Tampereen yliopisto

Auli Jukkola

KEINOJA LAAJAN ETÄTYÖN KYBERTURVALLISUUSUHKIEN HALLINTAAN ORGANISAATIOISSA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Toukokuu 2021

TIIVISTELMÄ

Auli Jukkola: Keinoja laajan etätyön kyberturvallisuusuhkien hallintaan organisaatioissa
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Toukokuu 2021

COVID-19-pandemian leviämisen ehkäisemiseksi asetettujen laajojen etätyösuositusten myötä etätyöstä tuli lyhyessä ajassa globaali ilmiö. Etätyöhön siirtyminen tuli organisaatioille nopealla aikataululla ja toi mukanaan myös erilaisia uhkia organisaatioiden kyberturvallisuuteen liittyen. Tämän tutkielman tarkoituksena on kirjallisuuskatsauksen avulla esittää keinoja organisaatioiden kyberturvallisuusuhkien hallintaan ja ennaltaehkäisemiseen laajoissa etätyötilanteissa. Tutkielmassa etätyötä tarkastellaan COVID-19-pandemian kontekstissa.

Kyberturvallisuusuhkien hallintakeinoja pohjustetaan tutkielmassa käsittelemällä etätyötilanteen kehittymistä ja sen mukana tulleita kyberturvallisuusuhkia. Tutkielmassa havaittiin säännöllisesti etätyötä tekevien osuudessa merkittävä kasvu heti pandemian alkuvaiheilla. Samanaikaisesti etätyötä tekemättömien ja satunnaisesti etätyötä tekevien osuudet laskivat. Myös kyberhyökkäykset yleistyivät pandemian aikana. Hyökkäystyypeistä erityisesti tietojenkalasteluhyökkäykset korostuivat. Pandemianaikaisissa kyberhyökkäyksissä hyödynnettiin myös tilannekohtaisia tekijöitä ja sosiaalisen manipuloinnin keinoja. Laajan etätyön kyberturvallisuusuhkien taas havaittiin liittyvän sekä tietoturvan että organisaation toiminnan vaarantumiseen. Yksi merkittävä tekijä kyberturvallisuusuhkien toteutumiselle on tutkielman mukaan työntekijöiden koulutuksen ja taitojen puute.

Tutkielman keskeisimpiä löydöksiä laajan etätyön kyberturvallisuusuhkien hallintaan organisaatioissa ovat turvallisen kyberympäristön ja tietoturvan varmistaminen sekä henkilöstön kouluttaminen ja yleisen kyberturvallisuustietoisuuden kasvattaminen. Turvallisen kyberympäristön varmistamisessa tärkeänä ilmenee kyberturvallisuuspolitiikan luominen etätyötilanteita varten. Toinen tärkeä aihe on verkon turvaaminen. Tietoturvan varmistamisessa korostuvat käytännöt varmuuskopioiden tekemiseen ja tiedostojen jakamiseen. Kirjallisuuskatsauksen tulosten perusteella voidaan myös todeta, että pelkästään teknisiä ratkaisuja ei nähdä riittävinä laajan etätyön kyberturvallisuusuhkien hallitsemiseksi. Teknisten ratkaisujen lisäksi organisaatioiden kyberturvallisuusuhkien hallintakeinoissa COVID-19-pandemian kontekstissa korostuvat yleisen kyberturvallisuustietoisuuden kasvattaminen ja kouluttaminen organisaation puolelta.

Avainsanat: COVID-19, etätyö, kyberturvallisuus, kyberturvallisuusuhka, kyberhyökkäys

Sisällysluettelo

1 Johdanto 1

2 Tutkimusmenetelmä 2

3 Keskeisimmät käsitteet 4

4 Laajan etätyötilanteen kehittyminen ja kyberturvallisuusuhat 5

4.1 Etätyöhön siirtyminen 5

4.2 Kyberhyökkäykset COVID-19-pandemian aikana 7

4.3 Laajan etätyön kyberturvallisuusuhkia organisaatioiden näkökulmasta 8

5 Laajan etätyön kyberturvallisuusuhkien hallinta organisaatioissa 10

5.1 Turvallisen kyberympäristön varmistaminen 10

5.2 Tietoturvan varmistaminen 12

5.3 Kouluttaminen ja yleisen kyberturvallisuustietoisuuden varmistaminen 13

6 Keskustelu 14

7 Yhteenveto 17

Lähdeluettelo 19

1 Johdanto

30. päivänä tammikuuta 2020 WHO (World Health Organization) julisti COVID-19-pandemian kansainväliseksi kansanterveysuhaksi (Public Health Emergency of International Concern, PHEIC) (THL, 2020). COVID-19-pandemia mullisti globaalisti työkenttää laajoilla etätyösuosituksilla (Herath & Herath, 2020), joiden pyrkimyksenä oli ehkäistä pandemian leviämistä. Tutkielmaa tehtäessä esimerkiksi Suomessa vallitsee toistaiseksi voimassa oleva valtakunnallinen etätyösuositus (STM, 2021). Etätyöhön siirtyminen tuli organisaatioille nopealla aikataululla ja toi mukanaan myös erilaisia uhkia liittyen organisaatioiden kyberturvallisuuteen.

Tämän tutkielman tarkoituksena on kirjallisuuskatsauksen avulla esittää keinoja organisaatioiden kyberturvallisuusuhkien hallintaan ja ennaltaehkäisemiseen laajoissa etätyötilanteissa. Tutkimuskysymykseksi lähteiden läpikäynnin jälkeen muodostui: ”Miten organisaatiot voivat hallita koronapandemian myötä laajentuneen etätyöskentelyn kyberturvallisuusuhkia?”. Kirjallisuuskatsauksen lähteistä myös tulevaisuuden työmuotojen kehittyminen laajan etätyöskentelyn myötä näkyi ajankohtaisena, joten kyberturvallisuusuhkien hallintaa pyritään peilaamaan myös pandemian jälkeiseen tilanteeseen.

Soni et al. (2020) kuvailevat kyberturvallisuutta jatkuvasti kehittyväksi kentäksi, jolla käydään toistuvasti kiistaa puolustajien ja hyökkääjien välillä. Pandemia pakotti organisaatiot siirtymään nopeasti etätyöskentelyyn, eikä vielä ole varmaa, milloin tilanne rauhoittuu tai tuleeko etätyöskentely jatkumaan laajemmassa mittakaavassa vielä pandemian jälkeisenäkin aikana. Tämän vuoksi organisaatioiden proaktiivinen työskentely etätyön kyberturvallisuuden varmistamiseksi on tärkeää nyt ja tulevaisuudessa.

Etätyötä ei kuvata tutkielmassa uutena ilmiönä, vaan sitä tarkastellaan erityisesti COVID-19-pandemian kontekstissa. Ennen pandemiaa etätyö on nähty ennemminkin yhtenä työn joustomuodoista (TTL, 2016). Tutkielmassa etätyöllä viitataan ansiotyöhön, jossa työskentely tapahtuu työpaikan ulkopuolella (Tilastokeskus). COVID-19-pandemian aikaista etätyötä kuvataan tutkielmassa laajana etätyönä.

Aiheen pohjustamiseksi tutkielmassa käsitellään laajan etätyötilanteen kehittymistä, kyberturvallisuusuhkia ja hyökkäysmuotoja sekä niiden esiintymistä COVID-19-pandemian aikana. Lisäksi tutkielmassa pohditaan aineiston tukemana

etätyön tulevaisuutta. Tutkielmasta on rajattu pois etätyötilanteeseen liittyvät maantieteelliset tai kansalliset eroavaisuudet, jotka voivat liittyä esimerkiksi valtioiden eri tilassa oleviin IT-infrastruktuureihin (Conger, 2020). Toimialakohtaisia eroja ei myöskään käsitellä erikseen tutkielmassa, vaan tarkoituksena on tarkastella laajan etätyön kyberturvallisuusuhkien hallintakeinoja organisaatioissa yleisellä tasolla.

Kirjallisuuskatsauksen perusteella keskeisiä keinoja etätyön kyberturvallisuus-uhkien hallintaan organisaatioissa erityisesti COVID-19-pandemian kontekstissa ovat turvallisen kyberympäristön varmistaminen, tietoturvan varmistaminen sekä henkilöstön kouluttaminen ja yleisen kyberturvallisuustietoisuuden kasvattaminen. Tietoturvan varmistamiseen kuuluvana on esitetty myös Lueckin (2020) 5-vaiheisesta suunnitelmasta (5 step plan) mukailtu etätyön vaikutustenarvioinnin prosessi.

Kandidaattitutkielmassa tutkimusmenetelmänä toiminutta kirjallisuuskatsausta käsitellään luvussa 2, jossa esitellään keskeisimmät lähteet ja hakusanat sekä käydään tarkemmin läpi tutkimusmetodia ja aineiston analysointimenetelmiä. Luvussa 3 määritellään keskeisimmät käsitteet ja niiden rooli tutkielmassa. Luvussa 4 pohjustetaan tutkielman aihetta käsittelemällä laajan etätyötilanteen kehittymistä, kyberhyökkäyksiä ja laajaan etätyöhön liittyviä kyberturvallisuusuhkia. Luku 5 on tutkielman varsinainen tulososio, jossa esitellään kirjallisuuskatsauksen varsinaisia tuloksia eli keinoja organisaatioiden kyberturvallisuusuhkien hallintaan ja ennaltaehkäisyyn laajoissa etätyötilanteissa. Näiden avulla pohjustetaan luvusta 6 löytyvää keskusteluosiota. Luvussa 6 pohditaan lyhyesti myös etätyön tulevaisuutta. Luvusta 7 löytyy tutkielman yhteenveto, jossa palataan tutkimuskysymykseen ja kootaan yhteen tutkielman keskeiset huomiot.

2 Tutkimusmenetelmä

Tutkimusmenetelmänä kandidaattitutkielmassa toimii kirjallisuuskatsaus, jota varten lähteitä etsittiin seuraavista tietokannoista: Science Direct, Computer Science Database (ProQuest), IEEE/IET Electronic Library sekä Tuni Andor. Hakujen edetessä tutkielman aiheen rajaamiseen kirjallisuuskatsauksen keskeisiksi hakulausekkeiksi muodostuivat ”remote work* AND COVID-19” ja ”remote work* AND cybersec*” sekä ”remote work* AND cybersec* AND COVID-19”. Hakuprosessissa huomioitiin myös etätyöhön viittaavat muut englanninkieliset termit kuten ”telework” ja ”distance work” sekä COVID-19-pandemiaan viittaavat eri kirjoitusasut. Valituilla hakulausekkeilla ja

helmenkasvatuksen avulla kuitenkin löydettiin tarvittava aineisto tutkielmaa varten. Rajauksena hauissa käytettiin vertaisarvioituja lehtiä sekä konferenssijulkaisuja. Haettaessa lähdeaineistoa hakulausekkeella ilman COVID-19-termiä rajattiin hakutuloksia relevantteihin vuosiin 2019 eteenpäin.

Tutkielmaan etsitystä aineistosta yhteensä 35 tekstiä tai muuta verkkolähdettä (21 tieteellistä artikkelia, 4 konferenssijulkaisua ja 10 muuta verkkolähdettä) valikoitui tarkemmin läpikäytävien joukkoon. Osa muista verkkolähteistä oli aiheen rajausta ja johdantoon tulevaa esittelyä varten olevia viranomaislähteitä, esimerkiksi Sosiaali- ja terveysministeriö (STM) sekä Terveyden ja hyvinvoinnin laitos (THL).

Seulontavaiheessa valitut tekstit luettiin huolellisesti läpi ja jokaisesta luetusta tekstistä tehtiin muistiinpanot lopullisen aineiston valintaa varten. Aineiston lopullinen valinta tapahtui lähteiden relevanttiuden perusteella, sillä muut rajaukset oli varmistettu jo hakuprosessissa. Seulonnan jälkeen varsinaiseen kirjallisuuskatsaukseen valittiin yhteensä 23 lähdettä, joista 12 on tieteellisiä artikkeleita ja 10 muita verkkolähteitä, lisäksi yksi tutkielman keskeisimmistä lähteistä on konferenssijulkaisu. Kirjallisuuskatsauksen keskeisimpiä lähteitä on kuvattu lyhyesti taulukossa 1.

Taulukko 1. Kirjallisuuskatsauksen keskeisimpiä lähteitä.

Otsikko	**Kirjoittaja(t) (vuosiluku)**	**Sisältö**
The Impact of the COVID-19 Pandemic on Information Systems Management	Conger, S. (2020)	Tutkimuksessa arvioidaan kuuden erityyppisen organisaation osalta COVID-19-pandemian vaikutuksia tietojärjestelmien johtamiseen.
Cyber security and the remote workforce	Curran, K. (2020)	Esittelee COVID-19-pandemian kontekstissa etätyön kyberturvallisuusuhkia ja niiden hallintakeinoja.
GDPR in the new remote-working normal	Lueck, M. (2020)	Esittelee keinoja GDPR:n noudattamiseen pandemian aikaisessa etätyötilanteessa. Artikkelissa esitellään myös etätyön vaikutustenarvioinnin prosessi.
Overcoming the security risks of remote working	Malecki, F. (2020)	Curranin (2020) artikkelin tavoin, artikkelissa esitellään pandemian kontekstissa laajaan etätyöhön liittyviä kyberturvallisuusuhkia sekä niiden konkreettisia hallintakeinoja.

The influence of the COVID-19 pandemic on the digital transformation of work	Nagel, L. (2020)	Artikkelissa tutkitaan, onko COVID-19-pandemia johtanut digitaaliseen muutokseen työpaikoilla.
A multi-level influence model of COVID-19 themed cybercrime	Naidoo, R. (2020)	Tutkimuksessa kehitetään monitasoinen vaikuttamismalli, jossa tutkitaan, miten verkkorikolliset käyttävät hyväksi COVID-19-pandemiaa.
Security vs. Flexibility: Striking a Balance in the Pandemic Era	Soni, V., Kukreja, D., & Sharma, D. (2020)	Julkaisussa kuvataan turvallisuus-kysymyksiä ja haasteita työntekijöille ja työnantajille etätyöhön liittyen. Julkaisussa korostetaan myös kyber-turvallisuusuhkia, jotka ovat syntyneet COVID-19-pandemian aikakaudella.
Analysis of cybersecurity standard and framework components	Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020)	Artikkelissa esitellään erityyppisiä kyberturvallisuus-standardeja ja -kehyksiä sekä niiden sisältämiä elementtejä.

3 Keskeisimmät käsitteet

Tutkielman keskeisimmiksi käsitteiksi muodostuivat COVID-19, etätyö, kyber-turvallisuus, tietoturva, kyberturvallisuusuhka ja kyberhyökkäys. Keskeisimmät käsitteet on kuvattu taulukossa 2, jossa määritellään jokainen käsite ja esitellään sen rooli tutkielman osalta. Tutkielmassa esiintyvät muut käsitteet määritellään ensimmäisen käyttökerran yhteydessä, jolloin esitetään myös mahdollinen alkuperäinen englanninkielinen termi.

Taulukko 2. Keskeisimmät käsitteet.

Käsite	**Määrittely**	**Rooli tutkielmassa**
COVID-19	WHO:n 11.3.2020 pandemiaksi julistama uuden koronaviruksen aiheuttama tauti (THL, 2020).	COVID-19- pandemia toimii kehyksenä tutkielmassa tarkasteltaviin etätyön kyberturvallisuusuhkien hallintakeinoihin.
Etätyö	Ansiotyö, jossa työskentely tapahtuu varsinaisen työpaikan ulkopuolella (Tilastokeskus).	Etätyötä tarkastellaan COVID-19-pandemian kontekstissa. Pandemian aikaista etätyötä kuvataan laajana etätyönä. Tekstissä käytetään myös muotoa etätyöskentely.

Kyberturvallisuus	Kyberturvallisuudella tarkoitetaan digitaalisen yhteiskunnan tai organisaation turvallisuutta sekä turvallisuuden vaikutusta toimintoihin (Kuntaliitto, 2021).	Kyberturvallisuutta tarkastellaan organisaation ja etätyön konteksteissa.
Tietoturva	Järjestelyt, joiden avulla varmistetaan tiedon luottamuksellisuus, eheys ja saatavuus (TEPA-termipankki).	Tietoturvaa tarkastellaan organisaation ja etätyön näkökulmasta.
Kyberturvallisuus-uhka	Kyberympäristöön kohdistuva mahdollinen haitallinen tapahtuma, joka vaarantaa toteutuessaan siihen liittyvän toiminnon. (Sanastokeskus TSK, 2018).	Tutkielmassa kyberturvallisuusuhalla tarkoitetaan organisaation näkökulmasta tarkasteltuna uhkaa, joka vaarantaa organisaation toiminnan. Kyberturvallisuusuhkia tarkastellaan tutkielmassa etätyön kontekstissa. Tietoturvaan liittyvät uhat ajatellaan osaksi kyberturvallisuusuhkia.
Kyberhyökkäys	Kyberympäristöön kohdistuva hyökkäys. Kyberhyökkäyksiin luetaan mukaan myös tietoverkon kautta tapahtuva toiminta, jolla pyritään vahingoittamaan tai käyttämään oikeudettomasti tietoverkkoa, tietojärjestelmää, laitteistoa tai dataa. (TEPA-termipankki).	Kyberhyökkäyksiä käsitellään organisaation näkökulmasta. Myös COVID-19-teemaisia hyökkäyksiä esitellään tutkielmassa.

4 Laajan etätyötilanteen kehittyminen ja kyberturvallisuusuhat

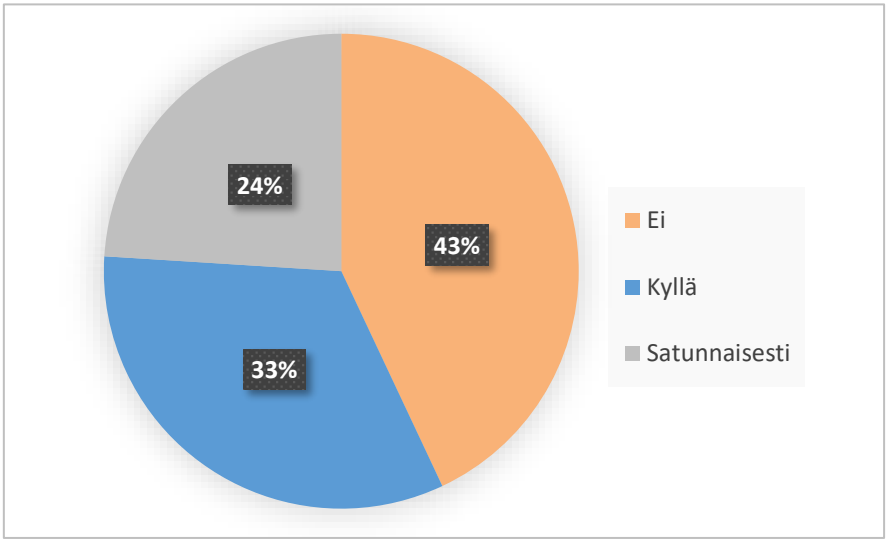
Tässä luvussa tarkastellaan COVID-19-pandemian myötä laajentuneen etätyön kyberturvallisuusuhkia organisaatioissa. Luku on jaettu kolmeen eri kohtaan. Kohdassa 4.1 esitellään COVID-19-pandemian tuomaa muutosta organisaatioiden toimintaympäristöön etätyöhön siirtymisen myötä. Kohta 4.2 käsittelee erilaisia kyberhyökkäysten muotoja, tuoden esille myös COVID-19-teemaisia hyökkäyksiä ja niiden ilmenemistä heti pandemian alkuvaiheilta. Kohdassa 4.3 tuodaan esille laajaan etätyöhön liittyviä kyberturvallisuusuhkia organisaation näkökulmasta.

4.1 Etätyöhön siirtyminen

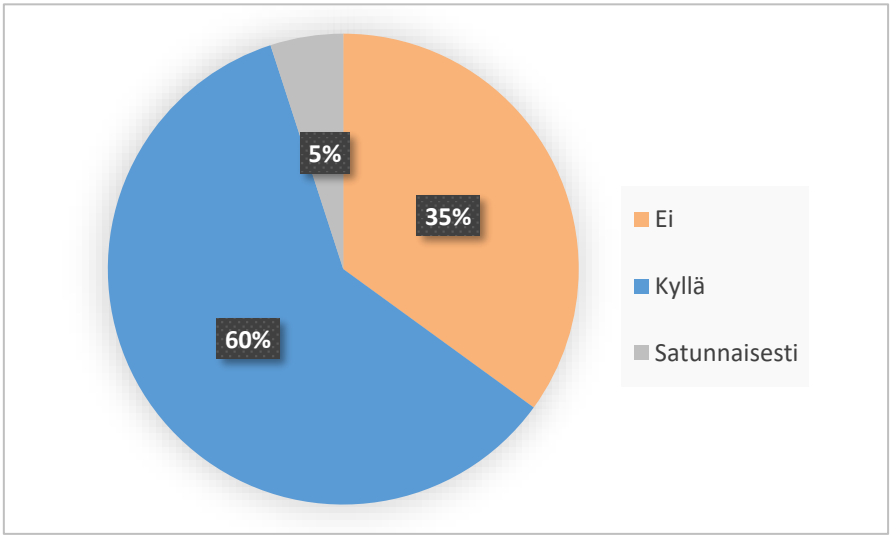
COVID-19-pandemian leviämisen ehkäisemiseksi asetettujen suositusten myötä etätyöstä tuli lyhyessä ajassa globaali ilmiö. Toimintaympäristön muutos koski miljoonia ihmisiä ympäri maailman (Malecki, 2020) ja nopeasti etätyöstä tuli niin sanotusti uusi normaali työnteolle (Conger, 2020; Herath & Herath 2020; Lueck, 2020; Soni et al., 2020.). Etätyöhön siirtymisen mittakaavaa havainnollistetaan Nagelin (2020)

tutkimuksen tuloksilla, jotka pohjautuvat pandemian alkupuolella Amazon Mechanical Turkin kautta toteutettuun kyselyyn.

Nagelin (2020) suorittaman tutkimuksen mukaan ennen pandemiaa etätöitä teki säännöllisesti 33 % työvoimasta. Ajoittain etätyötä teki 24 %, jolloin etätyötä tekemättömän työvoiman osuus oli 43 %. Pandemian puhjettua etätyötä tekevien tilanne muuttui seuraavasti: säännöllistä etätyötä teki 60 % ja ajoittaista etätyötä 5 %. Etätyötä tekemättömän työvoimaan osuus oli tällöin 35 %. Nagelin (2020) tutkimuksen tulokset on havainnollistettu kuvissa 1 ja 2.



Kuva 1. Etätyötä tekevien osuudet ennen COVID-19-pandemiaa. Mukaillen Nagel (2020).



Kuva 2. Etätyötä tekevien osuudet COVID-19-pandemian alettua. Mukaillen Nagel (2020).

Nagel (2020) mainitsee tutkimuksensa tulosten rajoitteeksi sen, että netissä toteutetun kyselyn vuoksi vastaajilla on voinut olla taipumusta digitaaliseen työskentelyyn. Tämän lisäksi tutkimus on suoritettu pandemian alkuvaiheessa, jolloin pandemiatilanne oli poikkeava eri maiden välillä (Nagel, 2020). Tulokset ovat kuitenkin riittäviä havainnollistamaan etätyöhön siirtymisen laajuutta pandemian alkuvaiheilla.

Laajaa ja nopeaa siirtymistä etätyöhön tukivat myös erilaiset teknologiset mahdollisuudet (Furnell & Shah, 2020; Herath & Herath, 2020). Esimerkiksi etäkommunikointia varten otettiin käyttöön kolmannen osapuolen tarjoamia sovelluksia (Soni et al., 2020), kuten Zoom, MS Teams ja Skype (Conger, 2020). Lisäksi turvallisten yhteyksien varmistamiseksi useissa organisaatioissa otettiin käyttöön VPN-yhteydet (virtual private network) (Conger, 2020). VPN, suomennettuna virtuaalinen yksityisverkko, tarkoittaa suojattua verkkoyhteyttä, jossa tietoliikenne on salattua, mutta päätelaitteet toimivat kuitenkin samalla tavalla kuin suljetussa lähiverkossa (TEPA-termipankki).

Congerin (2020) tutkimuksen mukaan organisaatiot, joissa etätyön tekeminen oli tuttua jo ennen pandemiaa, saivat etätyörutiinit toimimaan nopeammin verrattuna organisaatioihin, joissa etätyötä ei ennen pandemiaa ollut tehty. Toimintaympäristön muutos ja mahdollisten uusien teknologien käyttöönotto tapahtuivat nopealla aikataululla (Herath & Herath, 2020) – tämän myötä organisaatioissa ilmeni myös uusia kyberturvallisuusuhkia (Naidoo, 2020; Newlands et al., 2020).

4.2 Kyberhyökkäykset COVID-19-pandemian aikana

Etätyöhön siirtyminen loi organisaatioiden toimintaan uusia haavoittuvuuksia (Malecki, 2020), joita myös kyberrikolliset alkoivat nopeasti käyttää hyväkseen (Naidoo, 2020). Kyberhyökkäyksiin liittyvien uhkien merkitys organisaation toimintakyvylle korostuu, sillä kyberhyökkäykset yleistyivät merkittävästi COVID-19-pandemian aikana (Malecki, 2020). Yleisimpiä kyberrikollisten käyttämiä hyökkäysmuotoja ovat tietojenkalastelu-hyökkäykset (phishing attacks), haittaohjelmat (malware), kiristysohjelmat (ransomware) ja palvelunestohyökkäykset (denial-of-service, DoS) (Malecki, 2020; Naidoo, 2020).

Tietojenkalasteluhyökkäyksessä hyökkäyksen kohteita lähestytään sähköpostitse luotettavaa lähdettä jäljitellen; hyökkäyksessä hyödynnetään usein lähdettä jäljittelevän verkkosivun mallia (Naidoo, 2020). Haittaohjelmat, esimerkiksi virukset, aiheuttavat epätoivottuja tapahtumia tietokoneella (TEPA-termipankki). Kiristysohjelmalla taas

viitataan tietokoneeseen, esimerkiksi sähköpostin liitetiedostona, tulevaan haitta-ohjelmaan, jonka tarkoituksena on salata tietokoneella olevat tiedot ja vaatia lunnaita tietojen vapauttamisesta (TEPA-termipankki). Palvelunestohyökkäyksissä estetään käyttäjän pääsy haluttuun kohteeseen (Zaharia, 2020), tällöin hyökkäyksen kohteena oleva palvelu voidaan lamaannuttaa esimerkiksi suurella palvelupyyntömäärällä (TEPA-termipankki).

Yleisimmistä hyökkäyksistä erityisesti tietojenkalasteluhyökkäykset ovat korostuneet pandemian aikana (Naidoo, 2020; Shi, 2020). Myös COVID-19-teemaiset hyökkäykset ovat yleistyneet. Shin (2020) mukaan esimerkiksi COVID-19-teemaiset kohdennetut tietojenkalasteluhyökkäykset (spear-phishing attack) yleistyivät tammikuusta 2020 alkaen. Kohdennetuilla tietojenkalasteluhyökkäyksillä tarkoitetaan tietylle kohderyhmälle osoitettua tietojenkalasteluhyökkäystä. Tämä eroaa tyypillisistä tietojenkalasteluhyökkäyksistä, jotka osoitetaan yleensä laajoille kohderyhmille (Ani, 2020). Kohdennetuissa COVID-19-teemaisissa tietojenkalasteluhyökkäyksissä havainnoitiin 667 %:n nousu helmikuulta 2020 maaliskuulle 2020 (Shi, 2020).

Soni et al. (2020) mukaan kyberturvallisuutta voidaan kuvata jatkuvasti kehittyvänä kenttänä, jolla käydään toistuvasti kiistaa puolustajien ja hyökkääjien välillä. Organisaatioiden turvallisen toiminnan kannalta haasteena on myös se, että puolustusteknologioiden kehittyessä samanaikaisesti myös hyökkääjät löytävät uusia keinoja tavoitteidensa saavuttamiseksi (Soni et al., 2020). Lisäksi Naidoo (2020) korostaa, että kyberhyökkäysprosesseissa hyödynnetään myös tilannekohtaisia tekijöitä, kuten COVID-19-pandemiaa.

Naidoon (2020) mukaan tilannekohtaisten tekijöiden avulla valitaan hyökkäystapa ja hyökkäyksen kohteet, joihin voidaan hyödyntää lisäksi käyttäjän manipuloinnin (social engineering) keinoja. Esimerkiksi pandemian aikaan on ilmennyt etätyöntekijöihin kohdistuneita hyökkäyksiä, joissa kohdetta lähestytään esiintymällä etätyössä tarvittavien teknologiapalveluiden edustajina (Naidoo, 2020).

4.3 Laajan etätyön kyberturvallisuusuhkia organisaatioiden näkökulmasta

COVID-19-pandemian aikaisten etätyöskentelyyn liittyvien kyberturvallisuusuhkien voidaan ajatella poikkeavan organisaation normaaliin toimintaympäristöön kohdistuvista uhkista, sillä useat organisaatiot eivät olleet valmistautuneita äkilliseen toimintaympäristön muutokseen (Soni et al., 2020). Nopealla aikataululla toteutunutta laajaa etätyöhön siirtymistä voidaankin pitää merkittävänä toimintaympäristön muutoksena

usealle organisaatiolle (Furnell & Shah, 2020; Herath & Herath, 2020). Tutkielmassa laajaan etätyöhön liittyvällä kyberturvallisuusuhalla viitataan etätyötilanteesta johtuvaan mahdollisesti toteutuvaan haitalliseen tapahtumaan, joka kohdistuu organisaation kyberympäristöön ja toteutuessaan vaarantaa organisaation toiminnan. Syafrizal et al. (2020) mukaan kyberympäristö pitää sisällään toimintaympäristön käyttäjät, verkon infrastruktuurin, laitteiston ja ohjelmistot, prosessit ja palvelut sekä kyberympäristössä olevan tiedon.

Merkittäviä COVID-19-pandemian aikaiseen etätyöhön liittyviä kyberturvallisuus-uhkia organisaatioissa ovat tietoturvaan liittyvät uhat, sillä yhtenä organisaatioiden tärkeimmistä resursseista voidaan pitää organisaatiossa olevaa tietoa (Soni et al., 2020). Tietoturvaan liittyvät uhat voivat laajoissa etätyötilanteessa johtua esimerkiksi uusien teknologioiden nopeasta käyttöönotosta (Newlands et al., 2020; Soni et al., 2020), turvattomista verkkoyhteyksistä (Curran, 2020; Naidoo 2020), työntekijöiden käytössä olevista vaihtelevista laitetyypeistä (Naidoo, 2020; Soni et al., 2020), organisaatioiden puutteellisista kyberturvallisuuspolitiikoista (Soni et al., 2020), esimerkiksi tiedon jakamisen suhteen, sekä pandemian aikana yleistyneistä kyberhyökkäyksistä (Curran, 2020; Naidoo, 2020; Soni et al., 2020). Erityisesti COVID-19-pandemian aikana yleistyneet kyberhyökkäykset ovat uhka niin organisaation toiminnalle kuin organisaation tiedon turvaamiselle (Furnell & Shah, 2020; Naidoo, 2020).

Tietoturvaan kohdistuvat uhat vaarantavat organisaatiossa olevan tiedon luottamuksellisuuden, eheyden ja saatavuuden (Syafrizal et al., 2020). Organisaation tietoihin voidaan lukea mukaan myös työntekijöiden organisaatiossa käsiteltävät henkilötiedot – uhkana henkilötietojen käsittelyssä on esimerkiksi yksityisyyden suojan vaarantuminen (Lueck, 2020). Esimerkkinä organisaation tiedon luottamuksellisuuden ja yksityisyyden suojan vaarantumisesta voidaan käyttää etäkokoustyökalujen käyttöön liittyvää ”Zoombombing” -ilmiötä, joka yleistyi pandemian alkupuolella (Curran, 2020). ”Zoombombing” (Newlands et al., 2020) tai ”conference bombing” (Curran, 2020) viittaa tapahtumaan, jossa kolmas osapuoli kaappaa etäkokouksen hallintaansa tai liittyy luvattomasti mukaan kokoukseen (Newlands et al., 2020).

Kyberhyökkäysten onnistuminen voisi aiheuttaa organisaatiolle tietoturvaan liittyvien uhkien lisäksi myös toimintaan kohdistuvia uhkia, jos esimerkiksi hyökkäyksen kohteeksi joutuva työntekijä estyisi tekemästä työtään. Lisäksi organisaation toimintaa rajoittavat tai toiminnan kokonaan estävät uhat voivat laajoissa etätyötilanteessa liittyä puutteellisiin verkkoyhteyksiin, laitteiden toimimattomuuteen tai esimerkiksi ongelmiin

organisaation datan tavoittamisessa. Yhtenä kyberturvallisuusuhkana voidaan pitää myös mahdollista omien laitteiden käyttämistä etätyössä. Tällä viitataan BYOD-ilmiöön (Bring Your Own Device), jossa työntekijöillä on henkilökohtaisten laitteidensa kautta pääsy organisaation verkkoon ja dataan. (Soni et al., 2020)

Myös työntekijöiden koulutuksen ja taitojen puute voi olla merkittävä tekijä kyberturvallisuusuhkien toteutumisessa, sillä COVID-19-pandemian aikaisen etätyön alkaessa usealla organisaatiolla oli päätavoitteena saada työskentely jatkumaan nopeasti ja tehokkaasti (Soni et al., 2020). Samanaikaisesti tietoisuus turvallisesta toiminnasta etätyötilanteissa oli puutteellista (Naidoo, 2020), organisaatioissa ilmeni siis tarvetta koulutukselle. Koulutuksen puutteen voidaan ajatella COVID-19-pandemian aikaisessa etätyössä liittyvän myös siihen, etteivät organisaatiot tai työntekijät olleet valmistautuneita pandemian tuomaan äkilliseen toimintaympäristön muutokseen (Soni et al., 2020).

5 Laajan etätyön kyberturvallisuusuhkien hallinta organisaatioissa

Tässä luvussa tarkastellaan laajaan etätyöhön liittyvien kyberturvallisuusuhkien hallintakeinoja organisaatioissa. Luku on jaettu kolmeen eri kohtaan. Kohdassa 5.1 käsitellään turvallisen kyberympäristön varmistamista, joka toimii lähtökohtana laajaa etätyötä koskevien kyberturvallisuusuhkien hallinnassa. Kohdassa 5.2 käydään läpi tietoturvaa ja esitellään lyhyesti etätyöhön liittyvää tietosuojan vaikutustenarviointia. Kohta 5.3 tuo esille organisaation jäsenten kouluttamisen tärkeyttä kyberturvallisuusasioiden osalta.

5.1 Turvallisen kyberympäristön varmistaminen

Turvallisen kyberympäristön varmistaminen korostuu laajoissa etätyötilanteissa, kun organisaation toiminta tapahtuu normaalin, turvallisen toimintaympäristön ulkopuolella (Furnell, 2020; Naidoo, 2020). Turvallisen kyberympäristön varmistamiseksi organisaatiolla tulisi olla selkeä kyberturvallisuuspolitiikka etätyötilanteita varten; valmiiden toimintatapojen avulla organisaation on mahdollista varautua paremmin äkillisiinkin muutoksiin (Lueck, 2020).

Organisaation kyberturvallisuuspolitiikka voi pitää sisällään sekä organisaation puolesta toteutettavia toimia että yksittäiseen työntekijään kohdistuvia toimintaohjeita.

Esimerkiksi organisaation puolelta voidaan teknisten ratkaisujen avulla määrittää aika-katkaisu etätyössä käytettävien sovellusten istunnoille. Organisaation kyber-turvallisuuspolitiikkaan voidaan myös määritellä tarvittavat pakolliset koulutukset etätyön kyberturvallisuuteen liittyen. Yksittäiseen työntekijään kohdistuvia ohjeita voivat taas olla esimerkiksi organisaation määrittelemät salasanakäytännöt sekä sovellusten päivittäminen uuden version ilmestyessä. Etätyötilanteita koskevan kyberturvallisuus-politiikan ja toimintaohjeiden tulisi olla selkeitä jokaiselle organisaation jäsenelle. Kyberturvallisuuspolitiikan luomisen ja selkeiden toimintatapojen lisäksi Soni et al. (2020) korostavat vahvan turvallisuuskulttuurin luomista sekä henkilökunnan kouluttamista turvallisen toimintaympäristön varmistamiseksi. (Soni et al., 2020)

Yhtenä avaintekijänä turvallisen kyberympäristön varmistamisessa voidaan Syafrizal et al. (2020) mukaan pitää organisaation toiminnan turvaamista kyber-turvallisuusstandardien (cyber security standards) ja kyberturvallisuuskehysten (cybersecurity frameworks) avulla. Standardeilla viitataan joukkoon teknisiä sääntöjä ja käytäntöjä, joiden tavoitteena on vähentää kyberympäristöön kohdistuvia riskejä sekä ehkäistä tai lieventää kyberhyökkäysten onnistumista (Syafrizal et al., 2020). Esimerkkeinä kyberturvallisuusstandardeista voidaan mainita ISO/IEC 27032:2012 ja NIST SP 800 (Syafrizal ei al., 2020). Standardien noudattamisen voidaan ajatella tukevan turvallista toimintaa myös etätyötilanteissa. Kyberturvallisuuskehyksellä taas tarkoitetaan joukkoa suuntaviivoja tai ohjeistuksia, joiden avulla organisaatiot voivat paremmin tunnistaa, puolustautua ja reagoida mahdollisiin kyberhyökkäyksiin (Syafrizal et al., 2020).

Lisäksi Soni et al. (2020) korostavat kyberturvallisuuden merkityksen ymmärtämistä tärkeänä lähtökohtana laajan etätyön turvaamiselle - tässä ensimmäisenä askeleena on turvallisen verkon varmistaminen. Etäyhteyksissä tulisi suosia vahvoja VPN-yhteyksiä (Malecki, 2020), sillä VPN-yhteyksien avulla on mahdollista turvata datan siirto etäyhteyksistä organisaation omiin järjestelmiin (Curran, 2020). VPN-yhteyden käyttäminen tulisikin ottaa osaksi organisaation etätyötä koskevia toimintatapoja.

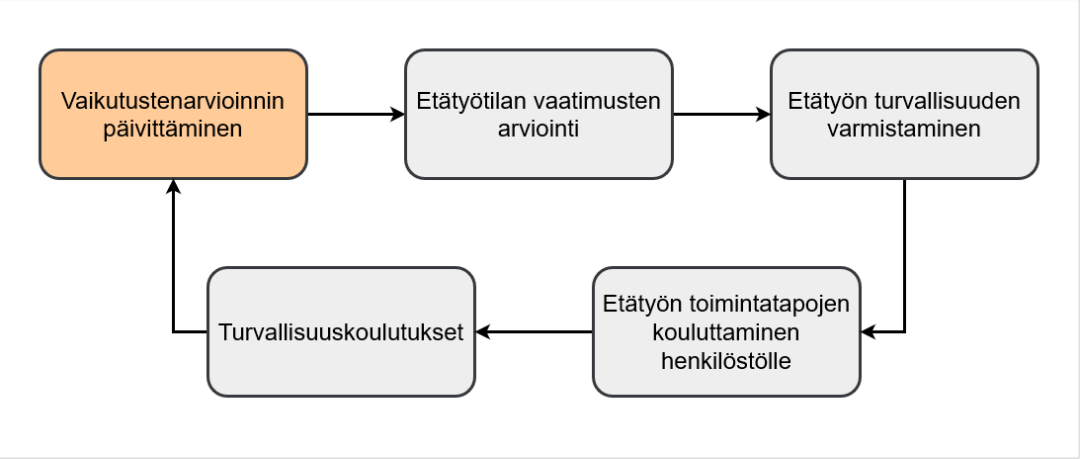
Verkon turvaamiseen liittyy myös etätyössä käytettävien laitteiden suojausten varmistaminen (Malecki, 2020), esimerkiksi virustentorjuntaohjelmat, palomuurin ja laitteiden salausten tulisi olla ajan tasalla (Curran, 2020). Lisäksi organisaation järjestelmiin kirjauduttaessa tulisi ottaa käyttöön kaksivaiheinen (two-factor) (Furnell & Shah, 2020) tai monivaiheinen tunnistautuminen (multi-factor authentication) (Soni et al.,

2020). Organisaation tulisi myös varmistaa riittävä tekninen osaaminen organisaation sisällä (Soni et al., 2020), sillä etätyötilanteissa yleinen kyberturvaosaaminen ja IT-toimintojen tärkeys korostuu. Erityisesti etätyötilanteissa henkilökuntaa tulisi rohkaista hyödyntämään organisaation IT-toimintojen ammattitaitoa, jotta mahdolliset tekniset ongelmat saataisiin ratkaistua nopeasti ja turvallisesti (Malecki, 2020).

5.2 Tietoturvan varmistaminen

Laajoissa etätyötilanteissa myös organisaation tietoturvan varmistaminen on tärkeää, sillä Soni et al. (2020) kuvaavat organisaatiossa olevaa tietoa yhdeksi sen tärkeimmistä resursseista. Yksi tärkeimmistä tekijöistä tietoturvan varmistamiseksi on säännöllisestä varmuuskopioinnista huolehtiminen (Malecki, 2020; Soni et al., 2020). Varmuuskopioinnilla on suuri merkitys sekä kiristysohjelmahyökkäyksiä ajatellen (Soni et al., 2020) että etätyöntekijöiden toiminnan kannalta, jos esimerkiksi etätyössä käytettävissä laitteissa ilmenisi ongelmia (Malecki, 2020). EU:n kansalaisten henkilötietojen kanssa työskenneltäessä tulee ottaa huomioon myös EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR) (Lueck, 2020; Newlands et al., 2020). Myös toimintatavat tiedon jakamiseen ja säilyttämiseen tulisi selkeyttää, jotta voidaan ehkäistä tietovuotoja ja mahdollisia hyökkäyksiä, joissa käytetään kiristysohjelmia (Curran, 2020). Voidaankin ajatella, että myös tietoturvaa koskevat asiat tulisi määritellä mukaan organisaation kyberturvallisuuspolitiikkaan.

Etätyötilanteita varten myös henkilötietojen käsittelyä koskeva tietosuojan vaikutustenarviointi (data protection impact assessments, DPIA) tulisi päivittää (Lueck, 2020). Vaikutustenarvioinnissa tunnistetaan, arvioidaan ja hallitaan henkilötietojen käsittelyyn liittyviä riskejä (Tietosuojavaltuutettu). Prosessina vaikutustenarvioinnin tulisi olla jatkuva kehä eikä jäädä vain yhteen arviointikertaan (Lueck, 2020). Lueck (2020) on esittänyt etätyötilanteita varten tehtävälle vaikutustenarvioinnille 5 kohdan suunnitelman, josta on esitetty mukaelma kuvassa 3.



Kuva 3. Etätyön vaikutustenarvioinnin prosessi. Mukaillen Lueck (2020).

Etätyön vaikutustenarvioinnin ensimmäisessä vaiheessa tehdään vaikutustenarvioinnin päivittäminen, jossa tarkastellaan ensin uuden toimintaympäristön vaikutusta tietoturvaan sekä käydään läpi henkilötietoja etätyössä käsittelevät henkilöt. Ensimmäisessä vaiheessa myös kategorisoidaan riskit henkilötietojen käsittelyyn liittyvät riskit. Tämän jälkeen tarkastellaan tiedon fyysistä turvallisuutta etätyötilassa. Tässä vaiheessa huomioidaan myös tarve lukittavalle työhuoneelle tai jopa videovalvonnalle erittäin arkaluontoisen datan käsittelyyn liittyen. Kolmannessa vaiheessa varmistetaan etätyölaitteiden ja yhteyksien riittävä tekninen turvallisuus. Neljännessä vaiheessa varmistetaan organisaation jäsenten tietoisuus toimintatavoista etätyötilanteissa. Vaikutustenarvioinnin viimeisessä vaiheessa keskitytään etätyöntekijöiden turvallisuuskoulutukseen, jossa käydään läpi työntekijän turvallisuusvastuita. (Lueck, 2020)

5.3 Kouluttaminen ja yleisen kyberturvallisuustietoisuuden varmistaminen

Luottamalla pelkästään teknisiin ratkaisuihin ei välttämättä voida taata organisaation kyberturvallista toimintaa (Ani et al., 2020). Tätä voidaan peilata myös turvalliseen kyberympäristöön laajoissa etätyötilanteissa, sillä yksi tapa ehkäistä organisaation kyberturvallisuusuhkia on Ani et al. (2020) mukaan yleisen kyberturvallisuustietoisuuden parantaminen ja kouluttamiseen panostaminen.

Ani et al. (2019) ajattelevat organisaation olevan yhtä vahva kuin sen heikoin lenkki, tässä he korostavat organisaation vastuuta kyberturvallisuustietoisuuden kasvattamisessa. Tunnistamalla henkilöstön kyberturvallisuusheikkouksia sekä osaamis- ja koulutustarpeita voidaan koulutuksia kohdentaa paremmin (Ani et al., 2020). Myös

Furnell & Shah (2020) korostavat organisaatioiden vastuuta kouluttamisessa. Lisäksi he huomioivat koulutuksen tarpeen organisaatiossa etätyötilanteita varten luotavan kyberturvallisuuspolitiikan osalta. Tämä korostuu myös COVID-19-pandemian aiheuttamassa etätyötilanteessa, sillä työskennellessään turvallisessa kotiympäristössä perinteisen työympäristön sijaan saattavat työntekijät tuntea itsensä vähemmän sitoutuneiksi työpaikan toimintapolitiikkaan (Furnell & Shah, 2020).

Kyberturvallisuuskoulutusta voidaan tukea myös kyberturvallisuuskehysten avulla (Syafrizal et al., 2020). Esimerkiksi NICE:n (the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework) tarkoituksena on luoda kestävää koulutusta sekä työntekijöiden kehittämisohjelmia ja kasvattaa tietoisuutta kyber-turvallisuudesta (Syafrizal et al., 2020).

Kyberturvallisuuskoulutusten osalta on tärkeää huomioida myös se, että kyber-hyökkäyksissä hyödynnetään usein inhimillisiä heikkouksia teknisten ratkaisujen päihittämisen sijaan (Ani et al., 2019). Tämä korostuu etätyötilanteissa, kun työtä ei tehdä organisaation normaalissa toimintaympäristössä, sillä siirtyminen etätyöhön on suuri muutos monille työntekijöille ja tuo mukanaan myös uusia turvallisuushaavoittuvuuksia (Naidoo, 2020). Lisäksi Naidoon (2020) mukaan alan ammattilaiset tiedostavat ja myöntävät inhimillisten tekijöiden olevan edelleen heikon lenkki kyberhyökkäyksissä.

Kyberhyökkäyksistä erityisesti etätyöntekijöihin kohdistetut tietojenkalastelu-hyökkäykset ovat korostuneet pandemian aikana ja myös muissa hyökkäyksissä on ollut kasvua (Soni et al., 2020). COVID-19-pandemiaa on hyödynnetty hyökkäyksissä myös tilannekohtaisena tekijänä (Naidoo, 2020; Soni et al., 2020). Myös Malecki (2020) korostaa, että organisaatioiden olisi tärkeää panostaa työntekijöiden koulutuksiin, jotta kyberhyökkäyksiä voitaisiin paremmin tunnistaa ja torjua.

6 Keskustelu

Kirjallisuuskatsauksen perusteella keskeisiä keinoja etätyön kyberturvallisuusuhkien hallintaan organisaatioissa erityisesti COVID-19-pandemian tilanteeseen viitaten ovat turvallisen kyberympäristön varmistaminen, tietoturvan varmistaminen sekä henkilöstön kouluttaminen ja yleisen kyberturvallisuustietoisuuden kasvattaminen. Kirjallisuus-katsauksen keskeisimmät tulokset on koottu taulukkoon 3. Taulukossa tulokset on lajiteltu löydösten mukaisesti kolmeen kategoriaan, joista jokaisesta löytyy kategoriaan

kuuluvia keinoja etätyön kyberturvallisuusuhkien hallintaan organisaatioissa. Myös kunkin kategorian lähteet löytyvät taulukosta.

Taulukko 3. Keinoja laajan etätyön kyberturvallisuusuhkien hallintaan.

Kategoria	**Keinoja**	**Lähteet**
Turvallisen kyberympäristön varmistaminen	Etätyötä koskevan kyberturvallisuuspolitiikan luominen, kyberturvallisuus-standardit ja -kehykset, verkon turvaaminen (VPN) ja työntekijöiden ohjeistaminen.	Curran, 2020; Furnell & Shah, 2020; Malecki, 2020; Soni et al., 2020; Syafrizal et al., 2020.
Organisaation tietoturvan varmistaminen	Säännölliset varmuuskopioinnit, GDPR:n noudattaminen, tiedon jakaminen / säilyttäminen, tietosuojan vaikutustenarviointi (DPIA).	Curran, 2020; Lueck, 2020; Malecki, 2020; Newlands et al., 2020; Soni et al., 2020.
Kouluttaminen ja kyberturvallisuustietoi suuden kasvattaminen	Heikkouksien sekä osaamis- ja koulutustarpeen tunnistaminen, organisaation kyberturvallisuuspolitiikan tuominen henkilöstön tietoon, tietoisuus kyberhyökkäyksistä ja niiden keinoista.	Ani et al., 2020; Furnell & Shah, 2020; Malecki, 2020; Naidoo, 2020; Soni et al., 2020; Syafrizal et al., 2020.

Kirjallisuuskatsauksen tulosten perusteella COVID-19-pandemian kontekstissa etätyön kyberturvallisuusuhkissa korostuu yleisen kyberturvallisuustiedon ja koulutuksen tärkeys. Pelkästään teknisiä ratkaisuja ei nähdä riittävinä kyberturvallisuusuhkien torjumiseksi. On siis tärkeää huomioida teknisen osaamisen lisäksi yleisen kyberturvallisuustietoisuuden tarve organisaatioissa, sillä esimerkiksi kyberhyökkäykset koettelevat sekä teknisiä että inhimillisiä haavoittuvuuksia (Naidoo, 2020).

Laajoihin etätyötilanteisiin liittyvää kyberturvallisuusuhkien hallintaa ei kuitenkaan voida organisaatioissa sysätä ainoastaan IT-alan ammattilaisten vastuulle, vaan sitä olisi tärkeää ajatella jokaisen etätyöntekijän oikeutena. Yleisen kyberturvallisuustietoisuuden kasvattamisen ja kouluttamisen avulla voitaisiin mahdollistaa turvallisempi toimintaympäristö jokaiselle. Tällöin olisi mahdollista myös ennaltaehkäistä kyberhyökkäysten onnistumista ja organisaatioiden toiminnan tai tiedon vaarantumista, sillä heikoimpana lenkkinä kyberhyökkäyksissä ovat usein inhimilliset tekijät (Naidoo, 2020).

Myös Naidoon (2020) huomiota tilannekohtaisen tekijöiden hyödyntämisestä COVID-19-pandemian aikaisissa kyberhyökkäyksissä voidaan pitää merkittävänä organisaatioiden kyberturvallisuuden kannalta, sillä Soni et al. (2020) mukaan,

ymmärtämällä vallitsevia kyberturvallisuushaasteita on organisaatioiden mahdollista varautua paremmin myös tuleviin uhkiin. Voidaankin ajatella, että hyödyntämällä teknisiä ratkaisuja ja samanaikaisesti kasvattamalla yleistä kyberturvaosaamista voidaan paremmin ennaltaehkäistä ja torjua laajoihinkin etätyötilanteisiin kohdistuvia kyberturvallisuusuhkia. Tätä tukee myös Naidoon (2020) näkemys, jonka mukaan käyttämällä ennakoivia teknologiaan perustuvia vastatoimia ja kasvattamalla turvallisuustietoisuutta voidaan ehkäistä COVID-19-pandemiaan liittyvän mahdollisten kyberhyökkäysten seuraavan aallon vaikutuksia.

Tutkielman tulosten kannalta yksi rajoittava tekijä on aiheen tuoreus. Tämän lisäksi lähdeaineisto on pyritty rajaamaan ainoastaan COVID-19-pandemiaan liittyviin julkaisuihin hakusanojen ja aikavälin rajauksen perusteella. On hyvä huomioida, että neljä tutkielman lähteistä on Computer Fraud & Security -lehden artikkeleita. Etätyöhön liittyvät julkaisut ovat COVID-19-pandemian kontekstissa olleet ajankohtaisia aiheita lehdessä. Lehti on Julkaisufoorumin luokituksen mukaan luokkaa 1 = perustaso, mutta lehti ei kuitenkaan ole vertaisarvioitu (JUFO, 2021). Artikkelit on kuitenkin valittu tutkielman lähteiksi aiheen relevanttiuden vuoksi. Computer & Fraud -lehden artikkelit eivät kuitenkaan ole ainoita tutkielman keskeisimpiä lähteitä.

Edellä mainittujen rajoitteiden lisäksi on hyvä huomioida, ettei pandemiatilanteesta poikkeavaa etätyön kyberturvallisuutta ole tarkasteltu tutkielmassa. COVID-19-pandemiaan liittyvän laajan etätyön kyberturvallisuusuhkien ja niiden hallintakeinojen voidaan kuitenkin ajatella poikkeavan niin sanotusta normaalista etätyötilanteesta, sillä etätyöntekijöiden määrä kasvoi merkittävästi pandemian aikana. Tulevaisuudessa olisikin mielenkiintoista tutkia tarkemmin millä tavalla COVID-19-pandemian myötä nopeasti laajentunut etätyö ja sen kyberturvallisuusuhkien hallinta poikkeavat niin sanotusta normaalista etätyötilanteesta. Yhtenä vaikuttavana tekijänä voitaisiin tarkastella kyberhyökkäysten määrää ja niiden ehkäisykeinoja organisaatioissa. Tämän lisäksi olisi mielenkiintoista tutkia onko ennen COVID-19-pandemiaa yleistä kyberturvallisuus-tietoisuutta pidetty teknisten ratkaisujen lisäksi tärkeänä osana kyberturvallisuusuhkien hallintaa.

COVID-19-pandemian aiheuttaman etätyön laajuutta voidaan kuvata myös työn digitaalisena murroksena (digital transformation of work) (Nagel, 2020). Etätyön jäädessä vain lyhytaikaiseksi COVID-19-pandemiaan liittyväksi ilmiöksi, voidaan Nagelin (2020) tutkimustulosten avulla kuitenkin peilata tulevaisuuden työkentän

kehittymistä. Tutkimuksessa digitaalisella työllä on viitattu uusia teknologioita hyödyntävään työhön, jossa yhtenä mahdollisuutena on etätyön tekeminen (Nagel, 2020).

Digitaalisten työmuotojen uskotaan olevan tulevaisuudessa huomattavasti tärkeämpiä kuin pandemiaa edeltävänä aikana (Nagel, 2020), tämän vuoksi organisaatioiden olisi tärkeää varautua etätyötilanteisiin luomalla selkeät toimintaprosessit ja kyberturvallisuuspolitiikka sekä panostaa henkilökunnan koulutukseen kyberturvallisuuden osalta. Etätyötilanteisiin varautumista tukee myös Congerin (2020) tutkimus, jonka mukaan organisaatiot, joissa etätyön tekeminen oli tuttua jo ennen pandemiaa, saivat etätyörutiinit toimimaan nopeammin verrattuna organisaatioihin, joissa etätyötä ei ennen pandemiaa ollut tehty.

Etätyöstä on noin vuoden kestäneen pandemiatilanteen myötä kehittynyt niin sanottu uusi normaali (Conger, 2020; Herath & Herath 2020; Lueck, 2020. Soni et al., 2020.), joten on mielenkiintoista nähdä, tuleeko etätyöskentely jatkumaan yleistyvänä ilmiönä myös tulevaisuudessa. COVID-19-pandemian vaikutuksesta lisääntyneen etätyöskentelyn myötä on mahdollista, että organisaatiot alkavat paremmin huomioida etätyön kyberturvallisuusuhkia ja suhtautua niihin vakavammin; organisaatiot voivat myös olla kiinnostuneita hakemaan ulkopuolista apua turvallisen kyberympäristön varmistamiseksi (Furnell & Shah, 2020). Tulevaisuuden kannalta olisi mielenkiintoista tutkia onko COVID-19-pandemia vaikuttanut merkittävästi organisaatioiden varautumiseen etätyötilanteita ajatellen.

7 Yhteenveto

Tämän tutkielman tarkoituksena oli kirjallisuuskatsauksen avulla esittää keinoja organisaatioiden kyberturvallisuusuhkien hallintaan ja ennaltaehkäisemiseen laajoissa etätyötilanteissa. Aihetta lähestyttiin seuraavan tutkimuskysymyksen avulla: ”Miten organisaatiot voivat hallita koronapandemian myötä laajentuneen etätyöskentelyn kyberturvallisuusuhkia?”. Tutkielman keskeisimmät löydökset voidaan lajitella kolmeen kategoriaan, jotka ovat: turvallisen kyberympäristön varmistaminen, tietoturvan varmistaminen sekä henkilöstön kouluttaminen ja yleisen kyberturvallisuustietoisuuden kasvattaminen.

Turvallisen kyberympäristön varmistamisessa keskeisintä on kyberturvallisuus-politiikan luominen etätyötilanteita varten (Lueck, 2020). Kyberturvallisuuspolitiikan luomista voidaan tukea hyödyntämällä valmiita kyberturvallisuusstandardeja ja -kehyksiä

(Syafrizal et al., 2020). Turvallisen toimintaympäristön varmistamiseen laajoissa etätyötilanteissa kuuluu myös verkon turvaaminen vahvojen VPN-yhteyksien avulla (Conger, 2020; Curran, 2020; Malecki, 2020). Organisaation tietoturvan varmistamisessa taas korostuvat selkeät toimintatavat varmuuskopioiden tekemiseen (Malecki, 2020; Soni et al., 2020) ja tiedostojen jakamiseen (Curran, 2020). Myös GDPR:n noudattaminen tulee huomioida käsiteltäessä EU-kansalaisten henkilötietoja. Tietoturvan varmistamista laajoissa etätyötilanteissa voidaan tukea tietosuojan vaikutustenarvioinnilla (data protection impact assessments, DPIA). Teknisten ratkaisujen lisäksi organisaatioiden kyberturvallisuusuhkien hallintakeinoissa COVID-19-pandemian kontekstissa korostuvat yleisen kyberturvallisuustietoisuuden kasvattaminen ja kouluttaminen organisaation puolelta, sillä Ani et al. (2020) mukaan yksi tapa hallita organisaation kyberturvallisuusuhkia etätyötilanteissa on parantaa yleistä turvallisuustietoisuutta ja panostaa kouluttamiseen.

Lähdeluettelo

Ani, U., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2–35. *https://doi.org/10.1108/JSIT-02-2018-0028*

Conger, S. (2020). The Impact of the COVID-19 Pandemic on Information Systems Management. *Information Systems Management, 37*(4), 327–331. *https://doi.org/10.1080/10580530.2020.1820636*

Curran, K. (2020). Cyber security and the remote workforce. *Computer Fraud & Security, 2020*(6), 11–12. *https://doi.org/10.1016/S1361-3723(20)30063-4*

Furnell, S., & Shah, J. (2020). Home working and cyber security – an outbreak of unpreparedness? *Computer Fraud & Security*, *2020*(8), 6–12. *https://doi.org/10.1016/S1361-3723(20)30084-1*

Herath, T., & Herath, H. (2020). Coping with the New Normal Imposed by the COVID-19 Pandemic: Lessons for Technology Management and Governance. Information *Systems Management, 37*(4), 277–283. *https://doi.org/10.1080/10580530.2020.1818902*

JUFO. (2021). *Julkaisukanavahaku.* Julkaisufoorumi. https://www.tsv.fi/julkaisufoorumi/haku.php?nimeke=Computer+fraud+and+security&konferenssilyh=&isn=&tyyppi=kaikki&kieli=englanti&maa=&wos=&scopus=&nappi=Hae (haettu 13.5.2021)

Kuntaliitto. (2021). *Digitaalinen turvallisuus* (*23.3.2021).* https://www.kuntaliitto.fi/osallistuminen-ja-vuorovaikutus/tietoyhteiskunta-/digitaalinen-turvallisuus (haettu 7.5.2021)

Lueck, M. (2020). GDPR in the new remote-working normal. *Computer Fraud & Security, 2020*(8), 14–16. *https://doi.org/10.1016/S1361-3723(20)30086-5*

Malecki, F. (2020). Overcoming the security risks of remote working. *Computer Fraud & Security, 2020*(7), 10–12. *https://doi.org/10.1016/S1361-3723(20)30074-9*

Nagel, L. (2020). The influence of the COVID-19 pandemic on the digital transformation of work. *International Journal of Sociology and Social Policy, 40*(9/10), 861–875. *https://doi.org/10.1108/IJSSP-07-2020-0323*

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems, 29*(3), 306–321. *https://doi.org/10.1080/0960085X.2020.1771222*

Newlands, G., Lutz, C., Tamò-Larrieux, A., Villaronga, E., Harasgama, R., & Scheitlin, G. (2020). Innovation under pressure: Implications for data privacy during the Covid-19 pandemic. *Big Data & Society, 7*(2). *https://doi.org/10.1177/2053951720976680*

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto.* http://www.tsk.fi/tsk/fi/kyberturvallisuuden_sanasto_tsk_52-1125.html (haettu 21.5.2021)

Shi, F. (2020). *Coronavirus-related phishing.* Barrakuda. https://blog.barracuda.com /2020/03/26/threat-spotlight-coronavirus-related-phishing/ (haettu 19.3.2021)

Soni, V., Kukreja, D., & Sharma, D. (2020). Security vs. Flexibility: Striking a Balance in the Pandemic Era. *2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 1–5. https://doi.org/10.1109/ANTS50601.2020.9342779*

STM. (2021). *Etätyöt koronavirustilanteessa (päivitetty 1.3.2021).* Sosiaali- ja terveysministeriö. https://stm.fi/etatyot-koronavirustilanteessa (haettu 7.3.2021)

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security, 12*(3), 417-432.

TEPA-termipankki. https://termipankki.fi/tepa/fi/ (haettu 9.5.2021)

Tietosuojavaltuutettu. *Vaikutustenarviointi.* Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/vaikutustenarviointi (haettu 8.5.2021)

Tilastokeskus. *Käsitteet.* https://www.stat.fi/meta/kas/etatyo.html (haettu 8.5.2021)

THL. (2020). *WHO julisti koronaviruksen kansainväliseksi kansanterveysuhaksi (31.1.2020).* Terveyden ja hyvinvoinninlaitos. https://thl.fi/fi/-/who-julisti-koronaviruksen-kansainvaliseksi-kansanterveysuhaksi (haettu 7.3.2020)

TTL. (2016). *Jousto-opas (25.11.2016).* Työterveyslaitos. https://issuu.com/-tyoterveyslaitos/docs/ttl_jousto_opas-2016 (haettu 18.3.2021)

Zaharia, A. (2020). Security Risks of Cloud and Mobile Technologies During the Pandemic and Their Opportunities. *Informatica Economica, 24*(3), 64–74. *https://doi.org/10.24818/issn14531305/24.3.2020.06*