasti muokata toteutettavaksi organisaation tarpeiden mukaisesti joko lyhentämällä analyysiä tai toteuttamalla analyysi useaan kertaan organisaation eri yksiköiden sisällä. Tarkoituksena on tuottaa jäsennelty kuvaus eri osa-alueiden (poliittinen, ekonominen, sosiaalinen, teknologinen, ekologinen ja lainsäädännöllinen) muutosvoimista ja saada siten toimintaympäristöä koskeva tieto käytettäväksi organisaation strategian laatimisen tueksi. (Vuorinen 2014, 220–222.)

Analyysissa on tarkoituksena löytää organisaation toimintaympäristöön vaikuttavat teemat, joiden voidaan olettaa muuttuvan ja siten vaikuttavan organisaation toimintaan. PESTEL-analyysin tarkastelu-ulottuvuudeksi ehdotetaan lähteissä noin 3–10 vuotta, mutta analyysia voidaan käyttää osana skenaariotyöskentelyä ja luoda ulottuvuuksia vieläkin pidemmälle aikavälille. Vuorinen (2014, 222) mainitsee, että on kuitenkin hyvä tiedostaa, että PESTEL-analyysi itsessään ei tuota organisaatioille suurta lisäarvoa, vaan sen tulisi olla enemminkin lähtökohta strategisen aseman tarkastelulle. PESTEL-analyysi tulisi toistaa tietyin väliajoin, esimerkiksi vuosittain, jotta voidaan tarkastella toimintaympäristön muutoksia ja tehdä tarvittavat strategiset päätökset. (Vuorinen 2014, 220–222.)

PESTEL- analyysissa on tärkeä pohtia muutosvoimien voimakkuutta ja todennäköisyyttä. Analyysissa voidaan pisteyttää eri osioista esiin nousseet teemat sen perusteella, miten todennäköisesti ja laajasti muutosvoimat tulevat vaikuttamaan organisaation toimintaan. Analyysistä tulisi löytää organisaatiolle tärkeimmät toimintaympäristön muutokseen vaikuttavat kokonaisuudet. Näin voidaan keskittyä niihin suurimpiin kokonaisuuksiin ja teemoihin, joita voidaan hyödyntää tai joilta tulisi suojautua. (Vuorinen 2014, 220–225.)

5.7.1 Poliittinen analyysi

Organisaatioon vaikuttavat poliittiset tekijät muovaavat oleellisesti organisaation toimintaympäristöä. Poliittiset päätökset ja vaikuttimet muovaavat organisaation toiminnalle raamit, joiden puitteissa organisaation tulee toimia. Muutosvaikuttimet voivat olla globaaleja, kansallisia tai organisaation sisäisiä. Esimerkiksi sodat ja konfliktit lisäävät pakolaisuutta sekä ääriliikkeiden ja terrorismin uhkaa, jotka tulee ottaa huomioon organisaatioiden toiminnassa. Muita tekijöitä ovat muun muassa verotus ja muutokset puolueiden voimasuhteissa. (Vuorinen 2014, 222; Sisäministeriö 2017, 30–33.)

Euroopan epävakaa turvallisuusympäristö ja jatkuvasti muuttuvat valtasuhteet heijastuvat vahvasti kansallisella tasolla luoden epävarmuutta lähes kaikkiin organisaatioihin (Sisäministeriö 2017, 30–33). On ymmärretty, että tietoturvaan ja

kyberturvallisuuteen tulee panostaa. Valtioneuvosto (2022b) on antanut asetuksen tietoturvan kehittämisen tarpeellisuudesta eli niin kutsutuista tietoturvaseteleistä. Seteleiden avulla organisaatiot voivat parantaa järjestelmien tietoturvaa tai kehittää tietoturvaosaamistaan. Kyberturvallisuuden varautumistason nostamisen yhteiskunnan kriittisillä sektoreilla on katsottu parantavan yhteiskunnan kykyä suojautua muun muassa hybridiuhkilta.

5.7.2 Ekonominen analyysi

Organisaation kannattavuuteen ja toimintaan vaikuttavat taloudelliset asiat monesta eri näkökulmasta. Yleinen korkotaso ja rahoitus vaikuttavat siihen, miten organisaatio voi toimintaansa edistää. Muita tärkeitä tekijöitä ovat muun muassa raaka-aineiden hinnat ja työvoiman saatavuus. Monessa organisaatiossa tasapainotellaan saatavilla olevien resurssien, ihmisten ja rahan, riittämisessä niihin tarkoituksiin, jotka edistävät organisaation toimintaa. Resurssit tulee sitoa organisaation strategian mukaisesti siten, että investoinnista saatu hyöty on mahdollisimman korkea. (Vuorinen 2014, 222–224.)

Kansallisella tasolla on tiedostettu, että Suomessa on pula kyberturvallisuuden osaajista (Traficomin julkaisuja 2/2020, 36–37; Limnéll 2022; YLE 2022). Saadakseen palkattua osaavaa henkilökuntaa, organisaatioiden tarvitsee olla valmiita investoimaan rahaa tähän tarkoitukseen, sillä raha ohjaa osaavien työntekijöiden työpaikkavalintaa. Organisaation johdon tulisi tunnistaa ne resurssitarpeet, joita se tarvitsee nyt ja tulevaisuudessa, ja joko onnistua rekrytoimaan nämä henkilöt tai kouluttamaan organisaation sisältä sitoutuneen osaajan tehtävään. Haasteena palkkaamiseen saattaa olla se, että kyberturvallisuus ei toimiessaan tuota mitään organisaatiolle vaan on enemminkin kuluerä. Näin ollen ei ole välttämättä tarpeeksi dataa käytettävissä, jonka perusteella voisi päättää, millaisilla summilla kyberturvallisuuteen tulisi panostaa. (Traficomin julkaisuja 2/2020, 36–37; Limnéll 2022; YLE 2022.)

5.7.3 Sosiaalinen analyysi

Sosiaalisten tekijöiden ja muutosvoimien tunnistaminen auttaa organisaatioita ymmärtämään ja ennakoimaan asiakkaiden ja työntekijöiden tarpeita ja toiveita. Toimintaympäristöön vaikuttavia tekijöitä voivat olla esimerkiksi väestötieteelliset, terveydelliset ja sosiaaliset muutokset (Vuorinen 2014, 222). Esimerkiksi sosiaali- ja terveydenhuollon palveluiden käyttäjien määrän oletetaan kasvavan väestön ikääntyessä, jolloin toimintaympäristöanalyysissa tulisi ottaa huomioon sekä käyttäjien määrän kasvaminen, että myös ikääntyminen. Yhtenäisten ja yhdenarvoisten palveluiden saatavuuteen tulee panostaa. (Puro, 2010.)

IT-alalla ja kyberturvallisuuden osa-alueilla työvoimapula on tunnistettu ongelmaksi ja tilanteen ratkaiseminen on haastavaa (Lehto ym. 2017; Limnéll 2022; YLE 2022). Työvoimapula näkyy toiminnan hitautena ja työn tekeminen yksilöityy helposti henkilöihin, jolloin organisaation toimintaan kasaantuu riskejä. Sosiaalisen ja yhteiskunnallisen eriarvoisuuden kasvu tulee nähdä negatiivisena muutosvaikuttajana. On huomioitava, että kyberuhkia esiintyy myös organisaatiosta sisälähtöisesti. Tämän osoittavat monet tutkimukset. Esimerkiksi IBM:n (Lehto ym. 2017, 12) mukaan kyberhyökkäysten taustalla on 60 %:ssa tapauksista joku organisaation sisäpiirissä oleva henkilö. (Lehto ym. 2017, 12; Limnéll 2022.)

Organisaatioiden toimintaympäristöön voidaan vaikuttaa myös välillisesti. Sosiaalista mediaa voidaan pitää yhtenä hybridivaikuttamisen muotona, jolla voi olla organisaatioita hyödyttäviä tai uhkaavia muutosvoimia. Yhteiskunnan ja organisaatioiden toimintaan pyritään vaikuttamaan ennakoimattomilla tavoilla sekä valtiollisella että ei-valtiollisella tasolla. Trollaamisen ja disinformaation levittämisellä pyritään muokkaamaan kansalaisten mielipiteitä, mikä voi johtaa kyberhaasteiden lisääntymiseen. Tämän kaltainen yllättävä, monimuotoinen ja eri keinoin toteutettu hybridivaikuttaminen toimii usein laillisen ja laittoman rajamaastossa, jolloin siihen viranomaistasolla puuttuminen on haastavaa. (Kansallinen riskiarvio 2018 2019, 14–17.)

5.7.4 Teknologinen analyysi

Teknologinen kehitys on nostettu esiin muun muassa YK:n yleiskokouksessa yhtenä suurimpana kansainvälisenä megatrendinä. Teknologinen kehitys sekä ratkaisee muutoshaasteita että luo niitä. Teknologisella kehityksellä voidaan parantaa ihmisten elinoloja ja hillitä ilmastonmuutosta, mutta samalla teknologian nopea kehittyminen lisää ilmastovaikutuksia. Lisäksi lisääntyneet kyberhyökkäykset, tietomurrot- ja väärennökset ovat negatiivisia muutosvaikutuksia. Digitaaliset palvelut ovat Suomessa riippuvaisia kansainvälisistä yhteyksistä, palveluista ja palvelinkeskuksista, joten muutokset kansainvälisissä tietoliikenneyhteyksissä ja infrastruktuurissa vaikuttavat ja muokkaavat organisaatioiden toimintaympäristöä. Tietomurrot ja kybervaikuttaminen kohdistuvat kybersodankäynnissä korostetusti kriittiseen infrastruktuuriin, kuten tietoverkkoyhteyksiin ja sähkölaitoksiin. Myös teknologiariippuvainen sosiaali- ja terveydenhuolto kuuluvat kriittiseen infrastruktuuriin ja on erityisen altis haavoittuvuuksille. (Kansallinen riskiarvio 2018 2019, 17–18; Puustinen & Kekki 2020, 20–21, 51.)

Sosiaali- ja terveydenhuolto digitalisoituvat nopeaa vauhtia. Teknologiset innovaatiot vaikuttavat organisaatioiden kehitykseen ja markkinoihin (Vuorinen 2014, 222). Teknologinen kehitys tulee nähdä sekä mahdollisuutena että uhkana. Yhä useamman laitteen tiedot, esimerkiksi uniapnean hoitoon tarkoitetut CPAP-laitteiden keräämät tiedot (Käypä hoito -suositus 2022) tai diabeetikkojen verensokerinmittaustulokset (Terveyskylä 2022) päätyvät pilvipalveluihin, joista sosiaali- ja terveydenhuollon ammattilaiset voivat seurata ihmisten terveyteen liittyvää dataa. Tiedon määrä on valtava ja se on verkostoitunut. Tämä lisää mahdollisuuksia hoitaa ja auttaa ihmisiä, kun tietoa voidaan analysoida paremmin. Älyteknologia parantaa hoidon laatua. Samalla tulee ymmärtää, että riskit tiedon väärinkäyttöön, tietoturvarikkomuksiin ja kybervaikuttamiseen kasvavat. Sosiaali- ja terveydenhuollon tietojärjestelmiin kohdistettu kyberhyökkäys saattaisi aiheuttaa ihmishengen menetyksiä. (Kansallinen riskiarvio 2018 2019, 48–50.)

Teknologisten ratkaisujen lisääntyminen on lisännyt energian tarvetta ja sähkön häiriötön saatavuus on yhteiskunnalle ja organisaatioille välttämättömyys. Laajamittaiset sähkön saatavuusongelmat voivat vaarantaa kriittisten toimintojen ylläpidon (Kansallinen riskiarvio 2018 2019, 43–45). Suomen sähköverkosto on osa

yhteispohjoismaalaista järjestelmää ja eurooppalaista sähkömarkkinoita, joten sähkönsaantiin vaikuttaa kansallisten vaikuttimien lisäksi maailman poliittinen tilanne ja sääolot. Suorat siirtoyhteydet Suomen sähköverkoista on Ruotsiin, Viroon, Norjaan ja Venäjälle (Fingrid 2022). Suomi on riippuvainen Ruotsin ja Norjan tuontisähköstä. Suomesta viedään sähköä pääasiassa Viroon. EU:n asettamien pakotteiden vuoksi sähkö- ja kaasukauppa Venäjän kanssa keskeytettiin keväällä 2022. Tämä johti Euroopassa tilanteeseen, jossa energiaa ei ole saatavilla tarpeeksi kulutukseen verrattuna, vaan Euroopan täytyy sopeutua energian käytön vähentämiseen, sähkön korkeaan hintaan ja mahdollisiin sähkökatkoksiin (Tynkkynen, Hietaniemi, Haanperä & Hakko 2022).

5.7.5 Ekologinen analyysi

Ekologiset tekijät liittyvät ympäristön kunnioittamiseen, kestävään kehitykseen ja vihreisiin arvoihin. Tärkeimpänä arvona voidaan pitää organisaatioiden tiedostettua hiilijalanjäljen pienentämistä. Ympäristöön liittyvät aiheet koskettavat jokaista organisaatiota nyt ja tulevaisuudessa ja näin ollen on kaikkien etu, että ekologisiin muutosvaikuttimiin paneudutaan ja päätöksiä tehdään kestävän kehityksen periaatteella, vihreitä arvoja kunnioittaen. (Vuorinen 2014, 222.)

Ilmastonmuutos vahvistaa sään ääri-ilmiöitä ja luonnonkatastrofit vaikuttavat organisaatioiden toimintaan sekä suorasti että välillisesti. Kansainvälisten organisaatioiden kuten YK:n yleiskokouksen, YK:n sosiaalisen kehityksen tutkimuslaitoksen (UNRISD) ja Maailman talousfoorumin (WEF) raporteissa on ilmastonmuutos tunnistettu kaikkein suurimmaksi organisaatioiden haasteeksi. Ilmastonmuutoksen torjunnassa on epäonnistuttu, jolloin vaikutukset näkyvät energian ja resurssien vähyydessä. Tilanteeseen vaikuttaa teknologian nopea kehittyminen. Periaatteessa teknologian kehittyminen hillitsee ilmastonmuutosta, mutta teknologioiden kehittäminen kuluttaa runsaasti energiaa ja luonnonvaroja. Kilpailu tärkeistä raaka-aineista ja energiasta voi vaikuttaa organisaatioihin monilla eri tavoin. Ääri-ilmiöiden vaikutus on laajavaltaista, sillä se voi lisätä pakolaisuutta, taloudellisia haittoja, ääriliikkeitä ja hybridivaikuttamista esimerkiksi sosiaalisen median kautta. (Kansallinen riskiarvio 2018 2019, 18–21; Puustinen & Kekki 2020, 20–21.)

5.7.6 Lainsäädännöllinen analyysi

Lainsäädännölliset tekijät ohjaavat organisaatioiden toimintaa. Lait määrittelevät reunaehdot sille, mitä organisaatioin tulee tehdä ja mitä se ei saa tehdä. Organisaation on huolehdittava henkilöstönsä tietotaidosta lainsäädännöllisiin asioihin. Lainsäädäntö määritellään EU-tasolla tai kansallisessa lainsäädännössä. (Vuorinen 2014, 222.)

6 TUTKIMUKSEN TAUSTA

6.1 Toimeksiantaja

Oy Apotti Ab tuottaa maailman ensimmäistä sosiaali- ja terveydenhuollon yhteistä tieto- ja toiminnanohjausjärjestelmää Uudenmaan alueella sosiaali- ja terveydenhuollon organisaatioille. Yritys on perustettu vuonna 2015 ja sen tarkoituksena on kehittää toiminta-alueelle yhdenvertaiset sosiaali- ja terveydenhuollon palvelut sekä yhtenäistää toimintatapoja. Oy Apotti Ab:n palveluksessa työskentelee nykyisin noin 540 henkilöä muun muassa hallinnon, ICT:n, tukipalveluiden, koulutuksen ja sovelluskehityksen tehtävissä. Apotti-tietojärjestelmää käyttää noin 47 000 eli 77 % Uudellamaalla työskentelevistä sosiaali- ja terveydenhuollon ammattilaisista. Apotti-tietojärjestelmän vaikutuksen piiriin kuuluu noin 1,7 miljoonaa suomalaista. Tietojärjestelmään on integroitu 139 integraatiota, joiden avulla taataan tarvittavat sosiaali- ja terveydenhuollon palvelut ja tuotetaan järjestelmään lisäarvoa. Näitä palveluita ovat muun muassa Kanta-palvelut, Duodecim ja Raisoft. (Oy Apotti Ab 2022b; Oy Apotti Ab 2022c; Oy Apotti Ab 2022e.)

Apotti-tietojärjestelmän toimittaa yhdysvaltalainen Epic Systems Corporation, joka on vuonna 1979 perustettu tieto- ja toiminnanohjausohjelmistoa tuottava yritys. Yrityksen järjestelmiä käytetään useassa yhdysvaltalaisessa sairaalassa ja Euroopassa muun muassa Tanskassa, Norjassa, Hollannissa ja Sveitsissä. Epic Systems Corporation toimii vahvassa yhteistyössä Oy Apotti Ab:n johdon ja järjestelmänkehityksen tukena kehittämiskohteiden ja haasteiden tunnistamisessa ja ratkaisussa. (Epic 2020; Epic Systems Corporation 2022.)

Kansalaisille Oy Apotti Ab näyttäytyy näkyvimmin Maisa-asiakasportaalin välityksellä. Maisa yhdistää kansalaisille sosiaali- ja terveydenhuollon palvelut yhteen sähköisen asioinnin portaaliin. Maisan kautta kansalainen voi kommunikoida ammattihenkilöiden kanssa, ottaa yhteyttä sosiaalihuoltoon, pyytää reseptien uusimista tai tarkastella omia sosiaali- ja terveystietoja. Joulukuun 2022 alkuun mennessä aktiivisia Maisa-käyttäjiä oli lähes 930 000. Maisasta oli lähetetty yli 1,3 miljoonaa viestiä sosiaali- ja terveydenhuollon ammattilaisille, jätetty yli 100 000

sosiaalihuollon hakemusta ja toteutettu yli 21 000 videovastaanottoa etänä. (Oy Apotti Ab 2022d.)

Oy Apotti Ab:n tietoturvatiimin kokoa on viime vuosina kasvatettu ja sitä on tuotu lähemmäs organisaation hallinnollista johtoa, mikä kertoo siitä, että kyberturvallisuus on ymmärretty tärkeäksi osaksi organisaation liiketoimintaa. Koko organisaation laajuista kyberkulttuurin kehittymistä on edistetty ja tietoturvaa ja kyberturvallisuutta toteutetaan läpinäkyvästi. Tietoturvatiimi on panostanut siihen, että kyberturvallisuudesta on tullut osa jokaisen työntekijän arkea. Tietoturvatiimi viestii henkilökunnalle aktiivisesti monia eri kanavia käyttäen. Esimerkiksi Apotin podcastissa (2022) keskusteltiin kyberturvallisuudesta, varautumisesta ja arkisista teoista, jotka parantavat sekä organisaation että henkilön kyberturvallisuutta. Kyberturvallisuutta ei toteuteta Oy Apotti Ab:ssa täysin itsenäisesti, vaan tiettyjä tietotaitoja ja palveluita on todettu olevan parempi ostaa ulkoisilta palveluntarjoajilta. Näiden tahojen kanssa tehdään tiivistä yhteistyötä.

Oy Apotti Ab:n asema kriittisessä infrastruktuurissa on tunnistettu. Organisaatio oli osallisena TIETO2022-harjoituksessa (Oy Apotti Ab 2022a), jossa harjoiteltiin monien suurien, kriittiselle infrastruktuurille tärkeiden ja yhteiskunnan toimivuuden kannalta oleellisten, organisaatioiden ja eri viranomaisten, kuten Kyberturvallisuuskeskuksen, Puolustusvoimien ja poliisin välistä yhteistyötoimintaa laajojen kyberhäiriöiden varalta. Valmiusharjoituksen tarkoituksena oli tukea organisaatioiden jatkuvuuden hallintaa, varautumista ja yhteistyötä. (Huoltovarmuuskeskus 2021.) Oy Apotti Ab:n tavoitteena on jatkaa edelleen tiivistä yhteistyötä kyberturvallisuuteen liittyen muiden organisaatioiden ja tahojen kanssa.

6.2 Tutkimuksen tausta ja nykytilanne

Oy Apotti Ab:ssa toteutettiin kyberturvallisuuden kypsyysarviointi vuonna 2021. Arvioinnissa saadut tulokset olivat hyvällä tasolla, mutta tästä huolimatta organisaatiossa nähtiin tarpeelliseksi nostaa tavoitetasoa johtuen organisaation toiminnan luonteesta ja kansallisesta merkityksestä. Saatujen arvioiden perusteella määriteltiin kehitysohjelma, joka pitää sisällään monia kyberturvallisuuteen ja tietoturvaan liittyviä kokonaisuuksia.

Yhtenä kehittämiskohteena nostettiin tarve saada toteutettua kyberturvallisuuden toimintaympäristön analyysi, jonka avulla voitaisiin tunnistaa ja tarkastella niitä Oy Apotti Ab:n kyberturvallisuuden toimintaympäristöön vaikuttavia muutosvoimia, joihin organisaatiossa tulisi reagoida. Tällä hetkellä toimintaympäristöanalyysia toteutetaan organisaation johdon tasolla, mutta se ei havaintojen mukaan tuota tarpeeksi käytännönläheistä tietoa mahdollisista toimintaympäristön muutoksista ja muutoksiin tarvittavista toimenpiteistä kyberturvallisuuden osalta.

6.3 Tutkimuksen tarkoitus, tavoitteet ja tutkimuskysymykset

Tutkimuksen tarkoituksena on löytää vastaus Oy Apotti Ab:n kohtaamaan haasteeseen, jonka mukaan kyberturvallisuuden toimintaympäristön kokonaiskuvan luomiseen ja varsinkin siihen kohdistuvien muutosvoimien tunnistamiseen ei ole sopivaa analyysityökalua. Tutkimuksessa haetaan vastausta kysymyksiin:

- Mitä kyberturvallisuuden toimintaympäristön muutosvoimia kohdistuu Oy Apotti Ab:hen?
- Millaiset PESTEL-analyysin kysymykset ohjaavat löytämään Oy Apotti Ab:n kyberturvallisuuteen vaikuttavat muutosvoimat?

Kysymyksiin etsitään vastausta PESTEL-analyysin perusteella. Sama kysymys esitetään poliittisesta, ekonomisesta, sosiaalisesta, teknologisesta, ekologisesta ja lainsäädännöllisestä näkökulmasta.

Opinnäytetyön tavoitteena on haastattelujen, kirjallisuuskatsauksen ja kansallisten ohjeistuksien perusteella löytää analyysityökaluun kysymykset, joiden avulla pystyttäisiin tunnistamaan tärkeimmät Oy Apotti Ab:sta riippumattomat kyberturvallisuuden toimintaympäristöön vaikuttavat muutosvoimat- ja ajurit. PESTEL-analyysin avulla pystytään tuottamaan tietoa niistä muuttuvista tekijöistä, jotka Oy Apotti Ab:ssa tulee huomioida. PESTEL-analyysia voidaan toteuttaa sekä strategisella, taktisella että operatiivisella tasolla. Opinnäytetyön tuloksista on hyötyä Oy Apotti Ab:n liiketoiminnan kehittämiselle ja johtamiselle kyberturvallisuuden näkökulmasta.

Opinnäytetyössä rakennetun PESTEL-analyysityökalun kysymyksien perusteella toteutettua analyysia tulisi toteuttaa Oy Apotti Ab:n eri yksiköissä vähintään kerran vuodessa, jotta saadaan luotua ajantasainen koko organisaation kattava kyberturvallisuuden toimintaympäristön tilannekuva. Analyysin avulla organisaation eri yksiköiden olisi tarkoitus löytää oman yksikön näkökulmasta oleelliset muutosvaikuttimet, joihin tulee kiinnittää huomiota ja kohdistaa toimenpiteitä. Toimintaympäristöanalyysin on tarkoitus toimia pohjana, kun suunnitellaan resursseja, kustannustehokkuutta, rahoitusta, aikataulutusta ja toimintasuunnitelmaa.

7 TUTKIMUSMENETELMÄ JA TOTEUTUS

7.1 Laadullinen tutkimusmenetelmä

Tutkimusmenetelmät jaotellaan tyypillisesti määrälliseen eli kvantitatiiviseen ja laadulliseen eli kvalitatiiviseen tutkimukseen. Tutkimusmenetelmiä voi myös yhdistellä tarvittaessa. Laadullisella tutkimuksella tarkoitetaan menetelmää, jossa tietoa kerätään ilman tilastollisia tai määrällisiä menetelmiä. Tiedon määrän sijasta painoarvo on tiedon laadussa. Laadullisen tutkimuksen etuna on joustavuus tiedonkeruussa. Haastateltavaa voi pyytää täydentämään tai tarkentamaan vastaustaan. Laadullinen tutkimus pyrkii selvittämään sanallisesti vastaukset tutkimuskysymyksiin haastattelujen, kyselyjen, dokumenttien ja muiden havainnointikeinojen perusteella. Laadullinen tutkimusmenetelmä soveltuu tilanteisiin, joissa pyritään ilmiöiden syvälliseen kuvaamiseen ja ymmärtämiseen. (Kananen 2017, 34–35; Tuomi & Sarajärvi 2018, 82–85.)

Laadullisen tutkimusmenetelmän keinoja ovat muun muassa erilaiset haastattelut. Haastattelutyyppejä ovat lomake-, teema- ja syvähaastattelut. Lomakehaastattelussa eli strukturoidussa haastattelussa kysymykset ovat valmiita ja vastauksille annetaan vaihtoehtoja. Teemahaastattelussa eli puolistrukturoidussa haastattelussa on ennalta valitut teemat, joiden perusteella haastattelu etenee. Haastattelua voi syventää lisäkysymyksin haastattelun aikana. Syvähaastattelussa eli strukturoimattomassa haastattelussa käytetään avoimia kysymyksiä, joihin pyritään saada vastaukset. (Tuomi & Sarajärvi 2018, 83–88.)

7.2 Menetelmällinen toteutus

Tämän opinnäytetyön menetelmäksi valikoitui laadullinen tutkimus, joka toteutettiin teemahaastatteluina. Haastattelut etenivät ennalta valittujen aihepiirien varassa, mutta haastattelutilanteessa oli kuitenkin mahdollisuus tehdä täsmentäviä kysymyksiä riippuen haastateltavan vastauksesta. Terminä kyberturvallisuus ei ole yksiselitteinen, vaan usein haastatteluun annettava vastaus on sanallisesti sidottava tiettyyn työtehtävään tai kokonaisuuteen. Tutkimuksessa haluttiinkin korostaa eri puolella organisaatiota työskentelevien ihmisten näkemystä ja kokemusta kyberturvallisuudesta mahdollisimman laaja-alaisesti.

Teemahaastatteluissa tärkeässä osassa on haastateltavien omakohtainen tulkinta haastateltavista asioista, jolloin kysymyksiä ja niiden järjestyksiä voi vaihdella vapaasti (Hirsjärvi & Hurme 2008, 48).

Tiedonkeruussa tukeuduttiin harkinnanvaraiseen näytteeseen (purposive sampling*)* (Cohen, Manion & Morrison 2003, 102). Haastateltaviksi valittiin seitsemän Oy Apotti Ab:n työntekijää, jotka ovat avainasemassa organisaation kyberturvallisuuden ylläpidossa ja kehittämisessä. Haastateltavat työskentelevät kukin oman työtehtävänsä mukaisesti ja näin ollen haastattelemalla eri yksiköiden henkilökuntaa, saadaan laaja käsitys siitä, miten organisaation kyberturvallisuuden toimintaympäristö näyttäytyy organisaation eri osa-alueilla. Teemahaastattelun toteutuksen osalta tukeuduttiin Hirsjärven & Hurmeen (2008) teokseen.

Opinnäytetyössä käytettyjen tietolähteiden perusteella opinnäytetyöhön kirjattiin ne löydökset, joihin Oy Apotti Ab:n tulisi kiinnittää huomiota kyberturvallisuuden osalta. Löydöksiin perustuen rakennettiin PESTEL-analyysityökalun kysymykset, joiden perusteella organisaation eri yksiköt voivat havainnoida ja ennakoida kyberturvallisuuden toimintaympäristön muutosvoimia. Tämä on opinnäytetyön lopputuote.

7.3 Tutkimuksen toteutus

Haastattelut, seitsemän kappaletta, toteutettiin marraskuussa 2022. Haastatteluissa noudatettiin hyviä tutkimuskäytänteitä kertomalla avoimesti haastateltaville, miten heidän haastattelujaan tullaan tutkimuksessa käyttämään hyväksi. Haastateltaville kerrottiin haastattelujen ja litterointien tallennuspaikan olevan Oy Apotti Ab:n omistamissa tiedostoissa ja että niihin ei pääse käsiksi kukaan muu kuin haastattelija ja että tiedostot tullaan tuhoamaan heti opinnäytetyön julkaisun jälkeen. Haastateltavat osallistuivat haastatteluihin vapaaehtoisesti ja he saattoivat lopettaa haastattelun, jos kokivat sen tarpeelliseksi. Kaikki haastattelut toteutettiin kuitenkin suunnitelman mukaisesti.

Teemahaastattelun runkona käytettiin PESTEL-analyysin mukaista aiheen käsittelyjärjestystä, jolloin ensin keskityttiin poliittisiin vaikuttimiin ja tämän jälkeen ekonomisiin, sosiaalisiin ja sosiaalikulttuurillisiin, teknologisiin, ekologisiin eli

ympäristöön liittyviin tekijöihin ja lopulta lainsäädännöllisiin asioihin. Haastatteluihin oli varattu aikaa 45 minuuttia, mutta kestossa joustettiin tarvittaessa. Toteutuneiden haastattelujen kesto vaihteli 35–50 minuutin välillä.

Haastattelut toteutettiin haastateltavan kanssa sovittuna aikana Teams-kokouksena Oy Apotti Ab:n verkossa. Toteutustavalla saatiin joustavuutta aikatauluihin ja haastattelut saatettiin toteuttaa paikasta riippumattomasti. Haastattelut litteroitiin ja litteroitua aineistoa kertyi yhteensä 42 sivua. Toteuttamistavan vuoksi tallenteet sekä litterointi pystyttiin säilyttämään koko tutkimuksen ajan Oy Apotti Ab:n hallitsemissa tiedostoissa.

7.4 Eettiset lähtökohdat

Tutkimuksessa noudatettiin tutkimuseettisen neuvottelukunnan (TENK) ohjeita hyvästä tieteellisestä käytännöstä. Tutkimuksessa sovellettiin tieteellisen tutkimuksen kriteerien mukaisia ja eettisesti kestäviä tiedonhankinta-, tutkimus- ja arviointimenetelmiä. Opinnäytetyössä julkaisuihin on viitattu asianmukaisella tavalla, jolloin toisten tutkijoiden saavutuksille on annettu niille kuuluva arvo ja merkitys.

Keskeinen eettinen kysymys oli tutkimukseen osallistuvien yksityisyyden ja intressien suojelu. Yksittäisen vastaajan anonymiteetti ei saa paljastua loppuraportista eikä mahdollisissa suorissa lainauksissa (Eskola & Suoranta 2001, 56–57; Cohen, Manion & Morrison 2003, 61–67). Ennen haastattelujen alkua haastateltavia informoitiin tutkimuksen tarkoituksesta ja siitä, miten heidän antamiaan vastauksia käsitellään (informed consent). Jokaiselle haastateltavalle kerrottiin sanallisesti ja kirjallisesti se, mihin tarkoitukseen haastattelussa saatua tietoa käytetään, mihin tieto tallennetaan ja että tietoa käytettäisiin vain ja ainoastaan tämän opinnäytetyön tekemiseen. Haastattelut tai litteroinnit eivät poistuneet organisaation hallinnoimilta fyysisiltä laitteilta ja tiedostoista, ja tieto tullaan tuhoamaan opinnäytetyön valmistuttua. Haastatteluihin osallistuminen oli vapaaehtoista.

Haastateltavien joukko oli heterogeeninen ja suurinta osaa työnimikkeistä on organisaatiossa vain yksi kappale, joten henkilöiden yksityisyyden turvaamiseksi

tässä opinnäytetyössä ei paljasteta haastateltavista mitään tunnistetietoja. Tämä lisää haastattelujen luotettavuutta ja eettisyyttä, kun haastateltava saattoi luottaa siihen, ettei mitään hänen sanomaansa voida yhdistää yksittäiseen työntekijään, jolloin haastattelussa uskallettiin puhua avoimemmin myös haastavista aiheista. Kun tutkimusta tehtiin yrityksen sisällä, oli tärkeä mainita myös se, että mitään yrityssalaisuuksia tai yrityksen turvallisuutta vaarantavia tietoja ei tulla kirjaamaan opinnäytetyöhön, vaikka tällaisia asioita haastatteluissa nousisi esiin.

8 TUTKIMUSTULOKSET

Aineiston analyysissä tukeuduttiin induktiiviseen sisällönanalyysiin (Mayring 2022). Muita analyysin tukena käytettyjä menetelmäteoksia olivat erityisesti lähdeluettelossa mainitut Berg (2007), Cohen, Manion & Morrison (2003), Denzin & Yvonne (2000), Eskola & Suoranta (2001), Tuomi (2013) sekä Silvermanin kaksi teosta (2002; 2005). Analyysissa keskityttiin teemoittelemalla löytämään litteroidusta aineistoista esiin nousseita tärkeitä kokonaisuuksia ja tarkasteltiin niitä tutkimusongelman näkökulmasta huolellisesti jokaisen haastattelun osalta. Teemoittelua toteutettiin PESTEL-rungon mukaisesti. Analyysissa otettiin huomioon se, että kaikissa haastatteluissa vastaukset eivät noudattaneet täysin haastattelun runkoa, vaan välikommentteina on saattanut nousta esiin asioita, joita haluttiin vielä nostaa esiin haastattelun aikaisempaan vaiheeseen. Litteroituja haastatteluja tarkasteltiin siis ennakkoluulottomasti ja ne pyrittiin analyysissa sijoittamaan PESTEL-runkoon.

Teemahaastatteluissa esiin nousseet toimintaympäristöön vaikuttavat tekijät on koostettu kunkin otsakkeen alle. Haastattelujen aikana haastattelija kiinnitti huomiota siihen, että samoja aiheita nousi esiin haastatteluissa useassa eri vaiheessa. Näin ollen samoja aiheita myös analysoitiin aineistossa useamman kerran. Haastattelija totesi tämän olevan tärkeää, sillä useassa aiheessa oli monta eri katsontakantaa, jotka tulee ottaa huomioon kyberturvallisuuden toimintaympäristön analyysia tehdessä.

8.1 Poliittiset muutostekijät

Haastateltavat totesivat, että Oy Apotti Ab:ssa toteutettavan politiikan reunaehdot rakentuvat maailman politiikasta, Suomen sisäisistä poliittista päätöksistä, asiakkaiden ja järjestelmätoimittajan vaatimuksista sekä lainsäädännön ja EU direktiivien vaatimuksista. Näissä tahoissa tapahtuvat muutokset toimivat Oy Apotti Ab:ssa joko suoraan tai välillisesti muutosvoimina.

Maailman poliittisen tilanteen muutokset vaikuttavat varsinkin kriittisen infrastruktuurin organisaatioihin, joihin Oy Apotti Ab luetaan kuuluvaksi. Suojelupoliisi ja

Kyberturvallisuuskeskus ovat varoittaneet kohonneesta kyberuhkien riskistä ja kehottaneet organisaatioita varautumaan mahdollisiin vaikutusyrityksiin. Haastateltavat nostivat esiin Suomen tämän hetken suurimpina geopoliittisina vaikuttajina olevan Venäjän läheisyys, Ukrainassa käytävä sota ja Nato-prosessi. Oy Apotti Ab:n tuleekin seurata maailmalla tapahtuvia muutoksia, sillä ne toimivat suoraan ja välillisesti organisaation toimintaympäristön muutosvoimina.

Myös Suomen sisäpolitiikan muutokset toimivat muutosajureina Oy Apotti Ab:ssa. Vuonna 2023 pidettävät eduskuntavaalit tuottavat uuden hallituksen, jonka tekemät päätökset vaikuttavat suoraan ja välillisesti Oy Apotti Ab:n toimintaan. Useampi haastateltava nosti esiin myös julkisen asenteen Oy Apotti Ab:ta ja varsinkin sen tuottamaa tietojärjestelmää kohtaan. Tämän vaikutusta kyberturvallisuuteen ei tule ohittaa.

Lähes kaikki haastateltavat nostivat esimerkkinä poliittiseksi vaikuttavaksi tekijäksi marraskuussa 2021 muuttuneen asiakastietolain, jonka vaatimuksen perusteella Oy Apotti Ab:n tuli määritellä tietoturvasuunnitelma. Dokumentin olemassaolo parantaa organisaation kyberturvallisuutta, mutta dokumentin laatiminen vaati huomattavan määrän tietoturvatiimin resursseja varsinkin, kun sen valmistumiseen kohdistui kova aikapaine. Positiivisena ja kyberturvallisuutta parantavana tekijänä on kuitenkin nähty se, että THL ja Valvira ovat ohjeistaneet esimerkkidokumentaatiolla, miten lakia tulee tulkita eli mitä suunnitelman pitää sisältää. Lakimuutosten trendinä on huomattu olevan vastuiden määrittely ja dokumentaation lisääminen. Haastateltavat summasivat, että olisi tärkeää, että organisaation toimintatapaa muokattaisiin siihen suuntaan, että yhä useampi vaatimus olisi täytetty jo ennen, kun se on lain mukaan pakko.

Euroopan Unionin direktiiveistä mainittiin erikseen CER (Critical Entities Resilience Directive), eli yhteiskunnan toiminnan kannalta kriittisten palveluiden resilienssin parantamiseen tähtäävä direktiivi sekä NIS2-direktiivi, jonka on tarkoitus tulla voimaan vuonna 2024. Nämä kyberturvallisuuteen ja tietoturvallisuuteen suoraan liittyvät direktiivit ohjaavat Oy Apotti Ab:n toimintaa. Direktiivit ovat organisaatioita velvoittavia määräyksiä.

Edellä mainittujen lain vaatimien ja velvoittavien poliittisten vaikuttimien lisäksi haastateltavat nostivat esiin muutosvoimina asiakkaiden asettamat vaatimukset ja sopimukset. Eräässä haastattelussa mainittiin asiakasorganisaation halu Oy Apotti Ab:n ISO 27001 -sertifioinnille. ISO 27001 -standardi vaatii runsaasti dokumentaatiota, jonka lisäksi dokumentoitu toiminta tulee olla jalkautettuna koko henkilöstön toimintatapoihin. Se siis on iso ponnistus toteuttaa. Useammat haastateltavat nostivat kuitenkin esille standardin positiivisen vaikutuksen kyberturvallisuuteen, sillä sen perusteella organisaatio voi osoittaa noudattavansa tietyntasoista tietoturvapolitiikkaa. Standardien sisältämiä vaatimuksia päivitetään tietyin väliajoin, joten nekin toimivat muutosvoimina, jotka tulee toimintaympäristöanalyysissa ottaa huomioon.

Haastatteluissa nousi esille epätietoisuus tulevasta hyvinvointialuemuutoksesta, jolla nähtiin olevan suuri vaikutus Oy Apotti Ab:n toimintaan. Esimerkkinä hyvinvointialueiden aloittamisen tuomasta haasteesta kyberturvallisuuden näkökulmasta haastatteluissa mainittiin Oy Apotti Ab:n tietoturvafoorumi, jossa asiakkaat ja Oy Apotti Ab kehittävät yhteistyössä laadukkaampaa tietoturvaa. Tätä väylää pidetään sekä asiakkaan että Oy Apotti Ab:n puolesta tärkeänä tietoväylänä tiedonjakamiseen ja yhteisten pelisääntöjen luomiseen. Vuoden 2022 viimeisimmässä kokouksessa asiakkaan edustajat ilmoittivat kokouksen olevan viimeisin heille, eikä kenelläkään ollut vielä tietoa siitä, miten yhteistyötä tulevien hyvinvointialueiden ja Oy Apotti Ab:n kanssa tultaisiin vuodenvaihteen jälkeen toteuttamaan.

Haastatteluissa korostui tarve tiiviistä yhteistyöstä asiakkaiden ja muiden sidosryhmien kanssa. Sosiaali- ja terveydenhuollon tietojärjestelmät ja niihin liittyvät muut ohjelmat ja palvelut luovat laajan ja monimutkaisen verkostoituneen maailman, joka on rikollisuudelle altis arkaluontoisten tietojen vuoksi. Oy Apotti Ab voi vaikuttaa vain oman organisaation tekemiseen ja tämän vuoksi haastatteluissa todettiin olevan elintärkeää, että organisaatioiden välillä on laadukas ja tiivis yhteistyö, jolloin voidaan yhdessä kehittää ja ylläpitää kokonaisturvallisuutta, jatkuvuutta, tilanteisiin varautumista ja mahdollisissa häiriötilanteissa tilanteista toipumista. Useampi haastateltava korosti sitä, että suunnitelmat ja prosessit tulee olla dokumentoituna ajatuksella, kun jotain jossain vaiheessa sattuu. Ei tule

tuudittautua ajatukseen, että kyberturvallisuus olisi koskaan täysin pitävä. Kyberturvallisuutta tulee kehittää organisaatiossa jatkuvasti ja varautua kaikkein huonoimpiin kuviteltaviin tapahtumaketjuihin.

Asiakkaiden kanssa toteutettavan yhteistyön lisäksi haastatteluissa painotettiin organisaation sisäisen yhteistyön tärkeyttä. Oy Apotti Ab:n tuottaman tietojärjestelmän toimittajana toimii yhdysvaltalainen Epic, jonka kanssa tehty sopimus luo omia kyberturvallisuuteen liittyviä muutosvoimia. Monet Oy Apotti Ab:lle osoitetuista vaatimuksista on pohjimmiltaan tietosuojavaatimuksia, jolloin niitä käsittelevät tietosuojatiimi ja juristit. Kuitenkin osa näistä vaatimuksista toteutetaan tietoturvakontrollien keinoin, kuten salauskäytännöt ja tiedon tallentamiseen liittyvät muutokset. Tiettyjä tietoturvaan liittyviä haasteita, kuten esimerkiksi kieltopotilaisiin, eli ihmisiin, jotka ovat kieltäneet potilastietojen luovuttamisen rekisterirajan yli, liittyviä asioita ratkotaan sovelluskehityksen kanssa yhteistyössä. Kyberturvallisuuden kehittäminen on siis osaltaan laaja-alaista verkostoitumista. Eräs haastateltava totesikin, että Oy Apotti Ab:n kyberturvallisuuspolitiikka on toimiva vasta siinä vaiheessa, kun se on onnistuttu jalkauttamaan koko organisaation tietoisuuteen ja toimintatapoihin.

Haastatteluissa nousi korostuneesti eri haastattelun vaiheissa prosessikuvausten ja tietämyksenhallinnan parantaminen ja sitä kautta hiljaisen tiedon ja ihmisriippuvuuksien vähentäminen. Lainsäädäntö ohjaa organisaatioita kohti prosessikuvausten laadukkaampaa dokumentaatiota, mutta muutama haastateltava mainitsi lainsäädännön muutosten hitauden eikä Oy Apotti Ab:ssa pitäisi tuudittautua tekemään vain sitä mitä on pakko, vaan kyberturvallisuuden pitäisi olla sisälähtöistä jatkuvaa kehittämistä ja toiminnan parantamista.

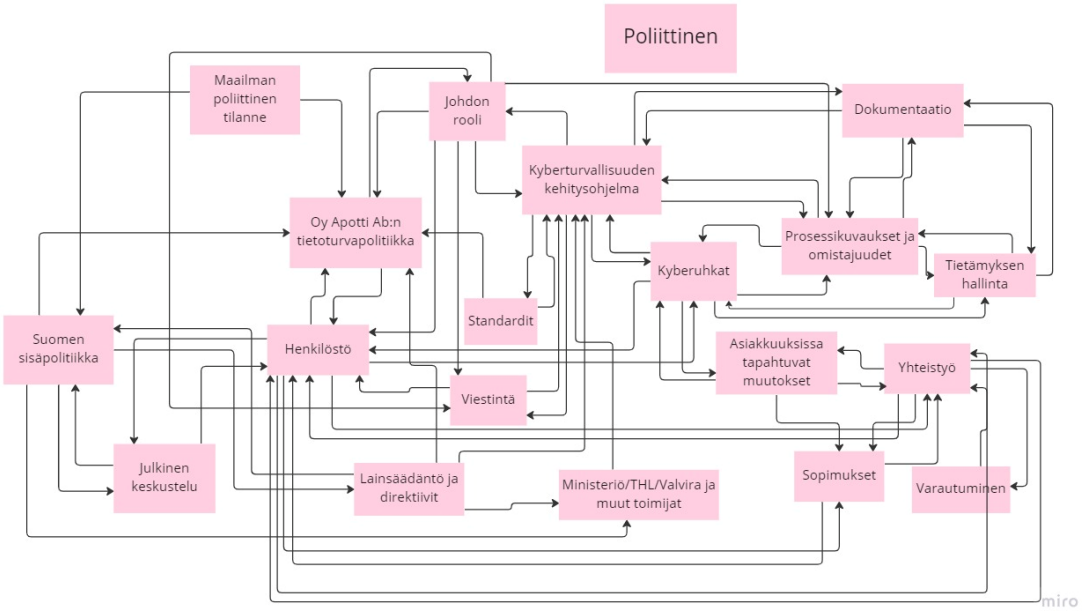
Kyberturvallisuuden laadun ja riskienhallinnan parantamiseksi prosessikuvausten ja ohjeiden kehittämiseen tulisi panostaa. Dokumentaation tulisi olla selkeästi toteutettua, säilöttyä ja versiohallittua. Haastateltavat olivat itse joutuneet useamman kerran siihen tilanteeseen, että aikaisemmin tehtyjen dokumenttien löytyminen tai niiden sisällön ajantasaisuuden varmistaminen olivat vieneet aivan turhan paljon aikaa. Tähän toivottiin selkeää parannusta, jotta voitaisiin todeta, että riskienhallinnan näkökulmasta olisi varauduttu päivittäisellä toiminnalla siihen, että

tarvittavat prosessikuvaukset on kirjattu, kaikki dokumentaatio on varmasti ajan tasalla ja löydettävissä ennalta sovitusta paikasta, ihmisriippuvuudet on minimoitu ja kyberturvallisuutta kyetään johtamaan tiedolla. Tämän pohjatyön kehittäminen ja ylläpitäminen nähtiin yhdeksi tärkeimmäksi tekijäksi, mihin kyberturvallisuudessa pitäisi Oy Apotti Ab:ssa kiinnittää huomiota.

Haastatteluissa otettiin kantaa myös kyberturvallisuuteen toimintona, joka voidaan nähdä kyberturvakulttuurin ja -politiikan kehityksen haasteena. Ongelma kyberturvallisuudessa on se, että toimiessaan se ei tuota organisaatiolle mitään, vaan se nähdään ainoastaan kulueränä. On haastava yrittää osoittaa se, mitä kyberturvallisuudella ja sen kehittämisellä taloudellisesti säästetään. Toisaalta, jos ongelmia ilmaantuu, niin rahalliset ja mainetappiot voivat johtaa jopa koko toiminnan loppumiseen. Oy Apotti Ab:ssa tietoturvatiimi sijaitsee hallinnollisesti lähellä johtoa. Tämä nähtiin haastatteluissa hyvänä politiikkana, sillä se näyttää olevan osoitus siitä, että kyberturvallisuuden tarkoitus on ymmärretty ja siihen kohdistuvaa työtä arvostetaan.

Organisaation johdon asemaa kyberturvallisuuspolitiikassa ja -kulttuurissa korostettiin. Ilman johdon selkeää viestiä kyberturvallisuuden tärkeydestä, ei pysyviä muutoksia saada aikaan. Kyberpolitiikan tulee ulottua johdolta aina tiimeille ja yksittäisille työntekijöille asti ollakseen toimiva. Vuonna 2021 Oy Apotti Ab:ssa suoritettiin kyberturvallisuuden kypsyystason mittaus ja sen perusteella luotiin uusi kyberturvallisuuden kehittämisohjelma. Tällainen johdolta suoraan tuleva viesti on tärkeässä roolissa kyberturvallisuuden kehittämisessä Oy Apotti Ab:ssa. Muutamassa haastattelussa kuitenkin nostettiin esille se, että johdon kyberturvallisuustietoudessa ja päätöksenteossa on vielä kehitettävää. Organisaation johto ei välttämättä ole niin perillä kyberturvallisuudesta, mitä haastateltavat toivoivat. Toisaalta tähän korjausehdotukseksi esitettiin sitä, että tulisi pohtia, minkälaista tietoutta johtoryhmälle tulee nostaa. Tulee pohtia, riittäisikö organisaation johdolle vain tieto tietoturvapolitiikkaan tehdyistä muutoksista, jolloin johtoryhmä saisi vain sen tiedon korostetusti, millä koetaan olevan suurin muutosvoima ja merkitys organisaation toiminnalle.

Eräässä haastattelussa mainittiin, että laadukas ja tarpeeksi usein toteutettu kyberturvallisuuden toimintaympäristöanalyysi on tärkeässä osassa kyberturvallisuuden parantamisessa. Muutama haastateltava mainitsi, että toimintaympäristöanalyysi tulisi tuottaa toiminnan tasolla, jossa tarkasteltaisiin niitä muuttuvia tekijöitä, jotka konkreettisesti tulee ottaa huomioon kyberturvallisuuden kehittämisessä. Toimintaympäristöanalyysin tekeminen vaikuttaa kustannustehokkuuden parantumiseen, laadukkaan toimintasuunnitelman tekemiseen, resurssoinnin suunnitteluun, aikataulutukseen ja budjettiin. Toimintaympäristöanalyysi siis nähtiin strategisen johtamisen pohjana, jonka perusteella kyberturvallisuutta tulisi Oy Apotti Ab:ssa toteuttaa. Poliittisen analyysin keskeisiä muuttujia ja niiden välisiä yhteyksiä on esitetty koosteena kuviossa 7.



Kuvio 7. Poliittisen analyysin muutostekijät ja vaikutussuhteet

8.2 Ekonomiset muutostekijät

Haastatteluissa vastaus teemaan oli yksinkertaistettuna, että taloudellisen toimintaympäristön kulmakivet ovat raha ja käytettävät resurssit. Oy Apotti Ab ei noudata täysin perinteisen liiketoimintalaitoksen toimintaperiaatteita, sillä sen omistavat asiakkaat, jolloin myös organisaation rahoituksesta vastaavat asiakkaat. Hyvinvointialueiden lopulliset budjetit eivät haastattelujen aikaan olleet vielä selvillä, mutta hyvinvointialueiden on uutisoitu olevan säästöjen tarpeessa, joten tämän voidaan olettaa heijastuvan myös Oy Apotti Ab:n rahoitukseen. Asiakkaiden

rahoituksen lisäksi muutostekijänä on yhteiskunnan antama panostus kyberturvallisuuden kehittämiseen organisaatioissa, eli mitä tukia valtiolta on haettavissa ja saatavissa.

Haastatteluissa todettiin, että toimiva kyberturvallisuus luo puitteet toiminnalle ja tuottavuudelle. Organisaation kyberturvallisuuteen varatun rahoituksen perusteella tulee määritellä rahoituksen viitekehys, joka ohjaa tekemistä. Haastatteluissa korostettiin rahan ja tekemisen välisen tasapainon löytämistä. Tulee ymmärtää syy-seuraussuhteet eli miten jonkun tietyn asian tekemättä jättäminen vaikuttaa kokonaiskuvaan ja kyberturvallisuuteen. Minimissään rahoituksen tulisi riittää perusasioiden ylläpitämiseen, mutta kyberuhkien kehittyessä tulisi myös kybersuojautumista kyetä kehittämään. Jos kyberturvallisuuteen muodostuu selkeitä puutteita tai organisaatioon kohdistuu mahdollisia iskuja, saattaa rahallinen ja mainehaitta olla huomattavat. Haasteena koettiin se, että kyberturvallisuus itsessään ei tuota yritykselle mitään, vaan toimii ainoastaan kulueränä. Tämän vuoksi toimintaympäristöanalyysia tehdessä tulisi olla selkeästi tiedossa ja määriteltynä organisaatiolle kaikkein kriittisimmät toimet, tiedot ja järjestelmät, joiden suojaamiseen pitää ja kannattaa panostaa. Eräs haastateltava kiteytti sanoman, että on hyvä ymmärtää, että ihan kaikkea ei edes kannata suojata ”kaikkein kovimmilla tykeillä”.

Osa haastateltavista teki tiivistä yhteistyötä asiakkaiden kanssa hankintoihin liittyen ja he totesivat, että raha ohjaa vahvasti toimintaa. Asiakasrajapinnassa pyritään löytämään hyvät ja oikeat ratkaisut toiminnan kehittämiselle. Hankintoja tehdessä korostetaan jatkuvuutta, jolloin hankintoja tulee tarkastella pitkäjänteisesti. Täytyy arvioida, tehdäänkö hankintaan liittyvää suunnitelmaa vuoden, kahden vai kymmenen mittaiselle ajanjaksolle, ja mitä päätöksen tekeminen tarkoittaa organisaatiolle nyt ja tulevaisuudessa. Kokonaisuudessaan kyberturvallisuustoimintaa ohjaa syy-seuraussuhteiden ymmärtäminen ja analysointi. Palveluiden ja tuotteiden elinkaari tulee ottaa huomioon, kun mietitään ratkaisun kokonaiskustannusta. Useampi haastateltavista totesi, että tällä hetkellä halvin ratkaisu saattaa loppupeleissä olla huomattavasti hinnakkaampi vaihtoehto kokonaiskustannukseltaan, mutta päätöshetkellä kalliimman ratkaisun tekemiseen

täytyy löytyä hyvät perustelut. Oy Apotti Ab:n tekemät ratkaisut nähtiin pääsääntöisesti hyvinä ja tietoturvallisuutta päätöksiä tehdessä arvostettiin.

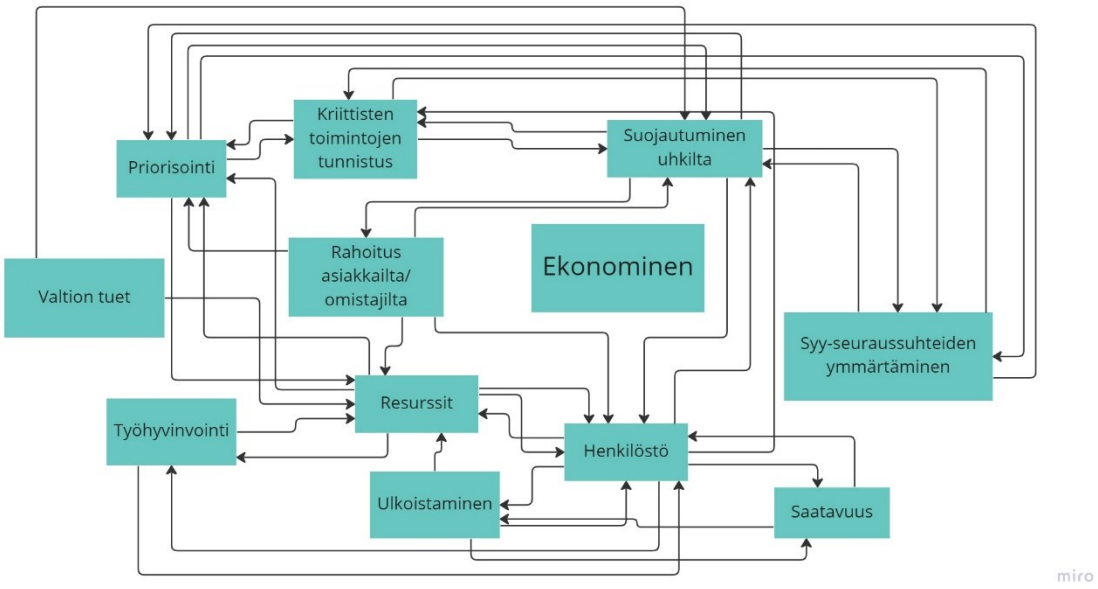
Haastateltavat nostivat esiin yhtenä muutosvoimana tietotaidon hankinnan organisaation käyttöön. Taloudellisesta näkökulmasta tulee pohtia sitä, mitä tietotaitoa kannattaa ostaa talon sisälle, milloin kannattaa käyttää resursseja oman henkilöstön kouluttamiseen, ja mitkä palvelut ovat järkevintä ulkoistaa. Haastatteluja tehdessä Oy Apotti Ab:lla oli käynnissä kilpailutukset esimerkiksi SOC:sta (Security Operation Centre), joka on tunnistettu sellaiseksi palveluksi, joka ainakin toistaiseksi hankitaan ulkopuoliselta tarjoajalta. Myös muita kyberturvallisuuteen liittyviä palveluita on ulkoistettu. Näiden sopimusten uusiminen ja kilpailuttaminen ovat luonnollisia muuttuvia tekijöitä organisaation kyberturvallisuuden toimintaympäristössä. Haastatteluissa korostettiin, että kun tietoa ostetaan ulkopuolelta, tulee sopimuksia tehdessä kiinnittää tarkasti huomiota sanamuotoihin ja sopimusten sisältöön, jotta palvelu vastaa organisaation vaatimuksia.

Aikaisemmin Oy Apotti Ab käytti runsaasti konsulttipalveluita, mutta viime aikoina henkilöstöstrategia on muuttunut ja tietoturvatiimin kokoa organisaatiossa on kasvatettu palkkaamalla tietoturva-ammattilaisia suoraan organisaation palvelukseen. Haastateltavat nostivat esiin henkilöstöön liittyvän kansallisen ongelman eli sen, että osaavia ammattilaisia ei ole tarpeeksi kysyntään verrattuna. Oy Apotti Ab:n tulee kilpailla niistä samoista resursseista, joita havittelevat monet muutkin. Työntekijöitä ohjaa tietenkin palkka, mutta raha ei ratkaise kaikkia ongelmia ainakaan pidemmällä aikajänteellä. Henkilöstö tulee myös saada pysymään talossa. Haastatteluissa nostettiin esiin Oy Apotti Ab:n kompleksinen rakenne, jossa tarvittavaa tietotaitoa vaaditaan paljon ja sen sisäistäminen vie aikaa. Vaihtuvuutta organisaatiossa tulisi pyrkiä vähentämään jo ihan tietotaidon katoamisen sekä uuden ihmisen kouluttamisen aiheuttamien kustannusten ja väliaikaisen tietotaitovajeen vuoksi.

Resurssit koettiin tietoturvatiimissä pääsääntöisesti riittäväksi, mutta uusien sopimusten ja konsulttien vähentämisen vuoksi tilannetta tulee tarkastella vähintään vuosittain. Muutama haastateltava nosti esille tietosuojatiimin niukan resurssoinnin, joka vaikuttaa välillisesti myös tietoturvatiimin toimintaan, ja on siten

muuttuva tekijä myös kyberturvallisuuden näkökulmasta. Myös teknisen henkilökunnan tiedostettiin olevan erittäin työllistetty.

On hyvä tiedostaa myös ekonomisesta näkökulmasta, että kyberturvallisuutta toteutetaan koko organisaation henkilökunnan voimin, eikä vastuu ole vain tietoturvatiimillä. Haastatteluissa nousi esille olemassa olevien resurssien innovatiivinen käyttö. Syksyllä 2022 aloitti toimintansa Oy Apotti Ab:n laajuinen kyberturvaverkosto, johon organisaation eri yksiköissä työskentelevät henkilöt, riippumatta heidän ammattinimikkeestään tai työtehtävästään, ovat saaneet liittyä. Nämä kyberturvalähettiläät nähdään tärkeänä resurssina kyberturvallisuuden edistämisessä monimutkaisen organisaation eri osissa. Verkosto nähdään kustannustehokkaana tapana lisätä ja syventää henkilökunnan kyberturvallisuustaitoja. Haastateltavien vastauksissa kuului syvä tyytyväisyys siitä, että organisaation johto on antanut ihmisille mahdollisuuden käyttää omaa työaikaansa vapaaehtoiseen kyberturvallisuuden edistämiseen. Tällainen talon sisällä tapahtuva kouluttaminen on pieni investointi, jolla saadaan kyberturvallisuuden osalta paljon aikaiseksi. Pitkäaikaisena muutosvaikuttajana nähtiin se, että verkoston ylläpitoon, kehittämiseen ja toimintaan tulee panostaa, jotta henkilökunnan asenne ja innostus aihetta kohtaan pysyy yllä ja siten kyberturvallisten toimintatapojen levittäminen ja kehittäminen Oy Apotti Ab:ssa jatkuu myös tulevaisuudessa. Kuvio 8 tiivistää ekonomisen analyysin tulokset.



Kuvio 8. Ekonomisen analyysin muutostekijät ja vaikutussuhteet

8.3 Sosiaaliset muutostekijät

Sosiaalisista muutostekijöistä haastateltavat nostivat vahvasti positiivisessa mielessä esiin uuden, vuoden 2021 lopulla tehtävään valitun, tietoturvajohtajan vaikutuksen Oy Apotti Ab:n kyberkulttuurin. Hänen kerrottiin onnistuneen avaamaan organisaation tietoturvan ja kyberturvallisuuden avoimeksi ja läpinäkyväksi prosessiksi, joka on aiheuttanut positiivisen kulttuurinmuutoksen työyhteisössä. Haastateltavat kokivat tämän kulttuurin positiiviseksi ja olivat sen kehityksessä mielellään osallisena.

Tietoturvajohtajan lisäksi haastateltavat nostivat esiin kyberturvallisuuden toimintaympäristön muuttuvana tekijänä kokonaisuudessaan henkilöstön ja siihen vaikuttavat tekijät. Työntekijöiden jaksaminen ja vaihtuvuus huolettivat. Henkilöstön vaihtuvuus on myös kyberturvallisuudelle haaste. Haastateltavien mukaan tulee kiinnittää erityistä huomiota siihen, että henkilöstö viihtyy organisaation palveluksessa. Tästä nostettiin esimerkeiksi, että työnantajan tulee tarjota mielenkiintoisia työtehtäviä, työilmapiirin tulee olla hyvä ja erityisesti työmäärän pitää olla järkevä. Uuden henkilön palkkaamisessa on aina oma haasteensa, jotta löydetään henkilöt, jotka ovat oikeilla intresseillä hakemassa työpaikkaa. Oy Apotti Ab:n työnhakuilmoituksissa mainitaan, että tarvittaessa voidaan tehdä henkilöturvallisuusselvitys, mutta sekään ei välttämättä pysty vaikuttamaan siihen, etteikö organisaatioon voisi päästä töihin sisälle henkilö, jonka vaikuttimet eivät ole täysin puhtaat.

Monessa haastattelussa nostettiin esille se, että Oy Apotti Ab:lla on julkisuudessa äärimmäisen huono maine, jonka syytä ei täydellisesti osata selittää. Sanomalehdet ja sosiaalinen media vaikuttavat siihen mielikuvaan, mikä ulkopuolisilla on Oy Apotti Ab:sta. Kansalaisten näkökulmasta Oy Apotti Ab on ristiriitainen yritys: toisaalta esimerkiksi Maisaa kehutaan runsaasti, mutta itse tietojärjestelmää kohtaan esitetään kohtuutontakin kritiikkiä. Kansalaisten kokemus Oy Apotti Ab:sta ja Apotti-tietojärjestelmästä on kyberturvallisuuden kannalta otettava huomioon, sillä digitaalisten palveluiden määrä lisääntyy ja varsinkin kun väestö ikääntyy, niin usein lisääntyy myös palveluiden tarve. Tämän vuoksi julkisuuskuvaan tulisi

saada muutos. Tällä hetkellä julkinen paine, joka on kohdistunut myös yksittäisiin työntekijöihin, lisää henkilökunnan kuormitusta ja vaikuttaa työhyvinvointiin. Työnhyvinvoinnin parantamiseen ja jaksamiseen tulee kiinnittää organisaatiossa huomiota.

Tietoturvaan tutustuminen on osana uusien työntekijöiden perehtymissuunnitelmaa, jolloin tärkeimmät Oy Apotti Ab:n kyberkulttuuriin liittyvät asiat tulevat esiin. Kuitenkin huomionarvoista on se, että eräs haastateltava kertoi tulleensa Oy Apotti Ab:hen töihin muutama vuosi sitten ja hänen kokemuksensa oli, että tietoturvaan ja kyberturvallisuuteen ei saanut kovin syvällistä perehdytystä. Hän vertasi saamaansa perehdytystä toiseen työpaikkaansa ja totesi siellä asioiden hoituneen paremmin. Tämän parantaminen tulee nähdä kehityskohteena.

Kyberturvallisuuden koettiin kuitenkin olevan Oy Apotti Ab:ssa hyvällä tasolla niin laajalla katselukannalla, mitä haastateltavilla oli organisaation henkilöstöön. Organisaatiossa on panostettu jo aikaisemmin kyberturvallisuuden parantamiseen muun muassa Hoxhunt-pelin kautta, jossa sähköpostiin lähetetään huijausviestejä, joiden tunnistaminen edistää käyttäjän etenemistä pelissä ja samalla tietoturvatuntemusta. Haastateltavat painottivat, että toiminnanmuutos kyberturvallisuuden parantamiseen tulee olla jatkuvaa ja se tulee pitää pinnalla ja keskusteluissa jatkuvasti monella eri tasolla. Tietoturvatiimi on erilaisten sähköisten kanavien kautta viestimisen lisäksi järjestäneet esimerkiksi kyberkornereita, teemaviikkoja ja jopa kyberturvallisuuspakohuoneen.

Haastateltavien mukaan kyberturvallisuudesta on viestitty avoimesti ja runsaasti ylhäältä alaspäin ja organisaatioon on sitä myötä rakentumassa oma kyberturvallisuusverkosto. Organisaation henkilökunnan joukosta on löydetty vapaaehtoiset ja aiheesta kiinnostuneet ihmiset, jotka toimivat linkkeinä kyberturvallisuuden edistämisessä organisaation jokaiseen yksikköön ja tiimiin. Nämä kyberturvalähettiläiksi nimetyt henkilöt koettiin tärkeäksi informaatioväyläksi muokkaamaan työntekijöiden päivittäistä työtä tieto- ja kyberturvallisemmaksi. Tämä toteutuu parhaiten, jos informaatio tulee oman työtehtävän näkökulmasta. Haastateltavat tunnistivat, että tietyissä asioissa viestinnän tulee tapahtua horisontaalisesti, jotta toimintatavat muuttuvat pysyvästi.

Tietoturvatiimissä tunnistettiin, että viestintäyhteys tulee olla myös alhaalta ylöspäin kohti tietoturvatiimiä. Tiimi on panostanut siihen, että se on tuonut itseään näkyväksi ja mahdollistanut useamman väylän tietoturva-asioista viestimiseksi myös toiseen suuntaan. Tavoitetilana nähtiin kyberturvallisuuden edistämiseksi organisaation laajuudella se, että lopulta kyberturvallisuuskulttuuri on organisaation jokaisessa osassa niin vahva, että se on osa päivittäistä elämää, jolloin jokainen uusi työntekijä oppii kuin vahingossa tekemään asiat oikein. Tällaisen kyberkulttuurin toteuttaminen vaatii laaja-alaista yhteistyötä. Haastateltavat näkivät, että tietoturvatiimiä on tuotu lähemmäs muuta henkilökuntaa ja kulttuurinmuutos on käynnissä, mutta yhteistyötä pitää vielä kehittää siten, että kommunikaatio tietoturvatietoudesta ja tietoturvahavaintojen tekemisestä ja niiden korjaamisesta paranee.

Organisaation sisäisen kyberkulttuurin edistämisen lisäksi koettiin, että on erittäin tärkeää, että johto viestii eteenpäin Oy Apotti Ab:n toimintatavoista myös asiakkaille ja yhteistyökumppaneille. Tulee muistaa, että Apotti-tietojärjestelmää käyttävät kymmenet tuhannet ammattihenkilöt ja myös heidän huomioimisensa Oy Apotti Ab:n tasolla on tärkeää. Tämä lisää kyberturvallisuutta, vahvistaa yhteistyötä ja estää väärän tiedon liikkumisen asiakkaiden ja Oy Apotti Ab:n välillä.

Yhtenä johtavana ajatuksena kyberturvallisuuden ja kyberkulttuurin edistämiseen nousi johdon ja esihenkilöstön asenne kyberturvallisuutta kohtaan. Johdon asenne vaikuttaa siihen, miten henkilökunta asennoituu kyberturvallisuuteen. Jos yksikin esihenkilö vähättelee kyberturvallisuutta, voi se johtaa kaikkien hänen alaistensa asenteeseen ja työtapoihin. Haastatteluissa korostettiin sitä, että organisaation kulttuuriin tulee saada sisäistettyä se, että työt tulee tehdä kyberturvallisesti ja tämä vaatii sen, että henkilöstöä tulee kouluttaa vuosittain. Tällä hetkellä on ohjeistuksena tietoturvakoulutuksen suorittaminen vuosittain, mutta esihenkilöstö ei tätä vahvasti valvo. Haastatteluissa nostettiin esille pakollisen yhteisen koulutuksen lisäksi se, että tulisi panostaa myös siihen, että jokainen työntekijäryhmä saisi tarpeelliset ohjeistukset tehdä työtään kyberturvallisesti. Organisaatiossa on esimerkiksi integraatio-osaajia ja raportoinnin parissa työskenteleviä, jotka tarvitsisivat erityiset ohjeistukset, jotta kaikki toimisivat samalla tavalla

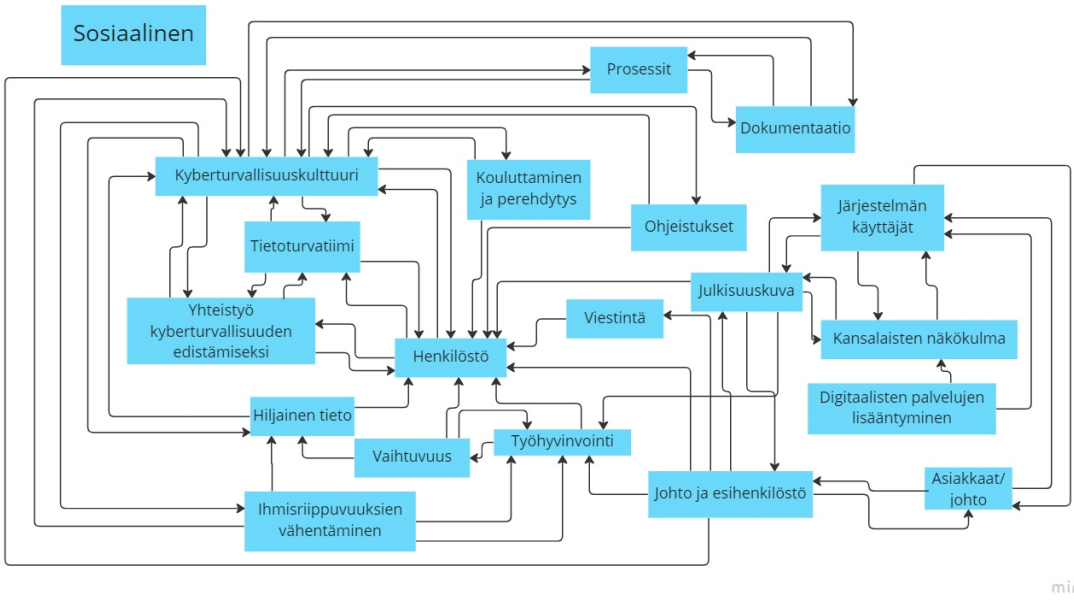
ja varmistettaisiin kyberturvalliset toimintatavat. Tietoturva haluttiin nostaa entistä korostetummin osaksi kaikkia organisaatiossa tapahtuvia prosesseja.

Haastateltavat totesivat kysyttäessä, että kyberturvallisuuden ja tietoturvan ohjeistuksiin ja niiden ylläpitoon tulisi panostaa. Ohjeet eivät ole tällä hetkellä löydettävissä helposti, vaikka niitä saattaakin olla. Haasteena nähtiin löydettävyyden lisäksi se, että ohjeista saattoi olla olemassa useita versioita, jolloin tiedon ajantasaisuudesta ei ollut taetta. Kehityskohteena olisikin tietoturvallisuuteen liittyvien ohjeiden päivitys ja versioiden ylläpito, sekä niiden löytyminen sellaisesta paikasta, josta jokainen työntekijä voi niitä tarvittaessa käydä lukemassa. Yhtenä positiivisena esimerkkinä mainittiin, että ICT julkaisee runsaasti informaatiota esimerkiksi siitä, mitä laitteille voi ladata tai miten fyysisiä laitteita tulee kohdella. Kuitenkin koettiin, että näiden ohjeiden löytäminen jälkikäteen oli hieman haastavaa ja julkaisumuodon toivottiin olevan vähemmän tekninen. Eräs haastateltava totesi, että ohjeistusten löytyminen ja ylläpitäminen on tärkeässä osassa kyberkulttuurin jalkauttamisessa koko henkilöstön toimintatavaksi.

Koko kyberturvallisuutta koskeva dokumentaatio nousi suurena vaikuttavana muutostekijänä esiin kyberturvallisuuden sosiaalikulttuurin muutoksessa. Haastateltavat korostivat, että hiljainen tieto ja ihmisriippuvuudet tulee nähdä riskinä ja riskein minimointiin tulisi käyttää resursseja. Organisaation tulee panostaa sekä ohjeistusten, että muiden dokumentaatioiden laadukkuuteen ja ajantasaisuuteen. Tietämyksenhallinta ja tiedolla johtaminen ovat osa-alueita, joihin panostamalla voidaan vähentää yllätyksiä kyberturvallisuuden toimintaympäristössä. Oy Apotti Ab tarjoaa työkalut ja ohjeistukset tiedon jakamiseen, hallintaan ja luokitteluun. Kokonaisuudessaan tekemistä tulisi kuitenkin dokumentoida paremmin, dokumentit tulisi olla löydettävissä ja niiden tulisi olla ajantasaisia. Organisaation tulisi pyrkiä luomaan toimintakulttuuri, jossa kaikki tietäisivät miten ja mitä pitäisi dokumentoida sekä minne dokumentit ja kuvatut prosessit tulee tallentaa. Esimerkkinä ongelmallisesta käytöksestä nostettiin se, että ihmiset tallentavat dokumentteja vain omalle koneelleen.

Erityisen tärkeäksi koettiin, että erilaisille prosesseille tulisi nimetä selkeästi omistajuudet, vastuut ja vetäjät. Tällä tavoin jokainen kyberturvallisuuden osa-alue

olisi joidenkin omistuksessa, jolloin ihmisriippuvuudet vähenisivät ja kaikki osa-alueet olisivat varmasti huomioitu päivittäisessä toiminnassa. Tavoitteena on, että dokumentit ja prosessit olisivat ajantasaisia ja niistä olisi löydettävissä vain viimeisin ja ajan tasalla oleva versio. Tällainen toimintakulttuuri loisi pohjan säännölliselle tekemiselle, joka voidaan helposti suunnitella ja tekeminen voidaan priorisoida. Sosiaalisen analyysin muuttujat ja niiden keskinäisiä yhteyksiä on esitetty kuviossa 9.



Kuvio 9. Sosiaalisen analyysin muutostekijät ja vaikutussuhteet

8.4 Teknologiset muutostekijät

Oy Apotti Ab tarjoaa erilaisia digitaalisia palveluita, jotka näyttäytyvät organisaation työntekijöille, palveluntarjoajien palveluksessa työskenteleville ammattihenkilöille ja tavallisille kansalaisille eri tavoin. Digitalisaatio kehittyy hurjaa vauhtia ja tässä vauhdissa myös Oy Apotti Ab:n tulee pysyä mukana. Uusia innovaatioita tulee tarkastella sen mukaisesti, miten ne mahdollisesti vaikuttavat organisaation, asiakkaiden ja palveluita käyttävien kansalaisten kyberturvallisuuteen. Muutamissa haastatteluissa pohdittiin teknologisen kehityksen kaarta pidemmälle tulevaisuuteen. Esimerkkeinä nostettiin se, miten kvanttitietokoneet tai tekoälyn kehitys vaikuttavat uhkana tai mahdollisuutena. Uudet innovaatiot tulee ottaa huomioon toimintaympäristöanalyysissa, sillä esimerkiksi jos mobiilivarmenteen ja

pankkitunnusten lisäksi kehitetään uusia tunnistautumismahdollisuuksia palveluihin, täytyy myös Apotin tietojärjestelmän taipua tähän.

Eräs haastateltava nosti esiin, että on ennustettu, että matkapuhelimet tulevat häviämään ja tämän vaikutus tulee ottaa teknologisessa toimintaympäristöanalyysissa huomioon, kun tietojärjestelmää käyttäville ammattihenkilöille tulee miettiä muita keinoja käyttää tietojärjestelmän mobiiliversiota ja kansalaisille pitää mahdollistaa kirjautuminen myös muilla tulevaisuuden laitteilla Maisaan. Teknologista kehitystä ja sen vaikutuksia tulee seurata sekä organisaation sisäisellä, kansallisella sekä globaalilla tasolla. Kansainvälisesti tapahtuvilla trendeillä on tapana rantautua jossain vaiheessa myös Suomeen. Se, miten riskeihin ja mahdollisuuksiin kyetään varautua, vaikuttaa suoraan liiketoiminnan onnistumiseen.

Oy Apotti Ab:n kyberturvallisuuden yhtenä oleellisena huomioon otettavana kokonaisuutena on huomioida se, että Apotti-tietojärjestelmä ja Maisa ovat vain yksi osa asiakkaiden ja kansalaisten käyttämistä digitaalisista palveluista. Järjestelmään on integroitu runsaasti laitteita, kuten tiettyjä lääkinnällisiä laitteita ja toimintaympäristö on jatkuvasti muuttuva. Nämä muutokset vaikuttavat Oy Apotti Ab:n kyberturvallisuuteen joko suoraan tai välillisesti. On tärkeää kyetä tehdä yhteistyötä sidosryhmien kanssa ja tarkastella myös näiden liitettyjen laitteiden teknologiaa ja turvallisuutta, ettei esimerkiksi jonkun lääkinnällisen laitteen kautta ole väylää tietojärjestelmään. Yhtenä nostona tietoverkon turvallisuutta ajatellen nostettiin, että varmuuskopiointi ja tarvittavien tietojen kahdentaminen tulee olla toteutettu laadukkaasti ja turvallisia periaatteita noudattaen.

Oleellisinta kyberturvallisuuden näkökulmasta on tiedostaa kaikkein kriittisimmät toiminnot, joiden toiminta tulee turvata kaikissa tapauksissa. Oy Apotti Ab:n järjestelmissä on tallennettuna runsaasti kriittistä ja arkaluontoista tietoa, jonka eheys, luotettavuus ja saatavuus tulee taata. Kaikissa haastatteluissa yhdeksi tärkeimmäksi teknologisen toimintaympäristön teemaksi nousi erilaisten prosessien kuvaus, niiden omistajuus ja vastuut. Varsinkin kriittisimpiin toimintoihin liittyvät prosessit tulee olla kirjattuna, sovittuna ja ylläpidettynä Oy Apotti Ab:n ja sen sidosryhmien kanssa. Tietämyksenhallintaa ja prosessikuvausten ajantasaisuutta painotettiin lähes jokaisessa haastattelussa. Prosessien ja

dokumentaation tulee olla helposti löydettävissä, selkeästi kirjattuna ja päivitettynä. Tästä huomioitiin, että edistysaskelia on otettu, mutta parantamisen varaa löytyy. Yhtenä ratkaisuna esitettiin ISO 27001 -standardin tavoittelua, koska se vaatii hyvän dokumentaation organisaation toiminnasta.

Haastatteluissa nostettiin prosessikuvauksista esille esimerkkinä, että pelkkä varmuuskopioiden olemassaolo ei uhkatilanteen toteuduttua ole riittävää kyberturvallisuuden ylläpitoa. Täytyy määritellä vastuut siitä, mikä taho määrittää sen, mihin varmuuskopiot palautetaan ja miten määritellään se, että toimintaympäristö on saatu puhdistettua ja toiminta voi jatkua normaalisti. Jatkuvuuden suunnittelu ja siihen liittyvät prosessit ovat toipumissuunnittelun ja siihen liittyvien prosessien kanssa yksi Oy Apotti Ab:n teknologisen varautumisen tärkeimpiä kokonaisuuksia.

Prosessikuvausten tarpeellisuudesta nostettiin esiin myös rutiinitoimenpiteet, jotka liittyvät jatkuvaan kehittämiseen ja kehitykseen, eikä toteutuneeseen uhkaan. Näitä toimintoja tehdään ja toteutetaan onneksi huomattavasti useammin kuin toteutuneiden kyberuhkien aikaisia ja jälkeisiä toimintoja. Esimerkiksi nostettiin muun muassa uuden palvelimen käyttöönotto. Prosessissa tulisi olla kuvattuna miten uusia fyysisiä laitteita tai palveluja otetaan käyttöön, miten ne integroidaan Oy Apotti Ab:n kyberturvallisuuden verkostoon, eli miten esimerkiksi SOC uuden palvelimen huomioi. Samalla tulisi olla kirjattuna laitteiden ja palvelujen koko elinkaari, eli mitä tapahtuu siinä vaiheessa, kun palveluita ja laitteita poistetaan käytöstä.

Monessa haastattelussa painotettiin elinkaariajattelua. Uutta palvelua tai laitteita hankkiessa tulee muodostaa selkeä käsitys siitä, minkälainen hankittavan tuotteen tai palvelun elinkaari tulee olemaan, miten se vaikuttaa kyberturvallisuuden kokonaiskuvaan ja siten toimintaympäristöön. Se, että kyetään ymmärtämään toimintaympäristö ja siinä olevien palvelujen ja laitteiden eri elinkaaren vaiheet, mahdollistaa se teknologisen toimintaympäristön hallinnan. Haastatteluissa tunnistettiin haasteeksi kyberturvallisuuden teknologisen kentän laajuus Oy Apotti Ab:ssa. Teknologisella puolella kyberturvallisuutta toteutetaan monessa eri yksikössä ja osa palveluista ostetaan Oy Apotti Ab:n ulkopuolelta. Lisäksi tuotteita ja

palveluita on monia, jotka kaikki ovat eri elinkaaren vaiheessa. Siksi esille nousi tarve siitä, että prosessien ylläpitoon tulisi saada kehitettyä jonkunlaista automatisaatiota, jolloin virheiden mahdollisuus pienenee ja kyberturvallisuus paranee. Kokonaisuus on muuten haastava hallita monimutkaisuutensa vuoksi.

Teknisen toimintaympäristön moniulotteisuus tunnistettiin haasteeksi myös henkilöstön näkökulmasta. Varsinkin Oy Apotti Ab:ssa teknologisella puolella tietotaito on erittäin henkilöitynyttä ja osaajat ovat hyvin työllistettyjä. Tämä koettiin suureksi riskiksi. Prosessien kuvaukset, dokumentaatio ja omistajuuksien nimeäminen nähtiin keinona vähentää ihmisriippuvuuksia ja siten lisääntyisi oleellisesti mahdollisuudet kehittää kyberturvallisuutta laadukkaammaksi. Yhteistyötä ja siihen luotavia pelisääntöjä toivottiin Oy Apotti Ab:n sisällä tietoturvatiimin, käyttöpalveluiden ja ICT:n kanssa. Eräs haastateltava mainitsi kokevansa, että eri tiimit ovat kaikki omalla tavallaan omissa kuplissaan ja tästä seuraa epätietoisuus siitä, onko kokonaisuus varmasti hallittu.

Haastatteluissa nousi esiin teknologisen toimintaympäristön kohdalla jatkuva viestintä kyberturvallisuuden kokonaisuuksista kaikille organisaation työntekijöille. Uusia teknologioita otetaan käyttöön jatkuvasti ja pelisäännöt on hyvä kerrata aika ajoin. Ne aiheet, jotka ovat teknologisen puolen ammattilaisille tai tietoturvaosaajille arkipäivää, saattavat olla sellaisia asioita, joita muut työntekijät eivät vielä ole omaksuneet. Ohjeiden selkeyteen, versiointiin ja sijaintiin intrassa tulisi korostetusti panostaa. Muutama haastateltava nosti esimerkiksi etätyön ja siihen liittyvät ohjeistukset, joilla voisi muistuttaa työntekijöitä kyberturvallisista toimintatavoista, vaikka Oy Apotti Ab:n teknologinen määräysvalta ei kotitoimistolle yletykään.

Kyberturvallisuuden teknistä toimintaympäristöä ei toteuteta vain Oy Apotti Ab:n sisäpuolella, vaan osa tietotaidosta on ostettu ulkopuolisilta palveluntarjoajilta. Haastateltavat korostivat sitä, että ulkoistaminen on tietyissä tapauksissa järkevin toimintastrategia, jotta kyberturvallisuus ja siihen kohdistuvat uhkat pystytään tunnistamaan ja tilannekuva Oy Apotti Ab:n kyberturvallisuudesta olisi selkeä ja valvottu. Esimerkiksi nostettiin tietyt palvelut, kuten esimerkiksi SOC tai SIEM, jotka todettiin kannattavaksi ostaa ulkopuoliselta taholta, joiden yritystoiminnan

ainoana tehtävänä on pysyä kybermaailmassa aallonharjalla. Näihin ulkoistettuihin palveluihin liittyy aina elinkaari, joka pitää ottaa huomioon organisaation toimintaympäristön muutostekijänä. Sopimukset uusitaan ja kilpailutetaan tietyin väliajoin. Tämä luonnollinen tapahtuma oli käynnissä haastattelujen aikaan. Haastatteluissa painotettiin sitä, että sopimusten sanamuotoihin ja sisältöön tulee kiinnittää erityistä huomiota, jotta kaikki osapuolet ovat selvillä, mitä on oikeastaan sovittu. Myös sopimusten kestoon tulee kiinnittää huomiota ja miettiä miten se vaikuttaa Oy Apotti Ab:n kyberturvallisuuteen vuoden, kahden tai kymmenen vuoden päästä. Ulkoisten tahojen lisäksi Oy Apotti Ab:n tulee tehdä sopimuksenmukaista yhteistyötä myös järjestelmätoimittajan kanssa, joka on osana Apotti-tietojärjestelmän tietoturvaa. Järjestelmätoimittajan tekemät ratkaisut tietojärjestelmään vaikuttavat myös Apotti-tietojärjestelmään ja sitä kautta Oy Apotti Ab:n kyberturvallisuuden toteuttamiseen.

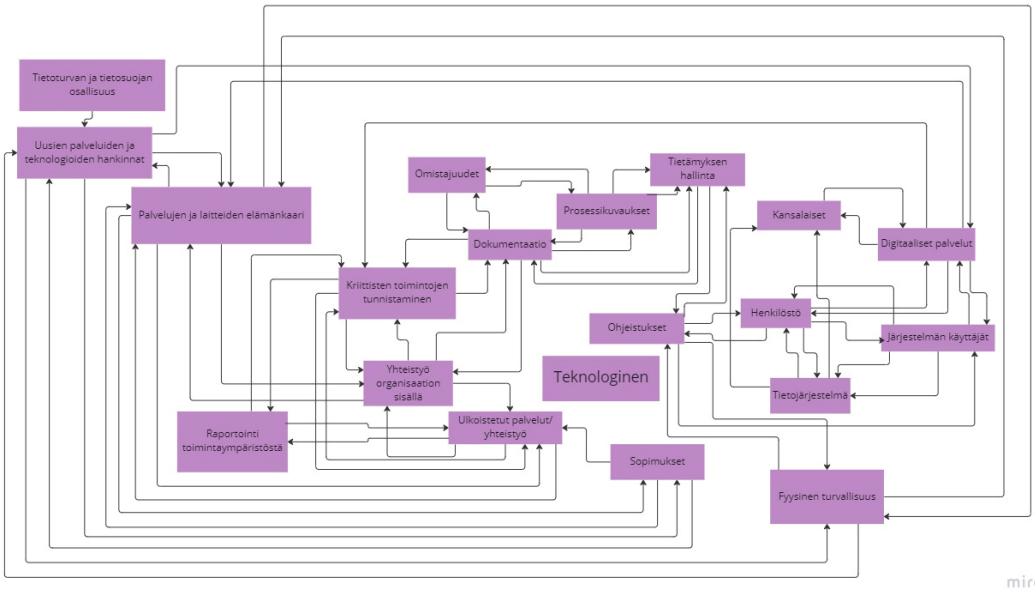
Tietoturvan ja tietosuojan osallistumista organisaatioon tehtävien hankintojen prosesseissa painotettiin. Teknologiat, joita organisaatioon hankitaan, tulee olla turvallisia. Toimittajaketjujen hallinta ja ymmärrys tulee pitää korkealla ja tarkastelu tulee tehdä myös mahdollisten alihankkijoiden osalta. Tämä koettiin toteutuvan pääasiallisesti hyvin. Kehityskohteena nostettiin Oy Apotti Ab:n ja asiakkaiden välinen teknologisen yhteistyön parantaminen. Hankinnoissa tulee tehdä tiivistä yhteistyötä asiakkaiden kanssa, jotta varmistetaan hankintojen yhteensopivuus, jolloin turvallinen tiedonsiirto mahdollistuu.

Oy Apotti Ab:n kyberturvallisuuden monimuotoista toimintaympäristöä seurataan monella eri tapaa. Organisaatio saa runsaasti raportteja, analyyseja ja muuta informaatiota järjestelmään kohdistuneista kyberuhkista ja muista vaikutteista, joten ongelmana ei ole tiedon määrä. Haasteena haastateltavat kokivat sen, että tietoa tulee todella runsaasti ja sen analysointiin ja käsittelyyn tulisi panostaa enemmän. Tiedolla ei ole arvoa, ellei sitä osata käyttää oikein.

Lisäksi fyysinen turvallisuus nousi esiin melkein kaikissa haastatteluissa. Tähän kokonaisuuteen sisältyivät sekä tietoverkkojen ja konesalien rakenteet että toimistotilojen ja käytössä olevien fyysisten laitteiden turvallisuus. Tietoverkot on rakennettu turvallisuusajattelulla, mutta pohdintaa herätti se, vaikuttaako

aikaisemmin tehdyt ratkaisut mahdollisesti haasteena tulevaisuuden tarpeille. Työntekijöiden fyysiset laitteet ja toimistoympäristö koettiin pääsääntöisesti turvalliseksi. Haastattelujen aikaan organisaatiossa pohdittiin toimistotilojen uudelleen järjestelyä, joka tulee ottaa muutostekijänä huomioon. Turvallisuutta on parannettu jatkuvasti, muun muassa turvaporttien rakentamisella toimiston oville, jolloin ulkopuolisten pääsyä toimistoalueelle on selkeästi vaikeutettu. Työkoneet ja muut liitännäislaitteet ovat uusia, turvallisia ja niiden toimintaa ylläpidetään organisaation puolelta. Työntekoon tarkoitettujen laitteiden elinkaari tulee pystyä pitämään tarpeeksi lyhyenä, jotta laitteet pysyvät turvallisina.

Kokonaisuudessaan voidaan summata, että teknologinen toimintaympäristön hallinta vaatii syvän ymmärryksen palveluiden ja laitteiden toimittajahallinnasta. Vastuunjakaminen ja prosessien kirjaaminen ohjaavat toimintaa organisaation sisällä, jolloin on selkeämmin ymmärrettävissä kustannusten ja uusien kyvykkyyksien vaikutus Oy Apotti Ab:n toiminnassa. Kuvio 10 esittää teknologisen analyysin tiivistetysti.



Kuvio 10. Teknologisen analyysin muutostekijät ja vaikutussuhteet

8.5 Ekologiset muutostekijät

Oy Apotti Ab nähtiin haastatteluissa olevan osa ympäristöystävällisyyden edistämistä ja ilmastonmuutoksen hillitsemistä. Organisaatio on Green Office -sertifioitu, jonka nähtiin vaikuttavan suoraan kyberturvallisuuteen. Tästä esimerkkinä nostettiin tulostamiseen liittyvät käytännöt. Turvatulostaminen ja tulosteiden määrän tavoitteellinen vähentäminen ovat johtaneet tilanteeseen, jossa mitään raportteja ei automaattisesti tulostu, vaan raportteja tulostetaan vain tarpeeseen ja ihmislähtöisesti. Tulostusnäkymän voi saada näkyviin myös tietokoneen näytölle, jos esimerkiksi sovelluskehityksessä on ollut tarkoituksena nähdä miltä tulostettava raportti näyttää. Näin ollen paperille ei edes tarvitse tulostaa. Tällainen toimintakulttuurin muutos on vähentänyt tietoturvauhkia toimistossa ja etätöissä, kun arkaluontoisen tai muuten tietoturvaa riskeeraavaan tiedon tulostaminen on minimoitu, jolloin ei tarvitse huolehtia tulosteiden oikeaoppisesta säilytyksestä ja hävittämisestä.

Green Office -sertifikaatin ei kuitenkaan tulisi ehkäistä kyberturvallisuuden ja -kulttuurin edistämistä. Tällaiseen tilanteeseen jouduttiin kyberturvakuukauden aikana. Tietoturvatiimin edustajat olivat huomioineet, että kokoustiloista ja puolijulkisesta kahvilasta löytyi muistiinpanoja kokouksen aiheista, esimerkiksi tietokantakaavioita. Kyberkulttuurin edistämiseksi olisi ollut hyödyllistä tulostaa laminoidut kokoushygieniasta muistuttavat tiedotteet kokoushuoneiden seinälle. Tähän ei kuitenkaan saatu lupaa sitä pyydettäessä. Tapaus osoitti sen, että kyberturvallisuuden ja kyberkulttuurin edistämisen ymmärtäminen kuuluu jokaiselle organisaatiossa työskentelevälle, ja joskus olisi suotavaa miettiä esimerkiksi tulostamisen hyötyjä ja haittoja laajemmalla näkökannalla.

Muutamassa haastattelussa nostetiin esille Oy Apotti Ab:n digitaalisten valintojen vaikutus ekologiseen toimintaympäristöön. Oy Apotti Ab:n tekemät ratkaisut uusien teknologioiden käyttöönotosta vaikuttavat turvallisuuden lisäksi ympäristöystävällisyyteen. Big Datan käyttö, digitalisaation kehitys ja Green IT:n mukaisten päätösten avulla tuetaan kestävää kehitystä ja ympäristövaikutukset näkyvät muun muassa siinä, että ratkaisut vähentävät toistuvia töitä. Kaikessa toiminnan suunnittelussa ja tekemisessä tulee ottaa ympäristöystävällisyys ja

ilmastovaikutukset huomioon, sillä nämä valinnat vaikuttavat kaikkien elämään ja suoraan tai välillisesti myös muihin PESTEL-analyysin osioihin.

Apotti-tietojärjestelmän koettiin olevan positiivinen muutostekijä ekologisen kyberturvallisuuden toimintaympäristössä, sillä järjestelmään kehitetään jatkuvasti keinoja ja tapoja olla yhteydessä sosiaali- ja terveydenhuollon ammattihenkilöihin digitaalisten palveluiden kautta. Tämä vähentää tarvetta hakeutua fyysisesti sosiaalihuollon yksikköön tai terveysasemalle, kun palvelu voidaan toteuttaa etätoimintana. Esimerkiksi päivystyskäynnit tai kotihoidon käynnit voidaan jo toteuttaa etänä. Tämän kehityssuunnan kyberturvallisuuteen tulee kuitenkin kiinnittää huomiota. Digitaalisten palvelujen tulee olla turvallisia ja muuttuvaa ympäristöä tulee kyetä hallitsemaan ja ennakoimaan.

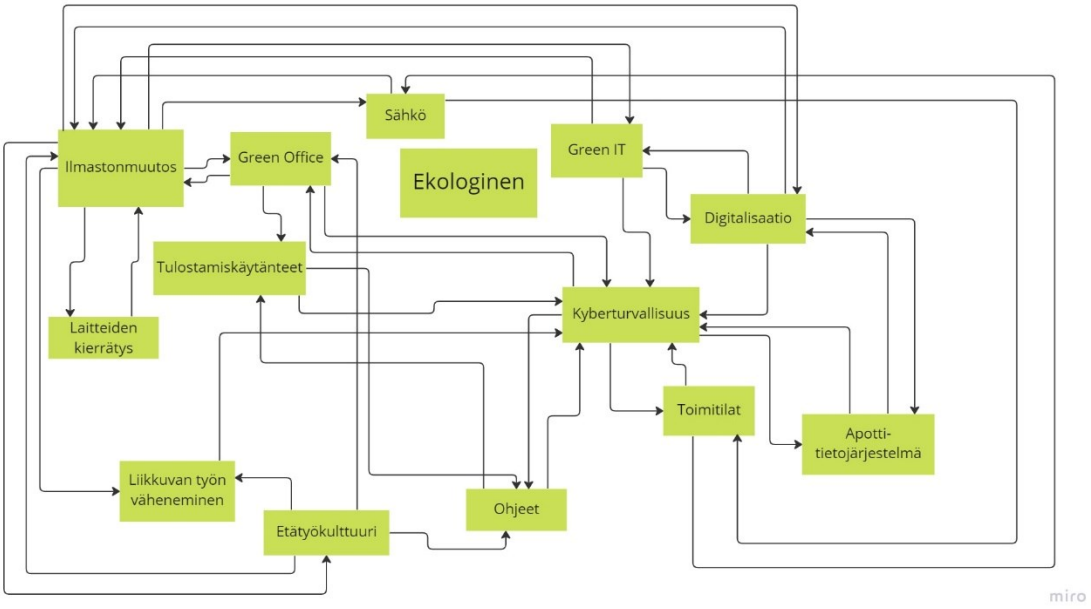
Oy Apotti Ab:n toiminnassa näkyy vihreät arvot myös muilla tavoin. Organisaatio tukee työntekijöitä työsuhdepolkupyörällä, joka on osoitus siitä, että ympäristöystävällisyys ja terveyden edistäminen ovat Oy Apotti Ab:ssa vaalittuja arvoja. Lisäksi etätyön tukeminen vähentää työmatkaliikenteen määrää. Etätyön lisääntymisen koettiin olevan kyberturvallisuuteen positiivisesti vaikuttava tekijä myös siinä suhteessa, että liikkuva työ on vähentynyt. Ihmiset eivät enää avaa niin usein työkonetta julkisissa liikennevälineissä tai muissa ympäristöissä, joiden kyberturvallisuutta ei välttämättä ole taattu. Tarpeeton liikkuminen lisää turvallisuutta myös siten, että työvälineitä ei unohdu kokoustiloihin tai asiakkaan luokse. Lisäksi nostettiin esiin etätyöskentelyn positiivinen puoli siltä näkökannalta, että avotoimistolla ei voi olla täysin varma, kuka kuulee kokouskeskustelut tai näkee näytöllä olevan toiminnan. Kaikki tekeminen ei välttämättä kuulu edes muille organisaation työntekijöille. Monella sovelluskehityksen tiimillä on edelleen niin sanottu pakollinen toimistopäivä, joka ei välttämättä tue kyberturvallista työkulttuuria edellä mainituista syistä.

Etätyöskentelyyn liittyvien ohjeistusten koettiin olevan hyvät. Tulevaisuuden suunnitelmana on muokata toimistotiloista pienemmät, sillä työpisteiden käyttöaste on pandemian jälkeen erittäin alhainen. Toimitilojen pienentäminen johtaa toimistokulttuurin muuttumiseen ja työntekeminen painottuu entistä vahvemmin etätyöskentelyyn. Fyysiset toimistotilat, niissä tulevaisuudessa tehtävä työ ja

niiden koko ja muutokset, ovat kyberturvallisuuden toimintaympäristöanalyysissa huomioon otettava aihe. Haastateltavat korostivat tämän toimintatavan muutoksen myötä, että etätyöpisteiden turvallisuus tulisi olla taattuna niillä keinoin, mitä ne Oy Apotti Ab:n puolelta on mahdollista toteuttaa.

Ilmastonmuutoksen vaikutuksista haastateltavat totesivat, etteivät ne suoraan yletä Suomeen, johtuen maantieteellisestä sijainnista. Ympäristöön vaikuttavia välillisiä tekijöitä on kuitenkin paljon, joista esiin nostettiin esimerkkeinä Euroopassa voimassa oleva sota, joka vaikuttaa muun muassa sähkön saatavuuteen ja riittävyyteen. Oy Apotti Ab:n palvelut ovat pääasiallisesti digitaalisia, jolloin sähkönsaanti on edellytys työnteolle ja tietojärjestelmän toimivuudelle. Varautumisesta sähkökatkoksiin on ICT ohjeistanut henkilökuntaa, mutta todellisia vaikutuksia talven tilanteesta ei vielä tiedetä. Tulevaisuuden ympäristövaikutuksia tulee seurata tiiviisti ja ennakoida mahdollisia vaikutuksia Oy Apotti Ab:n toimintaan.

Haastateltavien mielestä Oy Apotti Ab:n tulee myös ottaa paremmin osaa käyttämiensä laitteiden oikeaoppiseen kierrättämiseen. Jo nyt tiedetään, että teknisissä laitteissa käytettyjen arvometallien määrä on luonnossa vähäinen. Kierrättäminen ja arvometallien uusiokäyttö ovat jokaisen etu. EU:ssa valmistellaan ympäristöystävällisyyteen liittyviä vaatimuksia, joita tietynkokoiset organisaatiot on velvoitettu noudattamaan. Tämän edistymistä ja mahdollisia vaatimuksia tulee Oy Apotti Ab:n toimintaympäristössä seurata. Ekologisen analyysin muuttujat on koottu kuvioon 11.



Kuvio 11. Ekologisen analyysin muutostekijät ja vaikutussuhteet

8.6 Lainsäädännölliset muutostekijät

Haastateltavat tunnistivat monien lakien vaikuttavan Oy Apotti Ab:n toimintaan. Lähes kaikki mainitsivat, ettei lakiasiat kuitenkaan olleet heidän ominta alaansa. Haastateltavat tunnistivat lakien olemassaolon ja vaikuttavuuden, mutta sisällöt ja varsinkin lakien tulkinnat oman organisaation näkökulmasta tuntuivat hieman epämukavuusalueelta. Monet lakeihin liittyvät kokonaisuudet liikkuvat tietosuojatiimissä työskentelevän juristin pöydän kautta. Kokonaisuudessaan oli kuitenkin selvää, että organisaation toimintaan vaikuttavat sekä Euroopan unionin tasolla määritellyt vaatimukset että kansalliset lait. Haastatteluissa nostettiin esiin EU:n tasolta CER-direktiivi ja vuonna 2024 voimaan tuleva uudistunut NIS2-direktiivi, jotka tulevat toimimaan Oy Apotti Ab:n lainsäädännöllisinä muutosvoimina.

Yleisesti ottaen lakien vaikuttaminen toimintaympäristöön nähtiin samanaikaisesti hieman haastavana, mutta myös helppona kokonaisuutena. Haasteena koettiin se, että tietoturvaa ja kyberturvaa koskevat lakimuutokset sisältävät usein uusien prosessien ja vastuiden dokumentointia. Jos kyseisen kaltaisia prosesseja ei Oy Apotti Ab:ssa ole aikaisemmin dokumentoitu, saattaa tämä aiheuttaa runsaasti resursseja sitovaa työtä, sillä lakien vaatima toiminta on aikarajoitettua

ja pakottavaa. Kuitenkin esille nostettiin se, että lain vaatimat muutokset ovat usein yksiselitteisesti määrääviä, jolloin niiden toteutus on yksiselitteistä, ja ne tukevat organisaatiota kehittämään toimintaa kyberturvallisempaan suuntaan

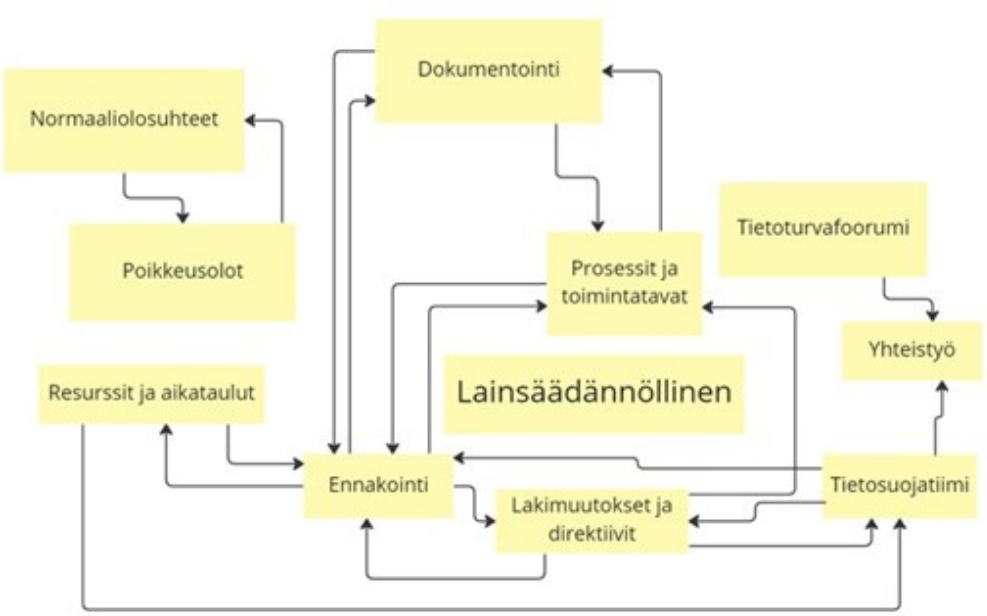
Yhtenä esimerkkinä lainsäädännöllisistä vaikutuksista nousi asiakastietolaki, jonka vaatima tietoturvasuunnitelma oli tietoturvatiimin toiminnan keskiössä haastatteluja tehdessä. Marraskuussa 2021 voimaan tulleessa ja 1.1.2023 siirtymäajan päätyttyä organisaatioiden vaatimuksena on ollut uuden asiakastietolain mukaisesti määritellä tietoturvasuunnitelma. Uusi lain vaatima tietoturvasuunnitelma on vaatimuksiltaan huomattavasti laajempi kuin aikaisemmin käytetty omavalvontasuunnitelma. Tietoturvasuunnitelmadokumentin vaatimuksiin havahduttiin erinäisien syiden vuoksi hieman myöhään ja suunnitelman tekeminen vaikutti tietoturvatiimin resursseihin syksyllä 2022. Tämä tietoturvasuunnitelman kiireinen toteutuksen aikataulu nostettiin esiin hyvänä esimerkkinä siitä, kuinka tärkeää olisi ennakoida toimintaympäristössä tapahtuvia lainsäädännöllisiä muutoksia, jotta dokumentaatioon ja muihin toimenpiteisiin tarvittavat resurssit ja aikataulutus voitaisiin toteuttaa järkevästi muiden tarpeellisten toimintojen ohessa ilman turhan suurta painetta.

Ratkaisuehdotuksena lainsäädännöllisen toimintaympäristön ennakointiin haastateltavat nostivat tarpeen siitä, että tuleviin lakimuutoksiin tulisi tutustua ennakkoon, jolloin valmistautumista ja tekemistä voitaisiin suunnitella toteutettavan suunnitelman mukaan mahdollisesti jo ennen kuin lakimuutokset ovat toteutuneet. Lakimuutokset ovat hitaita prosesseja ja laki usein laahaa hieman kehityksen perässä. Tämän vuoksi tavoitetilana voitaisiin nähdä se, että tulevia lakimuutoksia ennakoitaisiin ja kokonaisuudet olisi Oy Apotti Ab:ssa hoidettu tai ainakin tekeminen olisi suunniteltu ennen, kun laki on astunut voimaan.

Haastateltavat nostivat haasteena esille myös Oy Apotti Ab:n vaikutusvallan ylettymisen. Haasteena tunnistettiin tiettyjä yksityiskohtia, joissa asiakkaan toiminta ei välttämättä täyttänyt kaikkia Oy Apotti Ab:n itselleen asettamia kyberturvallisuuteen määrittelemiä kriteerejä. Joissain tapauksissa sidosryhmien tekemät toimet saattoivat vaikuttaa jopa ristiriitaisesti Oy Apotti Ab:n toimintamalliin. Tällaisten tilanteiden ratkaisuksi teemahaastatteluissa nostettiin korostuneesti esille

tietoturvafoorumin tärkeyttä, jossa asiakkaiden kanssa tiivistä yhteistyötä tekemällä voidaan luoda yhteiset toimintamallit ja pelisäännöt, joita kaikki organisaatiot sitoutuvat toteuttamaan.

Yhtenä lainsäädännöllisenä aspektina ja kyberturvallisuuteen vaikuttavana tekijänä osion haastatteluissa mainittiin myös poikkeusolosuhteet. Poikkeusolosuhteisiin liittyvät lait ei yleisesti ottaen ole muutosvaikuttajia sinänsä, sillä laki itsessään ei muutu kovin usein, mutta jos Suomessa otetaan käyttöön poikkeuslaki, vaikuttaa se myös Oy Apotti Ab:n toimintaan. Kuvio 12 esittää tiivistetysti lainsäädännöllisen analyysin muuttujat.



Kuva 12. Lainsäädännöllisen analyysin muutostekijät ja vaikutussuhteet

8.7 PESTEL-analyysityökalu Oy Apotti Ab:n kyberturvallisuuden tueksi

Oy Apotti Ab:n toiveena oli, että PESTEL-analyysityökalun runkoon nostettaisiin kunkin otsikon alle 1–3 kysymystä, joiden tulisi ohjata analyysin tekijöitä löytämään tärkeimmät ja vaikuttavimmat kyberturvallisuuteen liittyvät muutosvoimat organisaation eri yksiköissä. Kysymysten asettelussa tuli siis löytää ne kysymykset, joilla pystytään tarkastelemaan muutosvoimia mahdollisimman monesta

näkökulmasta. Kysymysten muodostamiseen käytettiin kirjallisuudesta, kansallisista ohjeistuksista ja haastatteluista saatuja tietoja. Lisäksi kysymyksiä laadittaessa käytiin keskustelua Oy Apotti Ab:n tietoturvajohtajan kanssa.

Poliittisten muutosvaikuttimien pohjalta laaditut kysymykset:

- Mitkä lait, direktiivit ja sopimukset luovat reunaehdot Oy Apotti Ab:n toiminnalle ja mitä muutoksia näissä on tapahtunut/ tapahtumassa kyberturvallisuuden näkökulmasta?
- Miten Oy Apotti Ab:n johdon määrittelemä kyberturvallisuusstrategia vaikuttaa kyberturvallisuuden toimintaympäristöön?
- Millaiset muut ulkoiset tekijät, kuten sidosryhmät, Suomen sisäpolitiikka ja maailman poliittinen tilanne vaikuttavat Oy Apotti Ab:n kyberturvallisuuden toimintaympäristöön?

Ekonomisten muutosvaikuttimien pohjalta laaditut kysymykset:

- Mitkä ovat ne kriittiset toimet ja tehtävät, jotka ovat välttämätön toteuttaa ja ylläpitää Oy Apotti Ab:n toiminnan jatkuvuuden varmistamiseksi?
- Millainen on Oy Apotti Ab:n rahoituksen viitekehys, eli mitä resursseja on käytössä ja mihin niitä tulisi käyttää?

Sosiaalisten muutosvaikuttimien pohjalta laaditut kysymykset:

- Onko Oy Apotti Ab:n kyberturvallisuuden prosessit dokumentoitu, nimetty omistajuus ja vastuut?
- Onko koko Oy Apotti Ab:n henkilöstön tarvittava kyberturvallisuusosaaminen taattu koulutuksin ja perehtymisen kautta oman roolinsa osalta?
- Miten toteutetaan Oy Apotti Ab:n sisäistä ja ulkoista viestintää kyberturvallisuuden eri osa-alueisiin liittyen?

Teknologisten muutosvaikuttimien pohjalta laaditut kysymykset:

- Mitkä ovat Oy Apotti Ab:n kriittiset palvelut ja tuotteet, joiden toiminnan jatkuvuus täytyy taata kaikissa tilanteissa?
- Onko kaikilla Oy Apotti Ab:n kriittisillä toiminnoilla määriteltynä prosessikuvaus, omistajuudet ja ylläpidon vastuut?
- Minkälaisia muutoksia Oy Apotti Ab:n teknologisessa toimintaympäristössä tapahtuu, kuten innovaatiot, elinkaari, uudet palvelut ja toiminnot?

Ekologisten muutosvaikuttimien pohjalta laaditut kysymykset:

- Miten digitalisaation kehittyminen vaikuttaa Oy Apotti Ab:n kyberturvallisuuden toimintaympäristöön?
- Miten ilmastonmuutos vaikuttaa Oy Apotti Ab:n toimintaan suorasti, välillisesti tai heijastevaikutuksin?

Lainsäädännöllisten muutosvaikuttimien pohjalta laaditut kysymykset:

- Miten ja millaiset lainsäädännölliset, kuten EU-direktiivit ja kansallinen lainsäädäntö, muutokset vaikuttavat Oy Apotti Ab:n toimintaympäristöön?

9 JOHTOPÄÄTÖKSET JA POHDINTA

9.1 Tulosten tarkastelu

Haastattelut toteutettiin kaikkien henkilöiden kanssa, joille haastattelupyyntö lähetettiin. Haastateltavat ottivat haastattelutilanteen vakavasti ja koettivat vastata mahdollisimman laadukkaasti ja monipuolisesti teemakysymyksiin. Haastatteluihin varattu aika oli riittävä ja keskustelut saatiin vietyä loppuun ilman kiirettä tai tilannetta, jossa jotain olisi jäänyt sanomatta. Haastatteluilla saatiin kattavasti ja monipuolisesti tietoa halutuista teemoista.

Ennen haastatteluja oletuksena oli, että haastateltavien näkökulma kyberturvallisuuteen ja Oy Apotti Ab:n toimintaympäristöön olivat erilaiset, mutta vastaukset olivat huomattavan monimuotoisia. Haastatteluissa nousi esiin samoja aihekokonaisuuksia, mutta jokaisen haastateltavan vastauksessa oli silti oma ainutlaatuinen näkökulma. Tämä lisäsi aineiston laadukkuutta ja arvoa. Haastattelujen monipuolisuus tuki opinnäytetyön tutkimuksen tarkoitusta ja vaikutti positiivisesti tutkimuksen laatuun.

Haastattelujen ja kirjallisuuskatsauksen perusteella onnistuttiin toteuttamaan tutkimuksen tarkoitus, eli luomaan PESTEL-analyysityökalun kysymykset Oy Apotti Ab:n kyberturvallisuuden toimintaympäristöanalyysin tueksi. Analyysityökalun kysymyksiä tulee kuitenkin tarkastella kriittisesti. Vaikka tutkimuksessa saatiin laaja-alaista näkemystä kyberturvallisuuteen ja kirjallisuus tuki haastattelujen tuloksia, silti tulokset perustuvat ihmisten kokemuksiin sekä esille nousseisiin aiheisiin organisaatiossa ja yhteiskunnassa nykyhetkessä.

On huomioitavaa, että haastattelut toteutettiin noin kuukausi ennen kuin hyvinvointialueet aloittivat toimintansa ja tämä aiheutti korostuneen tietämättömyyden ja valmistautumisen puutteen tunteen haastateltavissa. Tulevat muutokset koettiin haasteelliseksi, sillä kenelläkään ei tuntunut olevan tarkkaa tietoa siitä, mihin kaikkeen muutos tulisi vaikuttamaan ja miten toiminta vuoden 2023 alun jälkeen jatkuisi. Hyvinvointialueet vaikuttavat myös kyberturvallisuuden varautumiseen ja toteuttamiseen. Tulevaisuuden kyberturvallisuuden toimintaympäristö saattaa

tuoda tullessaan haasteita, joiden olemassaolosta ei vielä tiedetä, mutta joihin pitäisi jo varautua.

Toimintaympäristöanalyysin tuottamisessa tulee tarkastella toimintaympäristön muutoksia eri pituisilla aikajaksoilla. Voidaan todeta, että esimerkiksi lainsäädännöllinen pohdinta voidaan toteuttaa melko luotettavasti ja kattavasti tutkimuksessa löydetyn yhden kysymyksen perusteella. Lainsäädännöt muuttuvat hitaasti ja tulevia lakimuutoksia voi ja tulee tarkastella etukäteen. Aikajänne lainsäädännöllisten muutosvoimien tarkasteluun voidaan pitää lyhyenä, noin vuoden tai kahden mittaisena. Nämä muutokset tuottavat organisaatiolle työtä, mutta ovat silti helposti ennakoitavissa. Toisena ääripäänä voidaan pitää teknologista näkökulmaa, jossa aikajännettä tulee kasvattaa laajan ja laadukkaan toimintaympäristöanalyysin tuottamiseksi kymmeneen vuoteen tai jopa vielä pidemmälle ajanjaksolle. Analyysiä tehdessä tulisi osata ennakoida oikein sitä, mitä kymmenen vuoden aikajänteellä tapahtuu ja miten tämän päivän ratkaisut ja päätökset tulevat vaikuttamaan organisaation tilanteeseen tulevina vuosina. Teknologian kehittyessä hurjaa vauhtia täytyy todeta, että tällaisen ennakoinnin tekeminen on äärimmäisen hankalaa ja joka tapauksessa päätökset tulee toteuttaa parhaan arvauksen perusteella.

Teemahaastatteluista on nostettavissa viisi kokonaisuutta, joiden vaikutukset ovat moniulotteisia ja voimakkaita, ja jotka vaikuttavat jokaiseen PESTEL-analyysin osioon. Näistä eniten huomiota sai dokumentaation tärkeys sisältäen prosessikuvausten kirjaamisen, omistajuuksien nimeämisen, dokumenttien tallennukseen liittyvät määrittelyt sekä laadukkaan versiohallinnan. Dokumentaation laadukkuus voidaan nähdä pohjana sille, että kyberturvallisuuteen vaikuttavat tekijät tunnistetaan tehokkaasti ja laadukkaasti, jolloin luodaan perusta toimintaympäristöanalyysille. Toimintaympäristön reunaehtoihin vaikuttavat lainsäädäntö ja sopimukset, jotka tulee ottaa huomioon toimintaympäristöanalyysia tehdessä. Teemahaastatteluissa nostettiin esille myös laadukkaan kyberturvallisuuden kriteerinä organisaation kyberkulttuuri, joka alkaa johdon tekemistä päätöksistä ja vaikuttaa organisaation jokaisen työntekijän päivittäiseen työntekemiseen. Tämä nähtiin positiivisena muutoksena Oy Apotti Ab:ssa. Oman huomionsa haastatteluissa sai myös kyberturvallisuuden ja kyberrikollisuuden muuttuva maailma. On

tärkeää, että organisaatiossa pysytään tietoisena kybermaailman tapahtumista, jolloin resursseja voidaan ohjata oikein ja tehokkaasti. Viidentenä kokonaisuutena nostettiin syy-seuraussuhteiden ymmärtäminen, joka luo edellytykset laadukkaalle toiminnalle.

9.2 Luotettavuuden tarkastelu

Tutkimuksessa kiinnitettiin erityistä huomiota tulosten luotettavuuteen. Opinnäytetyön kirjallisuuskatsauksessa lähteitä tarkasteltiin kriittisesti ja vain luotettavia lähteitä käytettiin hyväksi. Raportoinnissa pyrittiin olemaan mahdollisimman avoimia kirjoittamalla johtopäätökset läpinäkyvästi, selkeästi ja ymmärrettävästi. Haastattelut nauhoitettiin ja ne litteroitiin. Tällä lisättiin luotattavuutta, kun voitiin varmistua sanatarkkaan, mitä haastateltava on sanonut. Luotettavuutta lisäsi myös se, että haastattelija on töissä samassa organisaatiossa ja tekee tietoturvatiimin kanssa yhteistyötä. Tällöin kommunikaatio ja ymmärrys toisen käyttämästä kielestä voidaan katsoa lisäävän luotettavuutta.

Haasteena voidaan nähdä se, että haastattelut perustuvat vain yksittäisten ihmisten havaintoihin ja näkökulmiin. Välttämättä kaikkia näkökulmia ei kirjallisuuden ja haastattelujen yhteydessä löydetä. Kyberturvallisuus on laaja kokonaisuus ja siihen vaikuttavat monet asiat. Kyberuhkia syntyy jatkuvasti lisää ja tämän opinnäytetyön tiedot saattavat olla jo työn julkaisuvaiheessa osittain vanhentuneita.

9.3 Jatkokehittämisaiheet

Tämä opinnäytetyö loi pohjan kyberturvallisuuden PESTEL-analyysin käytölle Oy Apotti Ab:ssa. Työhön haastateltiin kyberturvallisuuden ammattilaisia ja tämänhetkisestä kyberturvallisuuden toimintaympäristöstä saatiin hyvä tilannekatsaus. On kuitenkin ymmärrettävä kyberturvallisuuden, uhkien ja varautumisen jatkuvasti muuttuva maailma. Tämän opinnäytetyön tuottamaa analyysityökalua tulee tarkastella kriittisesti ja sitä tulee tulevaisuudessa tarvittaessa muokata, jotta se palvelee organisaation kyberturvallisuuden edistämistä.

Jatkossa on syytä tarkastella kriittisesti ohjaako analyysityökalulla tuotetut PESTEL-analyysit löytämään suurimmat kyberturvallisuuden toimintaympäristön

muutostekijät koko Oy Apotti Ab:n laajuisesti. Oy Apotti Ab:n toimintaympäristö on laaja ja organisaation sisällä olevien yksiköiden toiminnoissa on eroavaisuuksia. Olisi tärkeä tarkastella jokaisen yksikön osalta analyysityökalun käytettävyyttä ja tarkoituksenmukaisuutta.

LÄHTEET

Adams, K. 2022. Phishing attack exposes 54K patient records at West Virginia hospital. Becker's Health IT. Viitattu 19.11.2022 https://www.beckershospitalreview.com/cybersecurity/phishing-attack-exposes-54k-patient-records-at-west-virginia-hospital.html.

Ahjopalo, J. 2019. Lahden kyberhyökkäystutkinta: livahtiko haittaohjelma tuhanteen tietokoneeseen yksittäisen käyttäjän toiminnan vuoksi? Yleisradio. Viitattu 19.11.2022 https://yle.fi/uutiset/3-10832288.

Apotti podcast 2022. Kyberturvallisuus koostuu varautumisesta ja arkisista teoista. Viitattu 8.12.2022 https://www.apotti.fi/podcast-kyberturvallisuus/.

BBC 2016. Wiggings and Froome medical records released by 'Russian hackers. Viitattu 6.12.2022 https://www.bbc.com/news/world-37369705.

Berg, B. 2007. Qualitative Research Methods for the Social Sciences. Boston: Pearson/Allyn & Bacon.

C2M2 2022. Cybersecurity Capability Maturity Model. Viitattu 15.11.2022 https://c2m2.doe.gov/.

Cisco Press 2016. Responding to Real-World Cyber Threats. Viitattu 19.11.2022 https://www.ciscopress.com/articles/article.asp?p=2481826.

Cohen, L., Manion, L. & Morrison, K. 2003. Research Methods in Education. London: RoutledgeFalmer.

Coventry, L. & Branley, D. 2018. Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. Maturitas 113 (2018) 48–52. Viitattu 6.12.2022 https://www-sciencedirect-com.ez.lapinamk.fi/science/article/pii/S0378512218301658.

Davis, J. 2019. 326000 Patients Impacted in UConn Health Phishing Attack. Health IT Security. Viitattu 19.11.2022 https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack.

Denzin, L. & Yvonne S. (toim.) 2000. Handbook of qualitative research. Thousand Oaks (Calif.): SAGE.

Digi- ja väestötietovirasto 2022. VAHTI-verkosto. Viitattu 9.10.2022 https://dvv.fi/vahti.

ENISA 2022. ENISA Threat Landscape 2022. July 2021 to July 2022. Viitattu 7.12.2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

ETLA Muistio 2020. Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät? Viitattu 19.11.2022 https://www.etla.fi/julkaisut/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/.

Epic 2020. Advancing Health and Social Care in Finland with Epic. Viitattu 8.12.2022 https://www.epic.com/epic/post/advancing-health-social-care-finland-epic.

Epic Systems Corporation 2022. Epic software. Viitattu 8.10.2022 https://www.epic.com/careeverywhere/.

Eskola, J. & Suoranta, J. 2001. Johdatus laadulliseen tutkimukseen. Jyväskylä: Gummerus.

Fingrid 2022. Venäjältä tuotu sähkö Suomessa. Viitattu 16.10.2022 https://www.fingrid.fi/globalassets/dokumentit/fi/kantaverkko/suomen-sahkojarjestelma/ajankohtaista05042022_sahkontuonti.pdf.

HE 246/2022. Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen käsittelystä ja siihen liittyviksi laeiksi. Finlex. Viitattu 22.12.2022 https://www.finlex.fi/fi/esitykset/he/2022/20220246?search%5Btype%5D=pika&search%5Bpika%5D=asiakastietolaki.

Hege, I., Tolks, D., Kuhn, S. & Shiozawa, T. 2020. Digital skills in healthcare. GMS Journal for Medical Education 2020, Vol 37(6). Viitattu 5.12.2022 https://www-ncbi-nlm-nih-gov.ez.lapinamk.fi/pmc/articles/PMC7672379/pdf/JME-37-63.pdf.

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Huoltovarmuuskeskus 2021. TIETO22-Harjoitus. Viitattu 8.10.2022 https://www.digipooli.fi/fi/tieto22.

Huoltovarmuuskeskus 2022a. Huoltovarmuuskeskus. Viitattu 6.12.2022 https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/huoltovarmuuskeskus.

Huoltovarmuuskeskus 2022b. Sektorit ja poolit. Viitattu 8.12.2022 https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio/sektorit-ja-poolit.

HUS 2021. HUSin verkkopalveluhäiriöiden syy on selvinnyt. Helsingin ja Uudenmaan sairaanhoitopiiri. Viitattu 20.11.2022 https://www.hus.fi/ajankohtaista/husin-verkkopalveluhairioiden-syy-selvinnyt.

HUS 2022. Yhteispäivystyksen etävastaanotto. Helsingin ja Uudenmaan sairaanhoitopiiri. Viitattu 15.11.2022 https://www.hus.fi/yhteispaivystyksen-etavastaanotto.

ISO/IEC 27000 2022. Tietoturvallisuuden standardisarja. Suomen Standarditoimisto SFS.

Julkisen hallinnon tietoturvallisuuden arviointikriteeristä (Julkri): Suositus ja kriteeristö 2022. Valtionvarainministeriön julkaisuja 2022:43. Viitattu 15.11.2022 http://urn.fi/URN:ISBN:978-952-367-275-8.

Kananen, J. 2017, Laadullinen tutkimus pro graduna ja opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kansallinen riskiarvio 2018 2019. Sisäministeriön julkaisuja 2019:5. Viitattu 16.10.2022 http://urn.fi/URN:ISBN:978-952-324-245-6.

Kanta 2022a. Asiakastietolain siirtymäajat ja vaiheistus. Viitattu 12.11.2022 https://www.kanta.fi/ammattilaiset/asiakastietolain-siirtymaajat-ja-vaiheistus.

Kanta 2022b. Sosiaalihuollon asiakastiedon arkisto. Viitattu 16.10.2022 https://www.kanta.fi/ammattilaiset/sosiaalihuollon-asiakastiedon-arkisto.

Kinnunen, E., Seppo, T. & Rousku, K. 2021. Digiturvallisuuden hallinta – tukimateriaali digiturvan kehittäjille. VAHTI hyvät käytännöt tukimateriaali. Digi- ja väestötietovirasto. Viitattu 19.11.2022 https://dvv.fi/documents/16079645/0/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf/f6243645-79e2-81f7-5c3d-ccf2e972b2ec/Digiturvallisuuden_hallinta_NETTI_3105_2021.pdf?t=1622534350192.

Koivisto, J. 2021. Esiselvitys sosiaali- ja terveydenhuollon kansallisten digitalisaatio-ohjelmien arviointikehikon kehittämiseksi. Työpaperi 28/2021. Terveyden ja hyvinvoinnin laitos. Viitattu 5.12.2022 https://www.julkari.fi/bitstream/handle/10024/143248/URN_ISBN_978-952-343-756-2.pdf?sequence=1.

Koivisto, T., Ilomäki, S., Kurtti, E., Koskela, I., Weiste, E., Salo, S., Aalto, O. & Husman, P., Ruusuvuori, J. 2020. Terveydenhuollon työntekijät digimurroksessa. Moniaineistoinen tutkimus asiantuntijuuden ja yhteistyön rakentumisessa. Työterveyslaitos. Viitattu 10.12.2022 https://helda.helsinki.fi/bitstream/handle/10138/327547/Terveydenhuollon%20ty%C3%B6ntekij%C3%A4t%20digimurroksessa%20loppuraportti.pdf?sequence=1.

Kotipelto, H. 2022. Kyberturvallisuus osana kansallista turvallisuutta. Sisäministeriö. Viitattu 15.11.2022 https://intermin.fi/kansallinen-turvallisuus/kyberturvallisuus.

Kullas, J. 2022. Tunnistautumissovellus olikin haittaohjelma – jos latasit Androidille, poista välittömästi, vie rahat. Mikrobitti. Viitattu 19.11.2022 https://www.mikrobitti.fi/uutiset/tunnistautumissovellus-olikin-haittaohjelma-jos-latasit-androidille-poista-valittomasti-vie-rahat/ec581705-9d02-4cfd-a489-d5d573a29848.

Kyberturvallisuuden nykytila eri toimialoilla – kartoituksen keskeiset havainnot 2020. Huoltovarmuuskeskus. Viitattu 13.11.2022 https://www.huoltovarmuuskeskus.fi/files/b3671ecb5d0b5b431174fec9350e0251b75227ba/kyberturvallisuuden-nykytila-eri-toimialoilla2-verkkosivuille.pdf.

Kyberturvallisuuden sanasto 2018. Turvallisuuskomitea. Viitattu 14.10.2022 https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf&file=pdf/Kyberturvallisuuden_sanasto.pdf.

Kyberturvallisuuskeskuksen viikkokatsaus – 44/2022. Tietoturva nyt! Kyberturvallisuuskeskus. Viitattu 20.11.2022 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskuksen-viikkokatsaus-442022.

Kyberturvallisuuskeskus 2022a. Autoreporterin haittaohjelmahavainnot. Traficom. Viitattu 19.11.2022 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot?toggle=Hummer.

Kyberturvallisuuskeskus 2022b. ISAC-tiedonvaihtoryhmät. Viitattu 20.12.2022 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/isac-tiedonvaihtoryhmat.

Kyberturvallisuuskeskus 2022c. Kybermittarit. Viitattu 15.11.2022 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot/kybermittari?toggle=Mik%C3%A4%20on%20Kybermittari%3F&toggle=Kybermittarin%20k%C3%A4ytt%C3%B6%20ja%20tuki&toggle=Mittaustulosten%20jakaminen%20ja%20vertailutiedot&toggle=Kybermittariin%20pohjautuvia%20arviointi-%20tai%20kehitt%C3%A4mispalveluita%20tarjoavat%20yritykset.

Kyberturvallisuuskeskus 2022d. Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa – ohje johdolle ja asiantuntijoille. Viitattu 20.11.2022 https://www.kyberturvallisuuskeskus.fi/fi/kyberturvallisuuden-vahvistaminen-suomalaisissa-organisaatiossa-ohje-johdolle-ja-asiantuntijoille?toggle=1%09Huomioikaa%20muutokset%20kyberturvallisuuden%20uhkakuvassa.

Kyberturvallisuuskeskus 2022e. Palvelunestohyökkäykset ovat arkipäivää Suomessa. Viitattu 20.11.2022 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa.

Kyberturvallisuuskeskus 2022f. Tietoturva. Viitattu 14.10.2022 https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

Kyberturvallisuuskeskus 2022g. Tilannekuva ja verkostot. Viitattu 6.12.2022 https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostot.

Kybersää elokuu 2022. Viitattu 6.12.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20elokuu%202022.pdf.

Kybersää lokakuu 2022. Lokakuun kybersää synkisti syksyä. Kyberturvallisuuskeskus. Viitattu 15.11.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%20lokakuu%202022.pdf.

Kybersää marraskuu 2022. Viitattu 20.12.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20marraskuu%202022_0.pdf.

Käypä hoito -suositus 2022. CPAP-hoidon langaton etäseuranta. Duodecim. Viitattu 16.10.2022 https://www.kaypahoito.fi/nix02468.

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Finlex. Viitattu 17.11.2022 https://www.finlex.fi/fi/laki/alkup/2019/20190906.

Laki potilaan asemasta ja oikeuksista 785/1992. Finlex. Viitattu 5.12.2022 https://finlex.fi/fi/laki/ajantasa/1992/19920785.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. 784/2021. Finlex. Viitattu 12.11.2022 https://www-finlex-fi.translate.goog/fi/laki/akup/2021/20210784?_x_tr_sl=fi&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

Laakso, J. 2022. Nyt täytyy haittaohjelmia varoa myös Teams-keskusteluissa. Tivi. Viitattu 19.11.2022 https://www.tivi.fi/uutiset/nyt-taytyy-haittaohjelmia-varoa-myos-teams-keskusteluissa/16720567-8c5b-4ac2-9cd2-6eb73923fee5.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. Helsinki: Valtioneuvoston kanslia. Viitattu 15.10.2022 https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0.

Lehto, M., Pöyhönen, J. & Lehto, M. 2019. Kyberturvallisuus sosiaali- ja terveydenhuollossa. Viitattu 15.11.2022 http://urn.fi/URN:ISBN:978-951-39-7711-5.

Limnéll, J. 2022. Jarno Limnéll: Kyberturva-asiantuntijoiden koulutuksessa tarve yritysten ja korkeakoulujen väliselle yhteistyölle. Sivista. Viitattu 6.12.2022 https://www.sivista.fi/blogi/kyberturva-asiantuntijoiden-koulutuksessa-tarve-yritysten-ja-korkeakoulujen-valiselle-yhteistyolle/.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Saarijärvi: Docendo.

Lääkelaki 395/1987. Finlex. Viitattu 5.12.2022 https://www.finlex.fi/fi/laki/ajantasa/1987/19870395.

Mayring, P. 2022. Qualitative Content Analysis. A Step-by-Step Guide. London: SAGE.

Melanen, J. 2022. Kelan ja Kannan verkkopalveluihin kohdistuu palvelunestohyökkäyksiä – palveluissa voi olla katkoksia. Kansaneläkelaitos. Viitattu 23.12.2022 https://www.kela.fi/ajankohtaista-henkiloasiakkaat/4967375/kelan-

ja-kannan-verkkopalveluihin-kohdistuu-palvelunestohyokkayksia-palveluissa-voi-olla-katkoksia.

Mutanen, J., Tolonen, P. & Vepsäläinen., P. 2021. Toimintojen ja tietojärjestelmien kriittisyyden luokittelu. Terveydenhuolto. Huoltovarmuuskeskus. Viitattu 16.10.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Sote_toimintojen_ja_tietoj%C3%A4rjestelmien_kriittisyyden_luokittelu_v1.0.pdf.

National Audit Office 2017. Investigation: WannaCry Cyber Attack and the NHS. Viitattu 7.12.2022 https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS-Summary.pdf.

NIST 2022. Cybersecurity framework. Viitattu 15.11.2022 https://www.nist.gov/cyberframework.

Oy Apotti Ab 2022a. Apotti osallistuu TIETO22- harjoitukseen. Viitattu 8.10.2022 https://www.apotti.fi/apotti-osallistuu-tieto22-harjoitukseen/.

Oy Apotti Ab 2022b. Apotti yrityksenä. Viitattu 8.10.2022 https://www.apotti.fi/apotti/apotti-yrityksena/.

Oy Apotti Ab 2022c. Apottiin on integroitu kymmeniä erillisjärjestelmiä HL7-standardeilla. Viitattu 25.12.2022 https://www.apotti.fi/apottiin-on-integroitu-kymmenia-erillisjarjestelmia-hl7-standardeilla/.

Oy Apotti Ab 2022d. Maisa-asiakasportaali yhdistää sosiaalihuollon ja terveydenhuollon sähköisen asioinnin yhteen kanavaan. Viitattu 9.12.2022 https://www.apotti.fi/maisa/.

Oy Apotti Ab 2022e. Usein kysyttyä. Viitattu 8.10.2022 https://www.apotti.fi/apotti/usein-kysyttya/#apotti-1.

Pispa, K. 2022. TIETO2022: Kyberpuolustuksen keskeinen periaate on tiedon jakaminen. Digipooli. Viitattu 8.12.2022 https://www.digipooli.fi/fi/ajankohtaista/uutinen/tieto22-kyberpuolustuksen-keskeinen-periaate-tiedon-jakaminen.

Pelttari, A. 2022. Päällikön kolumni: Kyberympäristön uhkatason nousun taustalla on myös Venäjä. Suojelupoliisi. Viitattu 6.12.2022 https://supo.fi/-/paallikon-kolumni-kyberympariston-nousseen-uhkatason-taustalla-on-myos-venaja.

Puro, K. 2010. Ikääntymisen haasteet yhteiskunnalle. Lääketieteellinen aikakauskirja Duodecim. 210; 126(13): 1523–4. Viitattu 21.12.2022 https://www.duodecimlehti.fi/duo98919.

Puustinen, A. & Kekki, T. 2020. Pelastustoimen ja siviilivalmiuden toimintaympäristöanalyysi. Sisäministeriön julkaisuna 2020:18. Sisäministeriö. Viitattu 16.10.2022 http://urn.fi/URN:ISBN:978-952-324-634-8.

Security Week 2020. Vaccine Documents Hacked as Wes Grapples With Virus Surge. Viitattu 19.11.2022 https://www.securityweek.com/vaccine-documents-hacked-west-grapples-virus-surge.

Sengupta, K. 2017. Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images. The Independent. Viitattu 6.12.2022 https://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html.

Silverman, D. 2002. Interpreting Qualitative Data. Methods for Analysing Talk, Text, and Interaction. 2. painos. London: SAGE.

Silverman, D. 2005. Doing Qualitative Research. 2. painos. London: SAGE.

Sisäministeriö 2017. Hyvä elämä – turvallinen arki. Valtioneuvoston periaatepäätös sisäisen turvallisuuden strategiasta. Sisäministeriön julkaisu 15/2017. Sisäministeriö: Helsinki. Viitattu 16.10.2022 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80782/sisaisen-turvallisuuden-strategia-verkko.pdf.

Sosiaali- ja terveysministeriö 2019. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille. Sosiaali- ja terveysministeriön julkaisuja 2019:14 Viitattu 14.10.2022 http://urn.fi/URN:ISBN:978-952-00-4085-7.

Sosiaali- ja terveysministeriö 2012. Potilasasiakirjojen laatiminen ja käsittely. Opas terveydenhuollolle. Sosiaali- ja terveysministeriön julkaisuja 2012:4. Viitattu 5.12.2022 http://urn.fi/URN:ISBN:978-952-00-3337-8.

Suomen kyberturvallisuusstrategia 2013. Valtioneuvoston periaatepäätös 24.1.2013. Viitattu 19.11.2022 https://puolustusvoimat.fi/documents/2182700/0/Kyberturvallisuusstrategia/bb56d179-9b3a-4816-806d-84c84b04da30.

Suomidigi 2022. VAHTI-ohjeet. Viitattu 8.12.2022 https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet.

Terveyskylä 2022. Verensokeritulosten tarkastelu erilaisten sovellusten avulla. Viitattu 16.10.2022 https://www.terveyskyla.fi/diabetestalo/diabeteksen-omahoito/verensokerin-omaseuranta/verensokerin-omamittaustulosten-hy%C3%B6dynt%C3%A4minen/verensokeritulosten-tarkastelu-erilaisten-sovellusten-avulla.

THL 2021a. Määräys sosiaali- ja terveydenhuollon tietojärjestelmien luokittelusta ja sertifioinnista. Terveyden ja hyvinvoinnin laitos. Viitattu 17.10.2022 https://thl.fi/documents/920442/2816495/THL-Maarays_4-2021_Sote-tietojarj_Luokittelu-Sertifiointi.pdf/1d2fb82d-5bc1-e6b5-0bbc-803b220a138a?t=1638962140075.

THL 2021b. Määräys tietoturvasuunnitelmaan sisällytettävistä selvityksistä ja vaatimuksista. Terveyden ja hyvinvoinnin laitos. Viitattu 12.11.2022

https://thl.fi/documents/920442/2816495/THL_Maarays_3_2021_Tietoturva-suunnitelman_selvitykset_ja_vaatimukset.pdf/b4f17949-bace-b8d4-0cee-b215c6e5d372?t=1640009474365.

THL 2022. Määräykset. Terveyden ja hyvinvoinnin laitos. Viitattu 5.12.2022 https://thl.fi/fi/web/tiedonhallinta-sosiaali-ja-terveysalalla/maaraykset-ja-maarittelyt/maaraykset.

Traficom 2022. Kyberympäristön uhkataso on noussut – aktiviteetti Suomeakin kohtaan on lisääntynyt. Viitattu 6.12.2022 https://www.traficom.fi/fi/ajankohtaista/kyberympariston-uhkataso-noussut-aktiviteetti-suomeakin-kohtaan-lisaantynyt.

Traficomin julkaisuja 2/2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 19.11.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf.

Traficomin julkaisuja 12/2022. Toiminta kiristyshaittaohjelmatilanteessa – johdon ohje. Viitattu 20.11.2022 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toiminta%20kiristyshaittaohjelmatilanteessa%20-%20johdon%20ohje.pdf.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. 3. uudistettu laitos. Helsinki: Tammi.

Turvallisuuskomitea 2017. Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös. Viitattu 15.11.2022 https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/.

Turvallisuuskomitea 2022a. Toiminta ja tehtävät. Viitattu 14.10 https://turvallisuuskomitea.fi/turvallisuuskomitea/turvallisuuskomitea-toiminta-ja-tehtavat/.

Turvallisuuskomitea 2022b. Yhteiskunnan turvallisuusstrategia. Ennakointi ja varautuminen. Viitattu 20.11.2022 https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/ennakointi-ja-varautuminen/.

Tynkkynen O., Hietaniemi T., Haanperä, O. & Hakko, H. 2022. Energiakriisin kynnyksellä – mitä voimme oppia menneestä? Sitra. Viitattu 16.10.2022 https://www.sitra.fi/julkaisut/energiakriisin-kynnyksella-mita-voimme-oppia-menneesta/#tiivistelma.

VAHTI 2/2011. Johdon tietoturvaopas. Viitattu 7.12.2022 https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet/vahti-22011-johdon-tietoturvaopas.

VAHTI 3/2012. Teknisen ICT-ympäristön tietoturvataso-ohje. Viitattu 8.12.2022 https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_3_2012_pdf.pdf.

Valtioneuvosto 2019. Yhdenvertaisuus on taattava digitaalisessa Suomessa. Viitattu 5.12.2022 https://valtioneuvosto.fi/-/10623/yhdenvertaisuus-on-taattava-digitaalisessa-suomessa.

Valtioneuvosto 2022a. Uusi laki sääntelemään sosiaali- ja terveydenhuollon asiakastietojen käsittely. Sosiaali- ja terveysministeriö 27.10.2022. Viitattu 5.12.2022 https://valtioneuvosto.fi/-/1271139/uusi-laki-saantelemaan-sosiaali-ja-terveydenhuollon-asiakastietojen-kasittelya.

Valtioneuvosto 2022b. Valtioneuvostolta tukea yritysten tietoturvan kehittämiseen. Viitattu 27.12.2022 https://valtioneuvosto.fi/-/valtioneuvostolta-tukea-yritysten-tietoturvan-kehittamiseen.

Valtionvarainministeriö 2022. Palveluiden ja turvallisuuden ohjaus. Viitattu 8.12.2022 https://vm.fi/ohjaus.

Valvira 2015. Omavalvontasuunnitelma. Sosiaali- ja terveydenalan lupa- ja valvontavirasto. Viitattu 22.12.2022 https://www.valvira.fi/terveydenhuolto/yksityisen_terveydenhuollon_luvat/omavalvontasuunnitelma_2.

Valvira 2022a. Asiakastietolain mukaiset sosiaali- ja terveydenhuollon tietojärjestelmät. Sosiaali- ja terveydenalan lupa- ja valvontavirasto. Viitattu 17.10.2022 https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat.

Valvira 2022b. Ilmoita merkittävästä poikkeamasta. Sosiaali- ja terveydenalan lupa- ja valvontavirasto. Viitattu. 12.11.2022 https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat/ilmoita-poikkeamasta.

Valvira 2022c. Sosiaali- ja terveydenhuollon tietojärjestelmärekisteri. Sosiaali- ja terveydenalan lupa- ja valvontavirasto. Viitattu 5.1.2.2022 https://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat/sosiaali-ja-terveydenhuollon-tietojarjestelmarekisteri.

Vepsäläinen, P. & Tolonen, P. 2021. ISO 27001 Tietoturvallisuuden hallintajärjestelmän kypsyysarviointi. Tietoturvallisuuden hallintajärjestelmän kypsyysarviointi pohjana hallintajärjestelmän kehittämiselle. Huoltovarmuuskeskus. PowerPoint esitys. Viitattu 16.10.2022 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/iso-27001-tietoturvallisuuden-hallintajarjestelman-kypsyysarviointi.

Virranniemi, G. 2022. Korkeakouluille miljoonarahoitus kyberturvallisuuteen – ”Verkkopankkeja ei ryöstetä ja potilastietojärjestelmä toimii”, lupaa ministeri Honkonen. Yleisradio. Viitattu 23.12.2022 https://yle.fi/a/74-20009979.

Vuorinen, T. 2014. Strategiakirja – 20 työkalua. Helsinki: Talentum.

Williams, P. & Woodward, A. 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: Evidence and Research. Dovepress. Viitattu 7.12.2022 https://doi.org/10.2147/MDER.S50048.

Weber, K.& Kleine, N. 2020. Cybersecurity in Health Care. Teoksessa Cristensen, M., Gordjin, B., Loi, M. (toim.) The Ethics of Cybersecurity. Viitattu 7.12.2022 https://doi.org/10.1007/978-3-030-29053-5.

Zaboeva, C. 2020. IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain. Security Intelligence. Viitattu 19.11.2022 https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/.

Zhang, Y., Qui, M., Tsai, C-W., Hassan, M & Almari, A. 2017. Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. IEEE Systems Journal, 1 (88–95). Viitattu 15.11.2022 DOI: 10.1109/JSYST.2015.2460747.

Yleisradio 2022. Tietoturva-alan opiskelijoita ei valmistu riittävästi eikä koulutus vastaa työelämän tarpeita, kertoo yliopistotutkimus. Viitattu 23.12.2022 https://yle.fi/a/3-12637353.