SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Miikka Heikkinen

Etätyön tietoturvajohtamisen kehittäminen pk-yrityksessä

Opinnäytetyö
Syksy 2022
Insinööri (ylempi AMK), Teknologiaosaamisen johtaminen

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Insinööri (YAMK), Teknologiaosaamisen johtaminen

Tekijä: Miikka Heikkinen

Työn nimi: Etätyön tietoturvajohtamisen kehittäminen pk-yrityksessä

Ohjaaja: Alpo Anttonen

Vuosi: 2022 Sivumäärä: 72 Liitteiden lukumäärä: 1

Maailma on muuttunut paljon viimeisen kahden vuoden aikana, ja varsinkin koronapandemian takia etätyö ja muut joustavat työmuodot yleistyvät nopeasti. Tämä myös aiheutti lisävaatimuksia yritysten tietoturvan ja tietosuojan johtamiseen.

Liiketoiminnan jatkumisen kannalta kriittisen tiedon suojaaminen ja turvaaminen on yrityksille elintärkeää. Aktiivisen tietoturvan hallinnan ja tietoturvan johtamisen kehittämisen avulla pyritään varmistamaan tiedon eheys ja luottamuksellisuus myös etätyössä.

Tutkimuksen tavoitteena oli selvittää pk-yrityksen etätyön tietoturvan ja tietosuojan nykytilannetta, selvittää tarvittavat ja suositellut kehityskohteet etätyön tietoturvan parantamiseksi sekä kehittää etätyön tietoturvajohtamista.

Tutkimus oli luonteeltaan kvalitatiivinen toimintatutkimus, jossa teorioita sovellettiin tietoturvan soveltamiseen etätyössä. Kysely lähetettiin 21 eri pk-yrityksen IT-päättäjälle. Vastaukset saatiin 14 vastaajayritykseltä.

Työn teoriaosuudessa on selvitetty ja esitelty tietoturvan keskeisiä peruskäsitteitä, periaatteita, IT-riskienhallintaa tietoturvajohtamisen näkökulmasta, käytettyjä tietoturvasuosituksia ja -malleja sekä ohjeita.

Tutkimuksen tuloksena saatiin suosituksia, joilla voidaan parantaa useamman yrityksen tietoturvaa ja tietosuojaa.

Tutkimuksen tulokset sekä johtopäätökset ja kehitysehdotukset ovat koottu opinnäytetyön loppuun. Kysely on liitetty opinnäytetyön loppuun liitteeksi.

[1] Asiasanat: tietoturva, etätyö, johtaminen, tietosuoja, pk-yritys

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Master's Degree programme: Technology Competence Management

Author: Miikka Heikkinen

Title of thesis: Developing remote working cybersecurity management in small and medium enterprises

Supervisor: Alpo Anttonen

Year: 2022 Number of pages: 72 Number of appendices: 1

The world has rapidly changed during the last two years. Especially the coronavirus pandemic forced the introduction of remote work and other flexible forms of work. The change in forms of work introduced more demands for cybersecurity and data protection management.

The business continuity is one of the main focuses for enterprises. Protecting critical data and cybersecurity is an essential factor. With active cybersecurity management and development integrity, compliance, and consistency of data are improved and access control for right individuals is ensured.

The main goal for the thesis was to determine current needs and best practices for cybersecurity and data protection in remote work for small and medium enterprises. The goal was also to create recommendations to develop remote work cybersecurity management.

The study was qualitative, where the theoretical starting point was to implement the theory of cybersecurity to remote work use and a survey was conducted in the autumn of 2022. The survey was sent to 21 respondents and total of 14 responses was received.

Based on the results, recommendations and best practices were made to improve the cybersecurity and data protection in small and medium enterprises.

[1] Keywords: cybersecurity, remote, work, management, small and medium enterprise

SISÄLTÖ

Kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

Azure	Microsoftin julkisen pilven alusta sovellusten ja palvelujen rakentamista, testaamista, tuottamista ja hallintaa varten.
BEC	Tulee englanninkielisistä sanoista Business Email Compromise, ja sillä tarkoitetaan huijausta, jossa kyberrikollisen tavoitteena on päästä viestiketjuun mukaan tekeytymällä toiseksi yrityksen henkilöksi. Tavoitteena on yleensä rahallinen hyöty, kuten laskujen väärentäminen.
brute-force-hyökkäys	Hyökkäystapa, jolla yritetään järjestelmällisesti löytää oikea salasana tai salausavain kohdejärjestelmään.
Conditional Access	Suomeksi ehdollinen pääsynhallinta on Microsoftin kehittämä pääsynhallintaratkaisu.
COVID-19	Vuoden 2019 joulukuussa kiinalaisesta Wuhanin kaupungista alkanut uuden koronaviruksen SARS-CoV-2:n aiheuttama epidemia levisi maaliskuussa 2020 WHO:n julistamaksi maailmanlaajuiseksi pandemiaksi. SARS-CoV-2 aiheuttaa COVID-19-nimistä tartuntatautia.
Defender for O365	Microsoft 365 -tietoturvaperheeseen kuuluva tuote, joka sisältää mm. suojaustapoja tietojenkalasteluita vastaan.
Endpoint Manager	Microsoftin pilvipohjainen keskitetty päätelaitehallintaratkaisu. Toiselta nimeltään Intune.
GDPR	General Data Protection Regulation - EU:n yleinen tietosuoja-asetus (GDPR) (EU) 2016/679.
hybridityö	Hybridityöllä tarkoitetaan työskentelymallia, jossa töitä tehdään sekä ajoittain etänä että fyysisesti työpaikalla.

JIT	Just-in-time on englanninkielinen termi tarveperusteiselle pääsynhallinnalle. Sillä tarkoitetaan esimerkiksi virtuaalikoneiden hallintaportin käyttöä vain tarvittaessa.
MFA	MFA on lyhenne englanninkielisestä termistä Multi-Factor Authenticaton, ja sillä tarkoitetaan monimenetelmäistä tunnistautumista. Siinä perinteisen käyttäjätunnus ja salasana -yhdistelmän lisäksi tehdään lisätarkistus kirjautumisen yhteydessä.
Microsoft 365	Microsoftin hyötyohjelmapilvipalvelu, joka sisältää tuottavuutta ja kyberturvallisuutta parantavia työkaluja, kuten Office-sovellukset ja kehittyneet tietoturvaratkaisut. Voidaan myös käyttää termiä Office 365.
password spraying	Hyökkäystapa, jolla kyberrikollinen pyrkii arvaamaan käyttäjätunnuksen salasanan tai kokeilemaan yleisimpiä tai vuodettuja salasanoja.
phishing	Tarkoittaa tietojenkalastelua, jossa uhria pyritään huijaamaan ja luovuttumaan käyttäjätunnukset tai muita tietoja.
PIM	Priviliged Identity Management on Microsoftin kehittämä identiteetinhallintaratkaisu.
pk-yritys	Pienet ja keskisuuret yritykset (pk-yritykset) määritellään yrityksiksi, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa (40 miljoonaa euroa ennen vuotta 2003) tai taseen loppusumma on enintään 43 miljoonaa (27 miljoonaa euroa ennen vuotta 2003) euroa. (Tilastokeskus 2021.)
RDP	Remote Desktop Protocol on Microsoftin kehittämä protokolla graafiseen käyttöliittymään etätietokoneelle.
SaaS	Software as a Service, sovellus palveluna on pilvipalveluarkkitehtuurin kerros.

social engineering	Tarkoittaa ihmisen manipulointia tai huijaamista, jota hyödynnetään mm. verkkohuijauksissa, kuten tietojenkalastelussa.
upKeeper	Ruotsalaisen upKeeper Solutions AB:n kehittämä päätelaitehallinta-ratkaisu.
VPN	Virtual Private Network, tekniikka, jolla luodaan turvallisia tunneleita internetverkkoon.

.

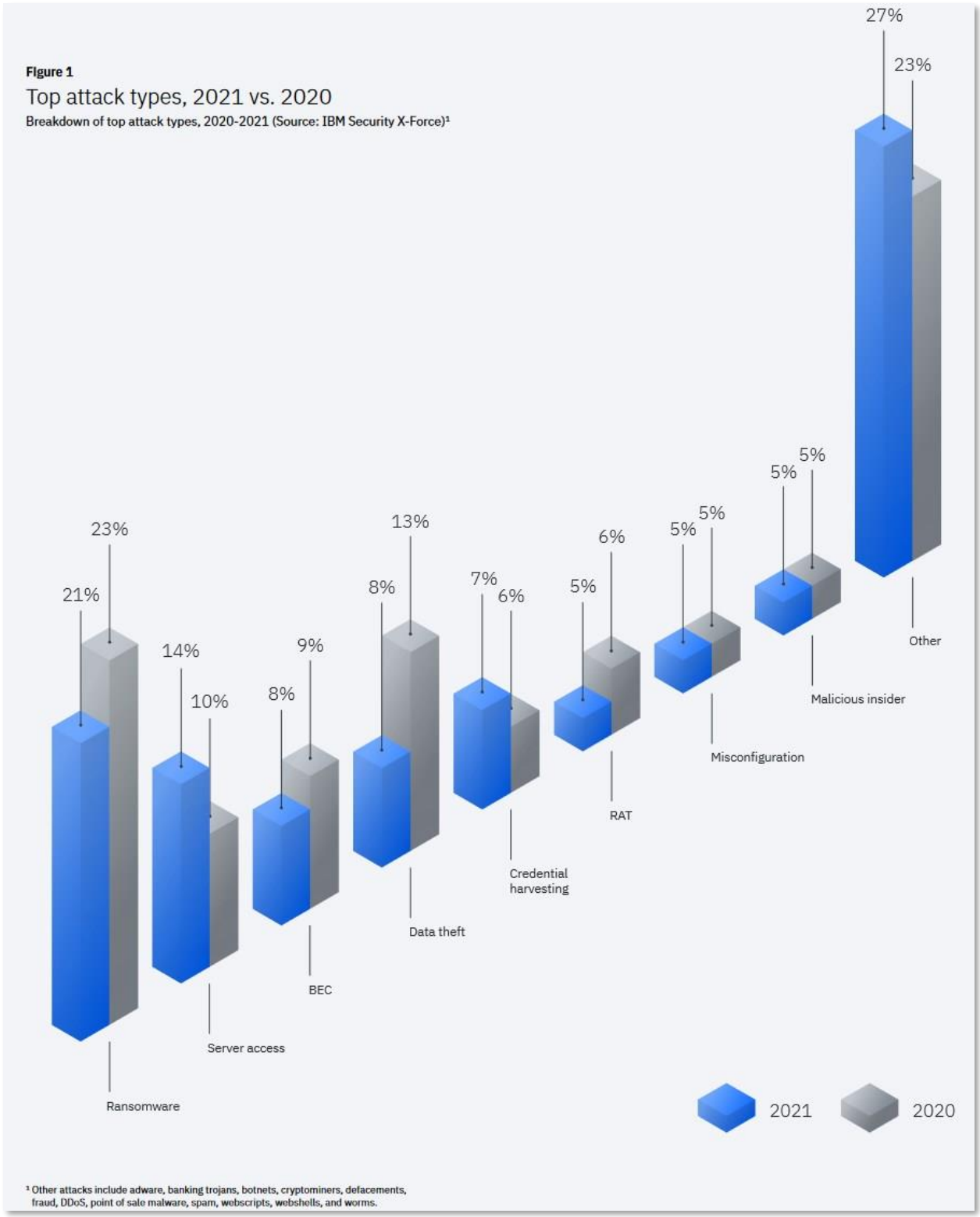
1 JOHDANTO

1.1 Työn tausta

Tämä opinnäytetyö on tehty Seinäjoen ammattikorkeakoulun teknologiaosaamisen johtamisen koulutusohjelmassa (ylempi ammattikorkeakoulututkinto). Tämän työn tarkoituksena on selvittää, miten ja millä tavalla pk-yritys voisi kehittää tietoturvan johtamista etätyössä. Aihe on työn kirjoitushetkellä ajankohtainen vuonna 2019 puhjenneen ja vuonna 2020 pandemiaksi edenneen COVID-19-taudin jälkimainingeissa. Pk-yrityksen tietoturvan johtamisen kehitystarpeita ja tietoturvan sekä tietosuojan yleistä tilaa kartoitetaan kyselytutkimuksella.

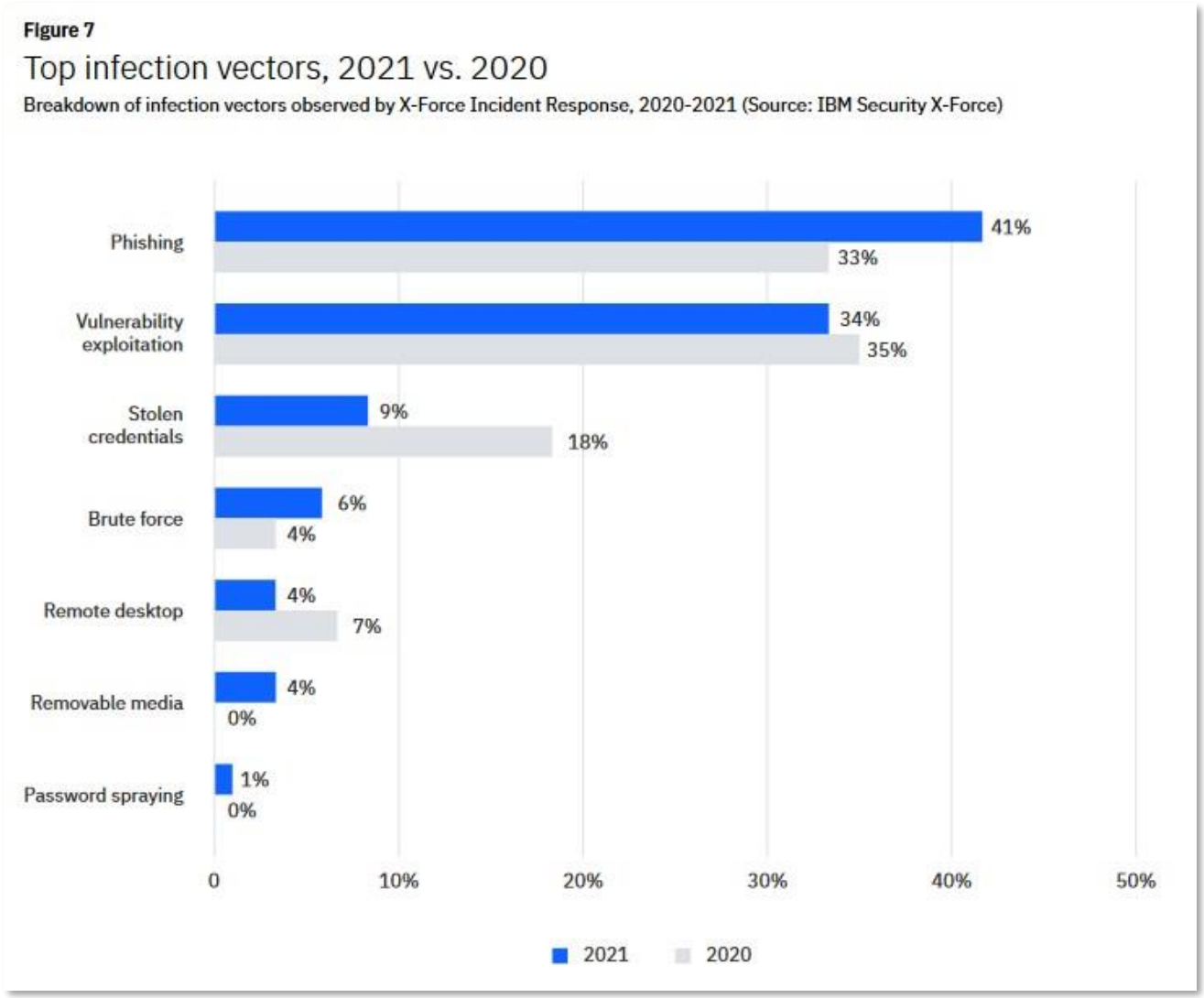
Yksi tuoreimmista aiheeseen liittyvistä tutkimuksista on Innolinkin toteuttama, Arrow ECS Finland Oy:n teettämä tutkimus. Siinä kartoitettiin koronan vaikutuksia yritysten liiketoimintaan ja digitalisaatioon vuonna 2020. Tavoitteena oli tutkia mm. toimintatapojen muutoksia. Kohderyhmänä olivat sellaiset yritykset kaupan, julkishallinnon, teollisuuden, palveluiden, rakentamisen ja terveydenhuollon toimialoilta, joiden liikevaihdon suuruus oli 2–100 miljoonaa euroa. Tutkimuksen mukaan jopa 71 prosentilla yrityksistä etätyöskentely oli lisääntynyt. Tulosta selittää myös se seikka, että tutkimuksen mukaan 55 prosentilla vastaajayrityksistä oli voimassa etätyösuositus ja kymmenellä prosentilla oli voimassa etätyömääräys. (Innolink 2020.)

Vielä tuoreemman IBM:n vuonna 2021 tekemän tutkimuksen mukaan maailma jatkaa edelleen kamppailua pandemian ja sen aiheuttaman etätyön sekä toimistolle paluun kanssa. Myös geopoliittiset muutokset aiheuttavat epäluottamuksen tunnetta. IBM:n mukaan nämä yhdessä luovat kaaosta, jossa kyberrikolliset mielellään viihtyvät. Tutkimuksen mukaan IBM on arvioinut globaaliin yritykseen kohdistetun onnistuneen verkkohyökkäyksen hinnaksi keskimäärin jopa 4,35 miljoonaa dollaria (IBM 2022b.) Yleisin yksittäinen hyökkäystapa oli kiristyshaittaohjelma, jonka osuus oli 21 prosenttia kaikista hyökkäyksistä. 23 prosenttia hyökkäyksistä tuli muista hyökkäystavoista, kuten mainos- ja valuutanlouhintahaittaohjelmat, troijalaiset ja madot. Muita yleisimpiä yksittäisiä hyökkäystapoja olivat luvattomat pääsyt palvelimille. (IBM 2022a.)



Kuvio 1. Yleisimmät hyökkäystavat 2021 vs. 2020 (IBM 2022a).

Luvaton pääsy palvelimeen saavutettiin yleensä käyttämällä tai hyödyntämällä tietojenkalastelua, haavoittuvuuksia, varastettuja käyttäjätunnuksia, salasanojen brute-force -hyökkäystä, RDP-etäyhteysprotokollaa, ulkoista mediaa tai ns. password spraying -hyökkäystä. (IBM 2022a.)



Kuvio 2. Yleisimmät tartuntavektorit, 2021 vs. 2020 (IBM 2022a).

1.2 Työn tavoite

Työn tavoitteena on kyselytutkimuksen analysoinnin perusteella kehittää pk-yrityksen tietoturvaa ja tietosuojaa etätyössä. Johtamisen näkökulmasta on tavoitteena saada tietoa

työntekijöiden etätyön tietoturvan haasteista, kuten esim. tietoturvaperehdytyksestä, käytettävien laitteiden ja palveluiden suojauksesta. Työn avulla on myös tarkoitus luoda suosituksia, joiden avulla voidaan kehittää etätietoturvaa yleisesti pk-yrityksessä.

Tyytyväisyys ja etätyön sujuvuus ovat tämän opinnäytetyön tekijän mielestä merkittävässä roolissa. Käytettävien työkalujen ja palveluiden tulee toimia moitteettomasti myös etätyössä. Tyytyväisyyteen liittyvät kaikki edellä mainitut aiheet. Jos työntekijä mieltää toisenlaisen tavan tai työkalun tehdä töitä etänä, voi olla suuri riski, että toisenlainen tapa tai työkalu muodostaa tietoturvauhan yrityksen datalle ja tietojärjestelmille. (Tivi 2016.)

1.3 Työn rakenne

Opinnäytetyö rakentuu kuudesta pääluvusta. Johdannon jälkeen työn toisessa luvussa käydään läpi etätyön määritelmä, etätyön lainsäädäntöä, tietosuojan ja tietoturvan merkitystä etätyössä sekä tietosuojan ja tietoturvan erot.

Kolmannessa luvussa käydään läpi yleisimpiä tietoturvauhkia ja tapoja varautua niiltä. Lisäksi käydään läpi tietoturvaratkaisuja sekä yleisiä suosituksia, joita voidaan käyttää yrityksessä parantamaan tai hallitsemaan tietoturvaa.

Neljännessä luvussa käydään läpi kyselytutkimuksen menetelmä ja toteutus. Viidennessä luvussa pohditaan ja analysoidaan kyselytutkimuksen tuloksia.

Viimeisessä luvussa käydään läpi johtopäätökset ja suositukset etätyön tietoturvan johtamisen kehittämiseen.

1.4 Tutkimusmenetelmät

Työn tuloksien analysoinnin tiedonlähteinä käytetään hyväksi kirjallisuutta, sekä mahdollisia tutkimuksia ja tilastoja. Tiedonlähteinä käytetään myös luotettavia internetlähteitä. Tärkeimmässä roolissa on kuitenkin kyselytutkimus ja siitä saatavat vastaukset. Kyselytutkimus toimitetaan sähköpostilla tai tarkoitukseen soveltuvalla järjestelmällä, josta saadaan tulokset

analysoitavaksi. Vastaukset annetaan anonyymina. Lisää tutkimusmenetelmästä ja toteutuksesta luvussa neljä.

2 ETÄTYÖ

2.1 Määritelmä

Etätyö tarjoaa työntekijöille ja työnantajille mahdollisuuden joustavaan ja tehokkaaseen työn tekemiseen siirtämällä painopistettä itse työntekijän läsnäolosta työn tulosten arviointiin. Etätyö auttaa lisäksi kehittämään eri työskentelytapoja ja johtamista. (Helle 2004, 41.)

Suomessa ei ole olemassa mitään virallista määritelmää etätyölle, vaikka etätyöllä on yleisesti vakiintunut merkitys. Käsitteenä etätyö voidaan määritellä joko työoikeudellisena tai organisatorisena. Työelämän lainsäädäntö ei varsinaisesti tunne etätyö-termiä, mutta työsopimus-, työaika- ja työturvallisuuslakia sovelletaan normaalisti etätyöntekijään muutamaa poikkeusta lukuun ottamatta. (Helle 2004, 41.)

Helle (2004) kuvailee etätyön organitorisena käsitteenä työn tekemisen paikan mukaan. Kun työ tehdään työpaikalla tai työnantajan tiloissa, käsitteenä on työ. Etätyötä on, kun työn tekemisen paikan oletetaan olevan etäällä varsinaisesta työnantajan toimitilasta. Jos työtä tehdään oletetusti vaihtelevissa paikoissa, joissa sijainti vaihtuu tarpeen mukaan, kyseessä on liikkuva tai joustava työ. (Helle 2004, 42.)

Työturvallisuuskeskus määrittelee etätyön tarkemmin seuraavasti:

> Etätyöllä tarkoitetaan joustavaa, vapaaehtoisuuteen, sopimukseen ja sääntöihin perustuvaa työn tekemistä muualla kuin työnantajan tiloissa. Työskentely voi tapahtua yhdessä tai useammassa paikassa ja olla kestoltaan ja säännöllisyydeltään hyvin vaihtelevaa. (Työturvallisuuskeskus 2017.)

2.2 Etätyöstä sopiminen

Lainsäädäntö ei tunne varsinaisesti termiä etätyö. Perustana ovat kuitenkin työsopimuslaki, työaikalaki ja työturvallisuuslaki. Koska etätyö ja muut joustavat työjärjestelyt ovat yleistyneet nopeasti, on niitä koskien syntynyt hyväksi havaittuja käytäntöjä. Nämä sovitut käytännöt

helpottavat arkea ja vähentävät ristiriitoja. (Työsuojeluhallinto 2020.) Lisää etätyötä koskevasta työelämän lainsäädännöstä on luvussa 2.6.

Lainsäädännön lisäksi on olemassa etätyötä koskeva puitesopimus, jonka Euroopan työmarkkinaosapuolet eli UNICE/UEAPME, CEEP ja EAY ovat allekirjoittaneet 16.7.2002. Sopimuksen täytäntöönpano tapahtui jäsenvaltioissa työmarkkinaosapuolten omien menettelyjen ja käytäntöjen mukaisesti. Puitesopimuksen kansallinen täytäntöönpano Suomessa toteutettiin työmarkkinajärjestöjen allekirjoittamalla asiakirjalla ja sen mukaisilla toimenpiteillä. (Etätyötä koskeva puitesopimus 2002.)

Puitesopimuksen 2. artiklan mukaan etätyö määritellään seuraavasti:

> Etätyö on tapa organisoida ja/tai suorittaa työtä työsopimuksen perusteella/työsuhteessa käyttäen tietotekniikkaa tavalla, jossa työ, jota voitaisiin tehdä myös työnantajan tiloissa, tehdään säännöllisesti noiden tilojen ulkopuolella.
>
> Tämä sopimus kattaa etätyöntekijät. Etätyöntekijä on jokainen henkilö, joka tekee edellä mainittua etätyötä. (Etätyötä koskeva puitesopimus 2002.)

Helteen (2004) mukaan etätyön puitesopimuksen määritelmä on melko monimutkaisesti muotoiltu ja se on osittain hieman vaikeasti avautuva. Määritelmään voidaan sisällyttää seuraavat elementit:

1. Etätyö on tapa organisoida työtä, ei erillinen työsuhdemuoto.
2. Etätyössä käytetään hyväksi tietotekniikkaa.
3. Etätyötä tehdään työnantajan tilojen ulkopuolella, mutta sitä voitaisiin tehdä myös työnantajan tiloissa.
4. Etätyötä tehdään säännöllisesti. (Helle 2004, 47–49.)

Puitesopimus ottaa myös kantaa etätyön tietoturvaan 5. artiklassa seuraavasti:

> Työnantaja on velvollinen ryhtymään tarvittaviin toimenpiteisiin, etenkin ohjelmistojen suhteen, varmistaakseen etätyöntekijän ammatillisiin tarkoituksiin käyttämän ja käsittelemän tiedon suojauksen.

> Työnantaja antaa etätyöntekijälle tiedot kaikesta tietosuojaa koskevasta asiaankuuluvasta lainsäädännöstä ja yrityskäytännöistä.

Työnantaja tiedottaa etätyöntekijälle erityisesti:

- kaikista rajoituksista tietotekniikkalaitteiden tai -välineiden käytössä, kuten internetin käytöstä
- sääntöjen laiminlyönnistä johtuvista seuraamuksista. (Etätyötä koskeva puitesopimus 2002.)

2.3 Etätyön muotoja

Etätyötä voidaan tehdä monella eri tavalla, eikä ole olemassa mitään virallista jaottelua etätyömuodoista. Etätyömuodot kehittyvät jatkuvasti tietotekniikan ja tietoliikenneyhteyksien kehittyessä. (Helle 2004, 49.)

Useimmiten voidaan erotella ainakin seuraavat etätyömuodot:

- Kokonaan tai osittain tehtävä etätyö työntekijän kotona tai muussa työntekijän valitsemassa paikassa (Helle 2004, 50).

- Etätyö voi olla myös niin sanottua liikkuvaa työtä, jota voidaan tehdä yrityksen muissa toimipisteissä tai esimerkiksi julkisissa tiloissa, kuten lentokentillä, hotelleissa, asiakkaan luona tai muissa satunnaisissa tiloissa. (Työturvallisuuskeskus 2017.)

- Etätyökeskuksessa tehtävä työ, esim. jaetuissa toimistotiloissa, jossa työskentelee useita eri työnantajien työntekijöitä.

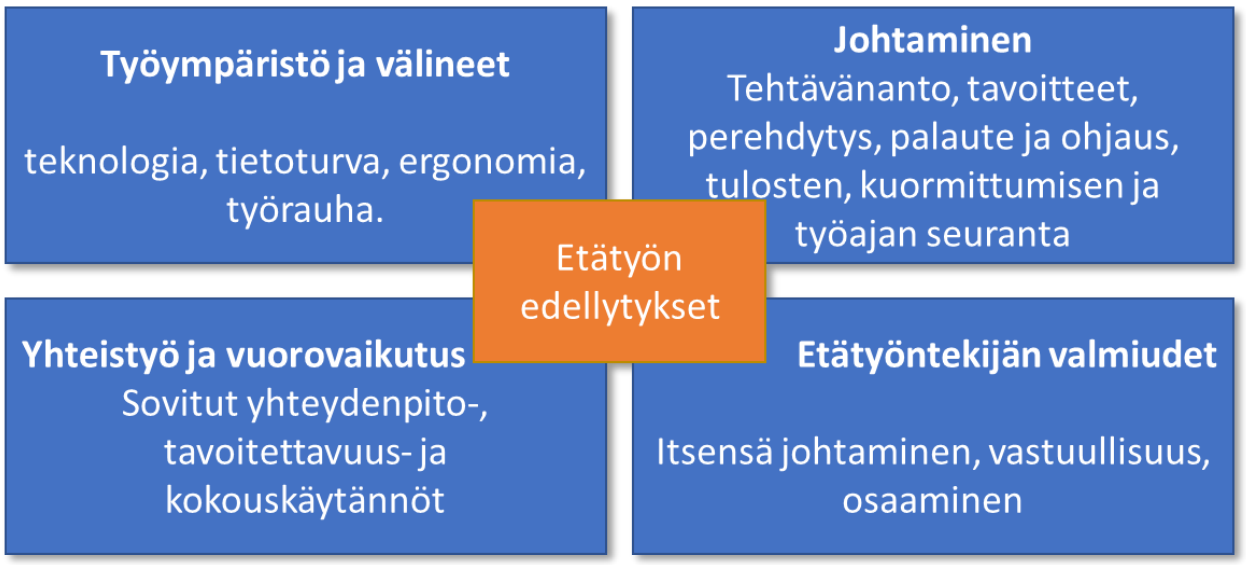
- Yrittäjänä, kuten esimerkiksi freelancerina tehtävä etätyö. (Helle 2004, 50.)

Etätyö voi myös olla epäsäännöllistä esimiehen kanssa sovittuna tai esimerkiksi työmatkan yhteydessä tehtyä työtä. Epäsäännöllistä etätyötä voi olla myös tietyn työtehtävän suorittaminen. (Työturvallisuuskeskus 2017.)

Säännöllinen etätyö voi olla sovitun työrytmin mukaan tehtävää, kuten tiettyinä viikonpäivinä, tai sitten tietty määrä päiviä viikossa tai kuukaudessa. Voidaan myös sopia kokoaikaisesta etätyöstä, jolloin työ on täysin tai pääosin etänä tehtävää. (Työturvallisuuskeskus 2017.)

2.4 Etätyön edellytyksiä

Toimivaa teknologiaa ja tietoturvan varmistamista ei voi liikaa korostaa, kun puhutaan etätyön edellytyksistä. Näiden ohella myös työnantajan ja työntekijän luottamus on tärkeää. Myös fyysinen ja henkinen ympäristö tulee olla terveellinen, turvallinen, rauhallinen, mutta etenkin työhön sopiva. Kun kasvokkain tapahtuvia kohtaamisia esimerkiksi esimiehen kanssa on harvemmin, etätyötä johdetaan mm. virtuaalisesti. On tärkeää ylläpitää luottamusta, pitää kiinni yhteisistä säännöistä, asettaa realistisia tavoitteita ja seurata niiden toteutumista. Etätyöntekijältä vaaditaankin kykyä työn ja vapaa-ajan rajaamiseen vastuullisuuden lisäksi. (Työturvallisuuskeskus 2017.)



Kuvio 3. Etätyön edellytykset (Työturvallisuuskeskus 2017).

Helteen mukaan etäyöhön vaaditaan seuraavat tekniset edellytykset:

- Etätyöntekijällä on etätyöpaikassa käytössään tarvittava tietotekniikka ja tietoliikenneyhteydet.

- Etätyöntekijällä on hyvä tietotekninen osaaminen.
- Etätyöntekijällä on käytössään tekninen tuki ongelmatilanteita varten.
- Etätyöntekijän esihenkilöllä, työtovereilla ja muulla työyhteisöllä on riittävä tietotekninen osaaminen.
- Etätyössä tarvittava tieto on saatavilla tietoverkkojen kautta.
- Yrityksen tiedonhallintajärjestelmien käyttö ja toimivuus myös etätyössä.
- Tietoturvallisuudesta huolehditaan tarvittavin lisäjärjestelyin. (Helle 2004, 96)

2.5 Etätyön johtaminen

Etäjohtaminen perustuu enemmän ihmisten johtamiseen kuin asioiden johtamiseen ja onkin siinä mielessä modernia johtamista. Perinteiset toimintamallit eivät tämän takia sovellu samalla tavalla etäjohtamiseen. Etäjohtajalta vaaditaan erityisesti kykyä kyseenalaistaa tämänhetkiset tavat ja toiminnat, sillä on tärkeää tunnistaa vanhentuneet ja toimimattomat toimintamallit sekä prosessit. On tärkeää miettiä etätyöntekijöiden kanssa yhdessä uusia toimintamalleja. Etätyön johtajalta vaaditaan erityistä panostamista viestintään ja vuorovaikuttamiseen. Koska yhteydenpito yleensä kestää etätyössä vähemmän aikaa, keskustelut onkin hyvä aikatauluttaa ja suunnitella varta vasten, ja joskus jopa varata aikaa vapaamuotoiselle keskustelulle. (Vilkman 2016a, 57–59.)

Tärkein menestystekijä on luottamus, ja sen saavuttaminen on haasteellista. Sillä on iso merkitys kommunikoinnin onnistumiseen, kehittymiseen, laatuun ja tehokkuuteen. Luottamus edistää luovuutta ja auttaa sitoutumisen ja yhteisöllisyyden rakentamisessa. Etäjohtamisen näkökulmasta on osattava arvioida valvonnan tason tarve sekä huolehdittava tarvittavasta työsuoritusten seurannasta. (Työturvallisuuskeskus 2017.)

Etätyön yleistymisen yksi suurimmista haasteista liittyy etätyön johtamiseen ja valvontaan. Työnantajalla on oikeus valvoa ja johtaa työtä normaalisti. Etätyössä on kuitenkin työn valvonta ajateltava kokonaan uudelleen. Esimerkiksi monilla työpaikoilla voidaan ajatella yhä, että työntekijä on oikeasti töissä vasta, kun työntekijä on fyysisesti ja näkyvillä työpöytänsä ääressä. (Helle 2004, 128–129.)

Etätyön johtaminen voi tuoda myös etuja johtamisen näkökulmasta. Vilkmanin (2016b) mukaan etätyön johtaminen ei ole sen haasteellisempaa kuin tiimin johtaminen fyysisesti samassa paikassa, mutta se on erilaista. Johtaminen voi muuttua haasteelliseksi, jos yritetään johtaa etätyössä olevia samoilla periaatteilla kuin toimistolla. Perinteiset tavat johtaa voi olla esteenä etätyön parempaan hyödyntämiseen. Monissa organisaatioissa on vielä läsnä vanhoja johtamiskulttuureita ja asenteita. Muun muassa kontrolloitu ja työaikaan sidottu työ ja sen arvostaminen hidastaa etätyön yleistymistä.

Joustavien työskentelymahdollisuuksien tarjoaminen on osoitus siitä, että työntekijään luotetaan. Tämä synnyttää samalla luottamusta itse organisaatioon ja sen johtoon. Näin syntyy lisäksi myös tunne, että työn tulos on merkittävä, eikä työpaikalla vietetty aika. (Vilkman 2016b.)

Vilkmanin (2016b) mukaan haastavinta etätyönjohtamisessa on toimivan tiimin rakentaminen ja yhteenkuuluvuuden tunteen saavuttaminen tiimien jäsenten keskuudessa. Jos tiimien jäsenet eivät tunne kuuluvansa tiimiin tai joukkoon, voi seurauksena olla viestinnän ja koheesion eli sidonnaisuuden vähentymistä, sekä heikentynyttä moraalia ja organisaatioon sitoutumista. Yhteenkuulumisen kannalta psyykkinen läheisyyden tunne on fyysistä oleellisempaa. Etätyö voi aiheuttaa työyhteisyyden tunteen puutetta ja onkin yksi esihenkilötyön suurimmista haasteista. Sosiaalinen tuki onkin yksi tärkeimmistä voimavaratekijöistä.

Etäjohtamisessa on suuri rooli erilaisten teknologioiden ja järjestelmien hyödyntämisessä. Teknologian tehtävänä on edistää ja auttaa työssä onnistumista ja yhteistyötä sekä mahdollistaa uudenlaisia etätyön muotoja. Pitää huomioida, että teknologia ei itsessään synnytä yhteistyötä, vaan mahdollistaa sen. Esihenkilön tehtävä on luoda yhteistyön kulttuuri työyhteisöön. (Vilkman 2016a, 63.)

2.6 Lainsäädäntö

2.6.1 Työturvallisuuslaki (738/2002)

Työturvallisuuslain tarkoituksena on parantaa työympäristöä ja työolosuhteita työntekijöiden työkyvyn turvaamiseksi ja ylläpitämiseksi sekä ennalta ehkäistä ja torjua työtapaturmia, ammattitauteja ja muita työstä ja työympäristöstä johtuvia työntekijöiden fyysisen ja henkisen terveyden haittoja. (L 738/2002.)

Usein etätyötä tehdään kotona tai sellaisissa olosuhteissa, joiden turvallisuutta on työnantajan mahdotonta tai ainakin vaikeaa arvioida, saati selvittää. Etätyössä korostuu myös etätyöntekijän vastuu omasta hyvinvoinnista ja riskien tunnistamisesta. Lakisääteinen tapaturmavakuutus on myös voimassa etätyössä, mutta korvattavuudessa voi olla rajoituksia. (Työsuojeluhallinto 2020.)

Työturvallisuuslain (L 738/2002) ensimmäisen luvun viidennessä momentissa säädetään lain soveltamista myös sopimuksen mukaiseen työhön, jota työntekijä tekee työntekijän kotona tai muussa valitsemassaan paikassa, työnantajan kodissa taikka työnantajan osoituksesta muun henkilön kodissa tai näihin liittyvissä olosuhteissa.

Lain toisen luvun kahdeksannessa momentissa on säädetty työnantajan velvoitteet tarpeellisilla toimenpiteillä huolehtia työntekijöiden turvallisuudesta ja terveydestä työssä. Tässä tarkoituksessa työnantajan on otettava huomioon työhön, työolosuhteisiin ja muuhun työympäristöön samoin kuin työntekijän henkilökohtaisiin edellytyksiin liittyvät seikat. (L 738/2002.)

Toisen luvun kymmenennessä momentissa on säädetty työnantajan velvollisuus ottaa huomioon työn vaarojen selvittäminen ja arviointi:

> Työnantajan on työn ja toiminnan luonne huomioon ottaen riittävän järjestelmällisesti selvitettävä ja tunnistettava työstä, työajoista, työtilasta, muusta työympäristöstä ja työolosuhteista aiheutuvat haitta- ja vaaratekijät sekä, jos niitä ei voida poistaa, arvioitava niiden merkitys työntekijöiden turvallisuudelle ja terveydelle. (L 738/2002.)

2.6.2 Työaikalaki (872/2019)

Vanha työaikalaki (L 605/1996), joka oli voimassa 31.12.2019 asti, jätti etätyön työaikalain soveltamisen ulkopuolelle, ja silloin vain työpaikalla tehty työ laskettiin työajaksi työaikalain ensimmäisen luvun toisessa momentissa. Uudessa 1.1.2020 voimaantullessa työaikalaissa (L 872/209) myös etätyö tuli työaikalain ja työajan seurannan piiriin. (HE 158/2018 vp.)

Työaikalain neljännen luvun 13. momentissa on säädetty joustotyöajasta. Siinä työnantaja ja työntekijä saavat työehtosopimuksen säännöllisen työajan pituutta ja sijoittamista koskevista määräyksistä poiketen sopia joustotyöaikaa koskevasta työaikaehdosta, jonka mukaan vähintään puolet työajasta on sellaista, jonka sijoittelusta ja työntekopaikasta työntekijä voi itsenäisesti päättää. (L 872/2019.)

2.6.3 Työsopimuslaki (55/2001)

Etätyöstä ja sen järjestelyistä sovitaan yleensä kirjallisesti. Yrityksessä voi olla myös käytössä yhteistoiminnassa sovitut pelisäännöt. (Työsuojeluhallinto 2020.)

Työsopimuslaissa (L 55/2001) on säädetty selvitys työnteon keskeisistä ehdoista lain toisen luvun neljännessä momentissa, jossa työnantaja velvoitetaan antamaan työntekijälle kirjallinen selvitys työnteon keskeisistä ehdoista.

2.6.4 EU:n yleinen tietosuoja-asetus

EU:n tietosuojalainsäädännön uudistaminen käynnistyi vuonna 2012, kun tietosuojalainsäädäntö ei enää vastannut globaalin tietoympäristön ja digitaalitalouden tarpeisiin. Tämän prosessin tuloksena syntyi EU:n yleinen tietosuoja-asetus, GDPR (EU 2016/679). Siinä pyrittiin turvaamaan henkilötietojen suoja perusoikeutena, mutta turvaamaan myös digitaalitalouden kehitys ja tehostamaan rikollisuuden ja terrorismin estämistä (Eduskunta 2018). Asetus tuli voimaan 24. toukokuuta 2016 ja sitä alettiin soveltamaan kahden vuoden siirtymäajan jälkeen alkaen 25.5.2018. (Andreasson, Riikonen & Ylipartanen 2019, 46.)

Asetus koskee sen soveltumisalan piiriin kuuluvaa henkilötietojen käsittelyä Euroopan unionin jäsenvaltioissa. Se on myös suoraan sovellettavaa lainsäädäntöä Suomessa. Asetus sisältää täsmennyksiä aiempaan sääntelyyn sekä huomattavasti uusia velvoitteita ja sanktioita. (Andreasson ym. 2019, 46.)

Tietosuojalla on yleisesti tarkoitettu tietosuojan yleislain ja erityislakien henkilötietojen käsittelyä koskevien oikeuksien ja velvollisuuksien huomioonottamista rekisterinpitäjän operatiivisessa toiminnassa, sekä luonnollisten henkilöiden yksityisyyden suojan ja oikeusturvan varmistamisessa. (Andreasson ym. 2019, 20.)

Henkilötietojen käsittely tarkoittaa muun muassa henkilötietojen keräämistä, säilyttämistä, siirtämistä ja luovuttamista. Kaikki toimenpiteet, jotka kohdistuvat henkilötietoihin, ovat henkilötietojen käsittelyä. Näitä toimenpiteitä ovat kaikki käsittelyn suunnittelusta henkilötietojen poistamiseen. Henkilötietoja ovat kaikki tiedot, jotka ovat liitettävissä tunnistettavaan tai tunnistettavissa olevaan henkilöön. Näitä tietoja ovat esimerkiksi nimi, puhelinnumero ja sijaintitiedot. Ihmistä tai organisaatiota, joka määrittelee miten ja mihin tarkoitukseen kerättyjä olevia henkilötietoja käsitellään, kutsutaan rekisterinpitäjäksi. Tiedot voivat olla esimerkiksi potilastietoja, verkkokaupan asiakasrekisteri tai vaikka sosiaalisen median palvelu. Henkilötietojen käsittelijällä tarkoitetaan ihmistä tai organisaatiota, joka käytännössä käsittelee henkilötietoja rekisterinpitäjän puolesta. Käsittelijä voi olla esimerkiksi IT-palveluntarjoaja, jolla on pääsy rekisterinpitäjän henkilötietoihin. (Tietosuojavaltuutetun toimisto 2022a.)

Henkilötietojen käsittelyssä on aina noudatettava tietosuojaperiaatteita, jotka on säädetty tietosuojalainsäädännössä. Tietosuojavaltuutetun toimiston ja tietosuojaperiaatteen mukaan henkilötietoja on

- käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi
- käsiteltävä luottamuksellisesti ja turvallisesti
- kerättävä ja käsiteltävä tiettyä, nimenomaista ja laillista tarkoitusta varten
- kerättävä vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- päivitettävä aina tarvittaessa ja epätarkat, sekä virheelliset henkilötiedot on poistettava tai oikaistava viipymättä

- säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. (Tietosuojavaltuutetun toimisto 2022a.)

Tietosuoja-asetus sisältää myös rekisterinpitäjän osoitusvelvollisuuden ja se on yksi keskeisistä periaatteista asetuksessa. Osoitusvelvollisuuden tarkoituksena on osoittaa, miten henkilötietojen käsittelyssä kunnioitetaan kohteena olevien tietosuojaa. Rekisterinpitäjän on myös osoitettava, että tarpeelliset tekniset ja organisaation sisäiset toimenpiteet on täytetty osoitusvelvollisuuden mukaisesti. Esimerkiksi tietoturvaloukkauksessa rekisterinpitäjä voi näyttää, että se on pyrkinyt tunnistamaan ja tehnyt toimenpiteitä tietosuojaan kohdistuvia riskejä varten. (Tietosuojavaltuutetun toimisto 2022b.)

Valvontaviranomaisella on valtuudet antaa huomautuksia ja määrätä sakkoja asetuksessa luetelluista teoista. Sakkoja voidaan määrätä tiettyyn enimmäismäärään asti huomioiden kunkin tapauksen olosuhteet. Hallinnollisen sakon enimmäismäärä on 20 miljoonaa euroa. Jos osuus on tätä suurempi, sakon määrä on 4 prosenttia yrityksen maailmanlaajuisesta kokonaisliikevaihdosta. (Andreasson ym. 2019, 47.)

2.7 Tietosuoja etätyössä

Henkilötietojen käsittelijän oma vastuu tietosuojan huomioimisessa korostuu etätyössä. Pääsääntönä tulee olla, että kaikki etätyöntekijän käsittelemät tiedot tulee olla yhtä suojattuja kuin työnantajan tiloissa. Etätyössä on kuitenkin erityisesti kiinnitettävä huomiota tietosuojan kannalta turvallisiin menettelytapoihin, kun toimitaan työpaikan ulkopuolella, kuten kotona. Jos etätyössä käsitellään luottamuksellisia tietoja, täytyy tietoturvan olla hyvätasoista etenkin silloin, kun etätyöntekijä käsittelee henkilötietoja. (Helle 2004, 195–196.)

Etätyössä voi olla tilanteita, jolloin tietojenkäsittely ei rajoitu vain tietotekniikkaan, vaan voi olla tarvetta käsitellä tietoja esimerkiksi asiakirjojen ja tulosteiden avulla. Tällöin säilytys voi edellyttää erikoisjärjestelyitä tiedon säilytykseen tai tiedon tuhoamiseen liittyen. (Helle 2004, 197.)

Tietoturvallisuuden ja tietosuojan varmistaminen vaatii, että organisaation toimintaohjeet ovat kunnossa. Luonnollisesti oikeat toimintatavat eivät toteudu, jos etätyöntekijä ei ole tietoinen niistä tai etätyöntekijällä on puutteelliset ohjeet (Helle 2004, 195). Liian vähäinen käyttökoulutus henkilötietojen ja niiden käsittelyssä käytettävien tietojärjestelmien käyttöön aiheuttaa viiveitä tietojen käsittelyssä, lisää johdon riskejä myös kustannusten osalta, voi vaarantaa salassapitovelvoitteen ja altistaa työntekijän lankeamaan erilaisiin huijauksiin ja kiristyshaittaohjelmiin. (Andreasson ym. 2019, 116–117.)

2.8 Tietoturva etätyössä

Tietoturva tai kyberturva on käsite, jolla tarkoitetaan tietokonejärjestelmien tietojen, laitteiden ja ohjelmistojen suojaamista varkauksilta ja vahingoittamiselta. Tietoturvaratkaisuilla turvataan tietojen, ohjelmistojen, laitteiden ja niiden laiteohjelmistojen (firmware) eheys, luotettavuus ja saatavuus. (Priyanka 2018, 7.)

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on luonut oppaita organisaatioille ja yrityksille tietoturvan perehdytykseen ja ylläpitämiseen. Yksi opas on suunnattu pienyrityksille. Oppaassa käydään läpi yleisimmät kyberuhat, jotka todennäköisesti ovat pienyritysten haittana. (Traficom 2020a.)

Yksi etätyön huono puoli etätyön kannalta on teknisten ongelmien lisääntyminen ja tietoturvallisuusriskit sekä tiedonhallinta. Useimmat ongelmat ovat hallittavissa hyvän ennakkosuunnittelun avulla. Etätyö voidaan myös järjestää tietoturvalliseksi, mutta se voi edellyttää lisätoimenpiteitä ja lisäkustannuksia. (Helle 2004, 25.)

Työnantajan kannalta etätyön tietoturva on erittäin keskeinen asia, koska etätyö saattaa aiheuttaa ylimääräisiä tietoturvariskejä. Näihin riskeihin on varauduttava etukäteen, ja vastuu tietoturvallisuudessa sekä työnantajalla että työntekijällä. Työntekijän vastuu on toimintatavoissa ja tietojen käsittelyssä. Tietoturvallisuuden järjestäminen on työnantajan vastuulla. Työnantaja myös valitsee ne keinot, joita tiedon suojaamiseen käytetään. Keinot voivat riippua työn luonteesta, suojattavan tiedon tärkeydestä, (esimerkiksi. arkaluonteiset tiedot, kuten

henkilötiedot), käytettävistä välineistä ja tietoliikenneyhteyksistä. Työntekijällä voi muun muassa olla yhteydet suoraan työpaikan sisäverkkoon. (Helle 2004, 192–193.)

Helle (2004) viittaa puitesopimukseen, jossa lähtökohtaisesti työnantaja hankkii etätyöntekijälle tarvittavat työvälineet. Työvälineitä ovat muun muassa tietokone, internet-yhteys, sähköposti jne. Työnantajan on myös tiedotettava etätyöntekijälle mahdollisista rajoituksista liittyen tietoteknisiin työvälineisiin. Lisäksi työnantajan on ilmoitettava mahdollisista seuraamuksista sääntöjen ja rajoitusten laiminlyönneistä. Seuraamukset tulee olla työsopimuslain mukaisia. Mikäli laiminlyöjä on työnantaja, seuraukset eivät voi kohdistua työntekijään. Seuraamukset tässä tapauksessa kohdistuvat työnantajaan itseensä. On myös huomioitava, että tietoturvallisuudesta huolehtiminen on työnantajan vastuulla niissäkin tilanteissa, joissa työntekijä käyttää työntekoon omia henkilökohtaisia välineitään. (Helle 2004, 194–195.)

Yleensä yritykset haluavat suojata etätyöntekijän päätelaitteet ja tietoliikenneyhteydet erilaisilla tietoturvaratkaisuilla. Tietoturvauhilta suojautuminen käydään läpi seuraavassa kappaleessa, ja tietoturvaratkaisuja käsitellään luvussa 3.3.

Yksi tärkeimmistä suositeltavista toimenpiteistä on johdon osallistuminen ja tuki tietosuojassa ja tietoturvassa. Johdon tulee laatia tietoturva- ja tietosuojapolitiikka, jossa selviää johdon näkemys siitä, mitä tavoitteita niille asetetaan. Johdon osallistuminen ja tuki on myös ehdoton edellytys onnistuneelle tietosuojalle ja tietoturvalle. (Andreasson ym. 2019, 109.)

Tietoturva- ja tietosuojapolitiikan lisäksi on hyvä laatia kyberturvallisuusstrategia, jossa on kysymys liiketoiminnan turvaamisesta normaalissa ja häiriötilanteessa. Sillä voidaan priorisoida toimenpiteitä ja proaktiivisesti reagoida kyberturvallisuuteen. Se on myös tärkeä osa turvallisuuden johtamista. Siinä on huomioitava yrityksen tietoturva- ja tietosuojapolitiikan tavoitteet ja prioriteetit, jotta kyberturvallisuusstrategian toimenpiteet tukevat niitä. Kyberturvallisuusstrategian on hyvä sisältää seuraavat asiat: häiriötilanteiden kestäminen nyt ja tulevaisuudessa, tietoturvan kulut, mainehaitan ja menetetyn liikevaihdon arvo, todennäköisimmät uhat ja niistä palautuminen, kyberturvan haluttu taso ja mitkä lait ja asetukset tulee ottaa huomioon. (TIVIA 2022.)

Traficomin Kyberturvallisuuskeskus kannustaa yrityksiä ottamaan kyberturvallisuuden osaksi yrityksen tavoitteita ja sisällyttämään sen riskinhallintaprosesseihin. Kyberturvallisuus vaikuttaa yritykseen kokonaisvaltaisesti, koska yritys on usein riippuvainen digitaalisten palveluiden turvallisuudesta monin eri tavoin. Näitä ovat muun muassa sähköpostipalvelut ja ohjelmistot. (Traficom 2020b.)

3 YLEISET TIETOTURVAUHAT JA VARAUTUMINEN

3.1 Tietojenkalastelu

Tietojenkalastelu tai englanniksi ”phishing” on vakiintunut käsite ja metodi, jolla tarkoitetaan huijausta, jossa rikollinen pyrkii saamaan vastaanottajan luovuttamaan tietoja. Hyökkäyksissä käytetään hyväksi sosiaalista manipulointia, joka on englanniksi ”social engineering”. (Mitre, 2022.)

Huijattavat tiedot voivat olla käyttäjätunnuksia eri palveluihin tai järjestelmiin, pankki- tai luottokorttitietoja ja muita henkilökohtaisia tietoja. Huijauksissa yleensä käytetään sähköpostia ja naamioitua verkko- ja kirjautumissivustoa, johon vastaanottajan tietoja pyritään keräämään. (Microsoft 2022d.)

Vuodettuja tietoja yleensä kaupataan rikollisten käyttämillä kauppapaikoilla, sekä niitä jaetaan suurina tietokantoina julkisesti (Traficom 2022b).

Kyberturvallisuuskeskus (Traficom 2022a) kuvaa tietojenkalastelun anatomiaa seuraavasti:

Kuvio 4. Tietojenkalastelun anatomiaa (Traficom 2019).

Tietojenkalastelu voi olla kohdistettua, jota kutsutaan englanniksi termillä ”spearphishing”. Kohdistetussa tietojenkalastelussa kalastellaan tiettyä yritystä tai sen työntekijöitä kohdistetusti lähettämällä yleensä sähköpostiviesti, joka sisältää haitallisen liitetiedoston tai linkin. Haitallisella liitetiedostolla pyritään siihen, että käyttäjä saadaan suorittamaan haitallista koodia yrityksen järjestelmässä. Haitallinen tiedosto tai koodi voidaan myös ajaa haitallisesta linkistä. Yleisimmin tietojenkalastelussa käytetään ei-kohdistettua tapaa, kuten sähköpostien massalähetystä, joista yleensä käytetään nimitystä tietojenkalastelukampanja. Kampanjassa voidaan käyttää kolmannen osapuolen palvelua, kuten sosiaalisen median alustoja. (Mitre 2022.)

3.2 Haittaohjelmat

Haittaohjelma on sovellus tai koodi, jolla halutaan vahingoittaa, häiritä tai kerätä tietoja luvattomasti päätelaitteista ja muista järjestelmistä. Haittaohjelmien yleisimpiä tyyppejä ovat

- virukset
- makrovirukset
- tietokonemadot (worm)
- troijalaiset
- mainosrahoitteiset haittaohjelmat
- vakoiluohjelmat
- kiristyshaittaohjelmat.

Virukset ovat yksinkertaisin muoto haittaohjelmista. Se on käytännössä yksinkertainen tietokoneohjelma, joka ladataan ja käynnistetään ilman käyttäjän lupaa. Virukset voidaan luokitella kolmeen eri luokkaan kohderyhmän mukaan:

- käynnistyssektorivirus (boot sector virus)
- tiedostovirus (file virus)
- makrovirus tai makrohaittaohjelma (macro virus). (Priyanka, 2018, 9.)

Käynnistyssektorivirus on ns. koodinpätkä, joka korvaa tietokoneen MBR- eli Master Boot Record -käynnistyssektorin, joka sijaitsee kiintolevyn ensimmäisessä sektorissa, ja se suoritetaan aina, kun tietokone käynnistetään. (Priyanka, 2018, 9.)

Tiedostovirus on yleisin viruksen muoto. Ne toimivat käyttöjärjestelmän tiedostojärjestelmässä, jossa ne tartuttavat suoritettavia ohjelmia ja ne suoritetaan aina, kun tartutettu ohjelmisto käynnistetään. (Priyanka, 2018, 9.)

Makroviruksia käytetään dokumenttitiedostoissa ja dokumenttimallitiedostoissa, joissa voidaan käyttää makroja. Makro on ohjelmointikieli, joka on sisällytetty ohjelmiin, kuten Microsoft Word

ja Excel. Makrovirus voidaan automaattisesti suorittaa joka kerta, kun dokumentti on avattu ohjelmassa. (Priyanka, 2018, 9.)

Tietokonemato on itseään toistava ja leviävä itsenäinen sovellus. Yleensä se osaa itse käynnistyä ja monistaa itseään verkossa, eikä se välttämättä tarvitse ihmisen toimenpiteitä. Madot voidaan kuitenkin luokitella aktivointitapojen mukaan seuraavasti:

- Ihmisen aktivoima – hitain aktivointitapa, koska siinä vaaditaan ihmisen toimia
- Ihmisen aktiivisuuteen perustuva aktivointitapa – esimerkiksi mato aktivoituu tietyn sovelluksen käynnistyksen yhteydessä
- ajastetun prosessin aktivoituminen – aktivointitapa riippuu järjestelmän aikataulutetusta prosessista, kuten automaattisesta ohjelmistolatauksesta
- itseaktivointi – tämä on nopein aktivointitapa, jossa mato käynnistyy hyödyntämällä aina käynnissä olevien ohjelmistojen haavoittuvuuksia (Priyanka 2018, 11–12.)

Yleensä madoilla ei ole mitään ns. painolastia, vaan ne aiheuttavat häiriöitä tietokoneessa ja verkkoliikenteessä. Joskus madot voivat avata ns. takaportin (backdoor) uhrin tietokoneeseen, jota rikolliset voivat hyödyntää ottamalla etäyhteyden uhrin tietokoneeseen. Jotkut madot muuttavat uhrin tietokoneen roskapostin välittäjäpalvelimeksi. (Priyanka 2018, 12.)

Troijalaiset ovat nimensä mukaan naamioituja sovelluksia tai tiedostoja, jotka yleensä näyttävät aidoilta ja harmittomilta. Troijalaiset yleensä aiheuttavat erilaisia tuhoja tai häiriöitä tietokoneella, kuten tiedostojen poistoja tai käyttöjärjestelmän rampauttamisen. Erona viruksiin ja matoihin on se, että troijalaiset eivät monistu itsestään vaan luottavat loppukäyttäjän toimiin aktivoituakseen. (Priyanka 2018, 14–15.)

Mainosrahoitteisten ja vakoiluhaittaohjelmien tarkoitus on kerätä henkilökohtaista dataa tietokoneelta ilman käyttäjän lupaa, sekä näyttävät mainoksia sekä uudelleenohjaavat hakutuloksia mainosrahoitteisille sivuille. Vakoiluohjelmat keräävät tietoja käyttäjän huomaamatta ja lähettävät ne kolmansille osapuolille. Ne voivat myös osittain ottaa kohdetietokoneen käyttöönsä. (Priyanka 2018, 18–19.)

Kiristyshaittaohjelmat ovat haittaohjelmia, jotka pyrkivät salaamaan kaikki tai tietyntyyppiset datat kohdejärjestelmästä. Tiedostot ovat käyttökelvottomia, ja niiden salauksen avaamista vastaan pyydetään lunnaita. (Priyanka 2018, 19.)

3.3 Tekninen varautuminen ja suojausmalli

On tärkeää varautua mutta myös ennaltaehkäistä tietoturvauhkia erilaisilla teknisillä toimilla ja ratkaisuilla. Lisäksi erilaiset suojausmallit tukevat teknisten ratkaisuiden toimintaa tai tehostavat niitä. Esimerkiksi IBM (2022a) suosittelee X-Force Threat Intelligence -raportissaan vähentämään tietoturvauhkien riskejä Zero Trust -suojausmallin avulla.

3.3.1 Tekniset toimet

Haittaohjelmia, etenkin kiristyshaittaohjelmia varten kriittisten ja liiketoiminalle elintärkeiden järjestelmien säännöllinen ja automaattinen varmuuskopiointi on tärkeää. Varmuuskopioita suositellaan säilytettävän 3-2-1 sääntöä noudattaen eli kolme kopiota kahdessa eri muodossa tai tallennusmediassa ja yksi kopioista täysin poissa verkossa. Varmuuskopioiden testaus ja palauttamisen harjoittelu on tärkeää tehdä säännöllisesti. (Traficom 2022e.)

Verkot tulisi erotella eli segmentoida ja varmistaa, että yrityksen hyökkäyspinta on mahdollisimman pieni. Hyökkäykset kannattaa pyrkiä havaitsemaan mahdollisimman aikaisessa vaiheessa keskitettyjen valvontaratkaisuiden avulla. (Traficom 2022e.)

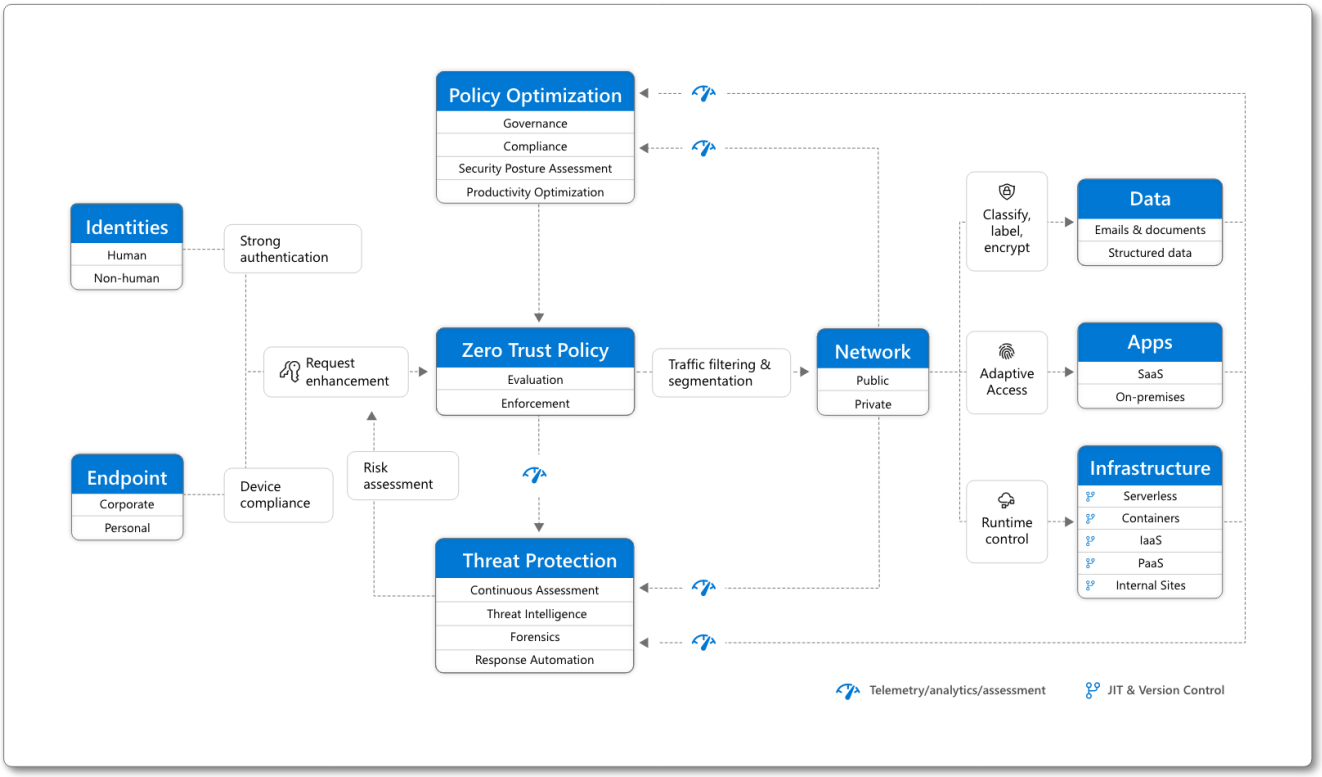
Päätelaitteille kannattaa asentaa EDR eli Endpoint Detection and Response -ominaisuutta käyttävät tietoturvaohjelmistot, joiden avulla voidaan tutkia epäiltyjä tietoturvaongelmia ja tarvittaessa eristää tietokone pois verkosta. Käyttöön kannattaa ottaa roskapostisuodatin, joka suodattaa haitallista sisältöä sisältävät sähköpostiviestit ja muut ei-toivotut sekä roskapostiviestit. Lisäksi suositellaan ottamaan käyttöön keskitetty lokienhallintaratkaisu, jolla voidaan tehokkaasti havaita ja tutkia tietoturvauhkia. (Traficom 2022e.)

3.3.2 Zero Trust -suojausmalli

Zero Trust on moderni suojautumismalli, jonka on kehittänyt entinen Forrester-analyytikko John Kindervag vuonna 2010. Zero Trust -suojausmallista on tullut yksi suosituimmista nykyaikaisista kyberturvallisuuden rajapinnoista. (Varonis 2022.)

Käytännössä Zero Trust -suojautumismallin päätarkoituksena on, ettei luoteta mihinkään, edes käyttäjiin, palomuurin takana. Tämä varsinkin sen takia, koska sisäverkon uhat, kuten käyttäjätunnusten tietoturvavuodot, ovat tehneet rikollisille tietoturvamurrot yritysten sisäverkkoihin triviaaliksi. Kaiken Zero Trustin keskiössä on yrityksen arvokas data. (Varonis 2022.)

Microsoft (2022c) kannustaa yrityksiä omaksumaan Zero Trust -suojausmallin, koska se soveltuu tehokkaasti yritysten nykyisiin monimutkaisiin moderneihin ympäristöihin, kannustaa tekemään etätöitä sekä suojelee käyttäjiä, laitteita ja dataa riippumatta niiden sijainnista. Microsoftin mukaan Zero Trust -suojausmalli opettaa meitä: ”Älä koskaan luota vaan tarkista aina”.



Kuvio 5. Microsoftin kuvio Zero Trust -suojausmallista (Microsoft 2022c).

Oheisen kuvion mukaan Zero Trust -suojausmalli käsittää tietoturvan suojauksen kokonaisuutena. Esimerkiksi päätelaitteet luokitellaan yrityksen omaksi tai työntekijän henkilökohtaiseksi laitteeksi, ja niiden yhteensopivuustilaa käytetään tarkistettavana seikkana. Identiteetti määritellään sen perusteella, onko se ihminen vai ei. Identiteetin pääsynhallinnassa vaaditaan vahva tunnistautuminen, kuten monivaiheinen tunnistautuminen (MFA). Pääsynhallintaan vaikuttaa myös uhkien hallinta ja identiteetin riskitaso. Verkko segmentoidaan ja kaikki verkkoliikenne suodatetaan ja pyritään tunnistamaan. Vain tunnistettu ja hyväksytty liikenne päästetään läpi. Data, kuten sähköpostit ja dokumentit, sekä esimerkiksi tietokannat luokitellaan, korvamerkitään tai kryptataan. Adaptiivinen pääsynhallinta varmistaa oikeiden henkilöiden pääsyn organisaation sisäisiin ja SaaS-palveluihin. Organisaation IT-infrastruktuurissa käytetään ”just-in-time” (JIT) eli tarveperusteista pääsynhallintaa ja suoritustenaikaista hallintaa, jolloin pääsy on sallittu vain silloin, kun pääsylle on tarve Perinteisissä järjestelmissä esim. virtuaalikoneiden etähallintaportit voivat olla aina auki. Kokonaisuuden hallintaa ja yhteensopivuutta parannetaan politiikkojen eli käytäntöjen optimoinnilla. (Microsoft 2022c.)

4 TUTKIMUSMENETELMÄ JA TOTEUTUS

4.1 Tutkimuksen taustaa

Tässä työssä käytetään aineiston keräämiseen ja analysointiin kyselytutkimusta, jossa tavoitteena on saada otanta kyselyyn vastanneiden yritysten osalta etätyön tietoturvan ja tietosuojan tilanteesta. Lisäksi kartoitetaan eri tietoturva- ja etätyöratkaisuiden käyttöä. Kyselyssä kartoitetaan myös yrityksen etätyön tarpeen kasvua viimeisen kahden vuoden aikana, tietoturvaohjeistuksen ja perehdytyksen saatavuutta sekä tietosuojan huomiointia etätyössä. Kyselyn avulla saadaan myös välitöntä tietoa yrityksen toiminnasta ja käyttäytymisestä liittyen etätyöhön. Kyselyllä tarkoitetaan tapaa kerätä aineistoa standardoidusti ja jossa otoksen sekä näytteen muodostavat kohdehenkilöiden perusjoukko. (Hirsjärvi, Remes & Sajavaara 2009, 193.)

Kyselyn aineistoa käsitellään yleensä kvantitatiivisesti. (Hirsjärvi ym., 194). Kvantitatiivinen tutkimus tarkoittaa Survey-tutkimusstrategiaa, jossa kerätään tietoa standardoidussa muodossa tietyltä joukolta ihmisiä. Kyseisen tutkimusstrategian tyypillisiä piirteitä ovat:

- Tietystä ihmisjoukosta poimitaan otos yksilöitä.
- Kerätään aineisto jokaiselta yksilöltä strukturoidussa muodossa.
- Käytetään tavallisesti kyselylomaketta tai strukturoitua haastattelua.
- Kerätyn aineiston avulla pyritään kuvailemaan, vertailemaan ja selittämään ilmiöitä. (Hirsjärvi ym. 2009, 134.)

Kvantitatiivisen (määrällisen) tutkimuksen lisäksi on kvalitatiivinen (laadullinen) tutkimus, ja ne ovat lähestymistapoja, joita on vaikea tarkkajakoisesti erottaa toisistaan. Ne voidaan myös kuvailla toisiaan täydentävinä suuntauksina, eikä kilpaileviksi suuntauksiksi. (Hirsjärvi ym. 2009, 136.)

Keskeisiä johtopäätöksiä kvantitatiivisessa tutkimuksessa ovat:

- Johtopäätökset aiemmista tutkimuksista ja teorioista, käsitteiden määrittäminen ja hypoteesin esittäminen

- Aineiston keruun suunnitelma, joka soveltuu määrälliseen ja numeeriseen mittaamiseen
- Tutkittavien henkilöiden valinta, perusjoukon muodostaminen, johon tulosten tulee päteä, ja otetaan tästä joukosta otos
- Tulosten tai aineistojen muodostaminen taulukkomuotoon ja tilastollisesti käsiteltävään muotoon
- Johtopäätösten teko havaintoaineistojen tilastolliseen analysointiin perustuen. (Hirsjärvi ym. 2009, 140.)

4.2 Kyselyn muodot

Kyselytutkimuksen aineistoa voidaan kerätä ainakin kahdella eri tapaa: posti- tai verkkokyselyllä tai kontrolloituna kyselynä. Käytännössä posti- tai verkkokyselyssä kyselylomake toimitetaan vastaajille, ja vastattuaan he palauttavat lomakkeen takaisin tutkijalle. Jos kyseessä on kirjeellä toimitettu lomake, on huomioitava, että kirjeen palautuksen postimaksu tulee olla valmiiksi maksettu. Siitä on syytä huomauttaa lähetekirjeessä. Posti- tai verkkokyselyssä suurin ongelma on kato, jonka takia tutkija joutuu yleensä karhuamaan vastauksia, yleensä kahteen kertaan. Hyötynä karhuamisesta on vastausprosentin nousu jopa 70–80 prosenttiin. (Hirsjärvi ym. 2009, 196.)

Toisena muotona pidetään kontrolloitua kyselyä, jossa kyselyjä on kahdenlaisia. Kyselyn muoto, jossa tutkija jakaa lomakkeet henkilökohtaisesti, kutsutaan informoiduksi kyselyksi. Käytännössä tutkija menee yrityksiin, messuille, koulutustilaisuuksiin tai sellaisiin paikkoihin, jossa kyselytutkimuksen kohdejoukot ovat lähtökohtaisesti tavoitettavissa. Toinen muoto on henkilökohtaisesti tarkistettu kysely. Siinä tutkija on lähettänyt lomakkeet henkilökohtaisesti ja jopa tarvittaessa noutaa ne itse ilmoitetun ajan kuluttua vastaajilta. (Hirsjärvi ym. 2009, 197.)

4.3 Edut ja haitat

Kyselytutkimuksen etuja on, että niiden avulla voidaan kerätä laaja tutkimusaineisto. Kyselytutkimukseen voidaan saada paljon henkilöitä, ja se voi sisältää monia eri kysymyksiä. Se on

myös yleensä tehokas ja säästää tutkimuksen tekijän aikaa ja vaivaa. Kyselytutkimuksen analysointi on myös yleensä vaivatonta, koska tieto voidaan helposti ja nopeasti käsitellä tallennettuun muotoon. Tämä vaatii, että kyselylomake on suunniteltu huolellisesti analysointia huomioiden. (Hirsjärvi ym. 2009, 195.)

Kyselytutkimuksen huonot puolet ovat Hirsjärven mukaan kyselytutkimuksen pinnallisuus ja teoreettinen vaatimattomuus. Tutkimukseen liittyy myös haittoja, kuten vastaajien inhimilliset seikat. Esimerkiksi ei ole varmaa, ovatko vastaajat vastanneet kyselyyn rehellisesti ja tarpeeksi huolellisesti. Myös riski kysymyksien väärinymmärtämisestä on olemassa. Lisäksi ei voida tietää, miten vastaajat ovat perillä tai kuinka hyvin kysyttävään asiaan on perehdytty. Kyselytutkimus vaatii myös hyvän lomakkeen ja kysymykset, mikä taas vaatii kyselyn tekijältä tietoa ja taitoa. Yksi haittaava seikka on myös kyselyyn vastaamattomuus eli kato, jolloin kyselyyn ei saada tarpeeksi vastauksia. (Hirsjärvi ym. 2009, 195.)

4.4 Toteutus

Kyselytutkimus toteutettiin kontrolloituna kyselynä ja kyselyt toimitettiin henkilökohtaisesti sähköpostitse, mutta vastaukset kerättiin anonyymisti. Kyselystä ei siis voi päätellä vastaajan henkilöllisyyttä tai hänen edustamaansa yritystä. Kyselyyn valittiin joukko pk-yrityksiä ja niiden tiedossani olevia IT-asiantuntijoita tai IT-asioista vastaavia henkilöitä. Kysely lähetettiin 21 yritykselle kahdessa erässä 11. ja 19.10.2022.

Tämä opinnäytetyö toteutettiin hyödyntäen kvantitatiivista tutkimusmenetelmää. Kvantitatiivisista tutkimusmenetelmistä tässä työssä käytettiin standardoitua sähköistä lomakekyselyä. Kysely toteutettiin strukturoituna eli suljettuna kyselynä, jossa vastausvaihtoehdot oli annettu valmiiksi. Tämän tyyppisten kysymysten tarkoitus on helpottaa vastausten käsittelyä ja vähentää virheiden määrää. Jos vastausvaihtoehtoja on vain kaksi, puhutaan dikotomisesta kysymyksestä, ja kun vastausvaihtoehtoja on useita, puhutaan monivalintakysymyksestä. (Heikkilä 2014a, 49.)

Aineistonkeruumenetelmänä käytettiin Webropol-kysely- ja raportointityökalua. Webropol soveltuu kyselyihin, joissa on mahdollista saada edustava aineisto aikaan eli perusjoukon

jäsenillä on mahdollista käyttää internetiä. Se on helppokäyttöinen ohjelmisto tiedon keräämiseen, analysointiin, ja raportointiin ja tulokset ovat käytettävissä reaaliajassa (Heikkilä 2014b).

Kysely koostui kahdestakymmenestä strukturoidusta kysymyksestä, joissa osassa kysymyksistä oli käytössä yksi valittava vaihtoehto ja osassa monivalintainen. Osassa strukturoiduissa kysymyksissä hyödynnettiin myös Likertin-asteikkoa, jossa asteikot ovat tavallisesti viisi- tai seitsemänportaisia. Asteikkoihin perustuvassa kysymystyypissä esitetään väittämiä ja vastaaja valitsee asteikon vaihtoehdoista sen, josta hän on voimakkaasti samaa mieltä. (Hirsjärvi ym. 2009, 200.)

Taulukko 1. Esimerkki Likertin asteikosta.

1.	Kysymys	2.	Kysymys	3.	Kysymys
X	täysin samaa mieltä		täysin samaa mieltä		täysin samaa mieltä
	jokseekin samaa mieltä		jokseekin samaa mieltä		jokseekin samaa mieltä
	neutraali kanta		neutraali kanta		neutraali kanta
	jokseekin eri mieltä	X	jokseekin eri mieltä		jokseekin eri mieltä
	täysin eri mieltä		täysin eri mieltä		täysin eri mieltä
	ei osaa sanoa		ei osaa sanoa	X	ei osaa sanoa

5 KYSYMYKSET JA TULOKSET

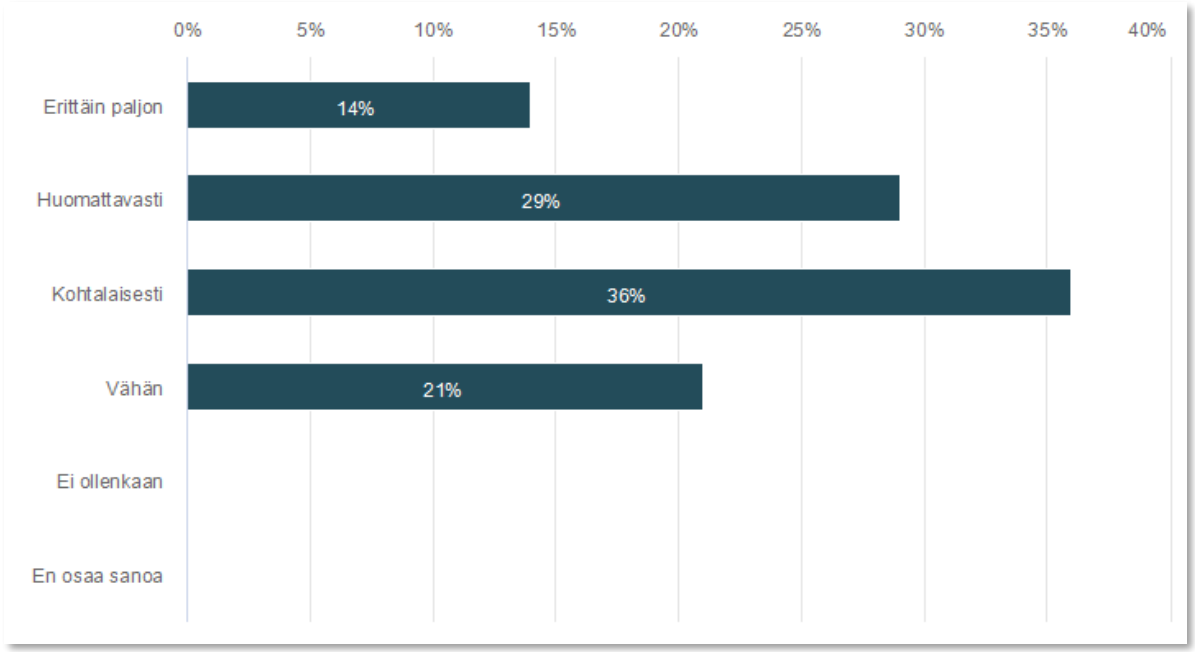
Kyselyyn saatiin määräaikaan (23.10.2022) mennessä 14 vastausta, eli kyselytutkimukseen vastasi n. 67 % kyselytutkimukseen pyydetyistä yrityksistä.

Kyselyn kysymykset voidaan karkeasti jakaa kolmeen osaan. Ensimmäisessä osassa kysymykset kohdistuivat etätyön tarpeen muutokseen ja etätyön mahdollistamiseen. Toisessa osassa kysymykset liittyivät yrityksen tietoturvan ja tietosuojan huomioimiseen ja kolmannessa osassa käytettyihin tietoturvaratkaisuihin.

5.1 Kysymykset etätyön tarpeen muutoksesta ja sen mahdollistamisesta

Ensimmäisessä kysymyksessä kysyttiin etätyön tarpeen kasvamisesta yrityksessä kahden viimeisen vuoden aikana.

Kysymys 1: Onko etätyön tarve kasvanut pysyvästi yrityksessänne viimeisen kahden vuoden aikana?

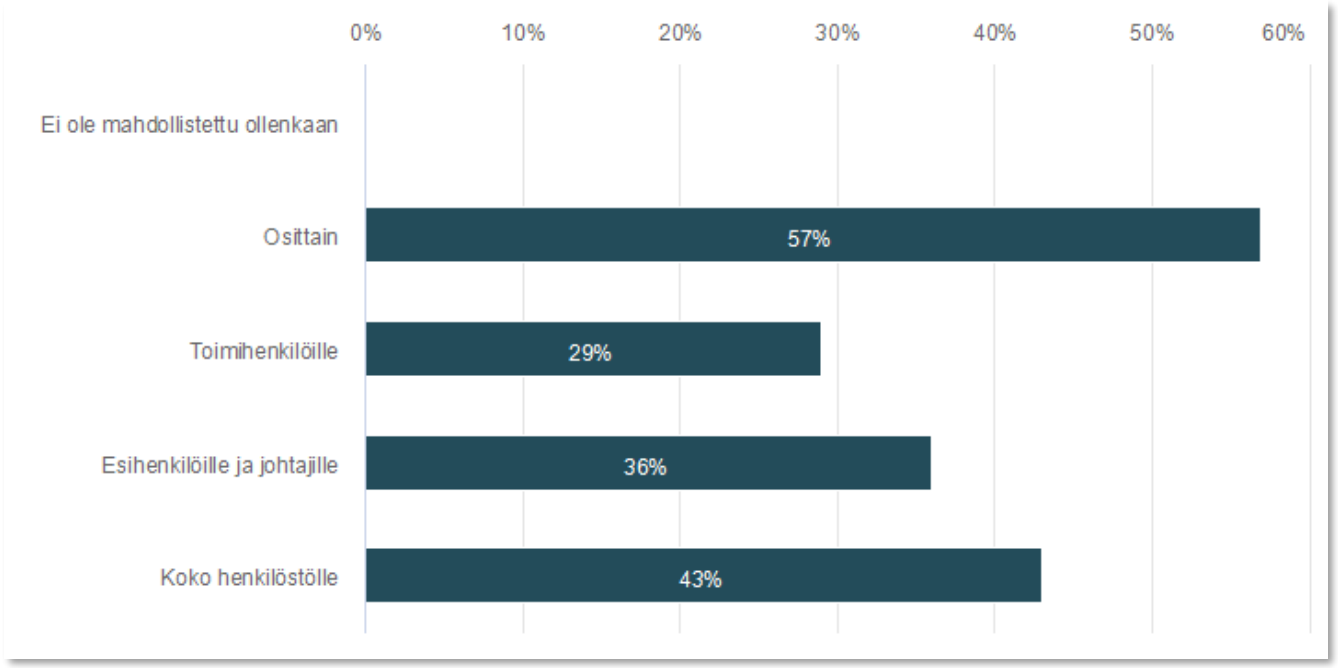


Kuvio 6. Etätyön tarpeen kasvu viimeisen kahden vuoden aikana vastaajayrityksissä.

Kyselyn vastaajista suurin osa koki, että tarve on kasvanut vähintään kohtalaisesti tai huomattavasti. 14 prosenttia vastaajista koki tarpeen kasvaneen erittäin paljon ja 21 % vain vähän. Vastauksissa on huomioitava COVID-19-taudin aiheuttaman pandemian vaikutus viimeisen kahden vuoden aikana, sillä se on todennäköisesti vaikuttanut etätyön tarpeen kasvuun vastaajayrityksissä.

Toisessa kysymyksessä kartoitettiin yrityksen etätyön mahdollistamisen laajuutta. Tämä kysymys oli moniosainen ja sisälsi säännön, jossa vastaajan piti täsmentää vastausta, jos hän vastasi vaihtoehdon ”osittain”. Tällöin vastaajalle tuli myös vastausta täsmentävät vaihtoehdot: ”toimihenkilöille” ja ”esihenkilöille ja johtajille”.

Kysymys 2: Miten laajasti yrityksessänne on mahdollistettu etätyötä?



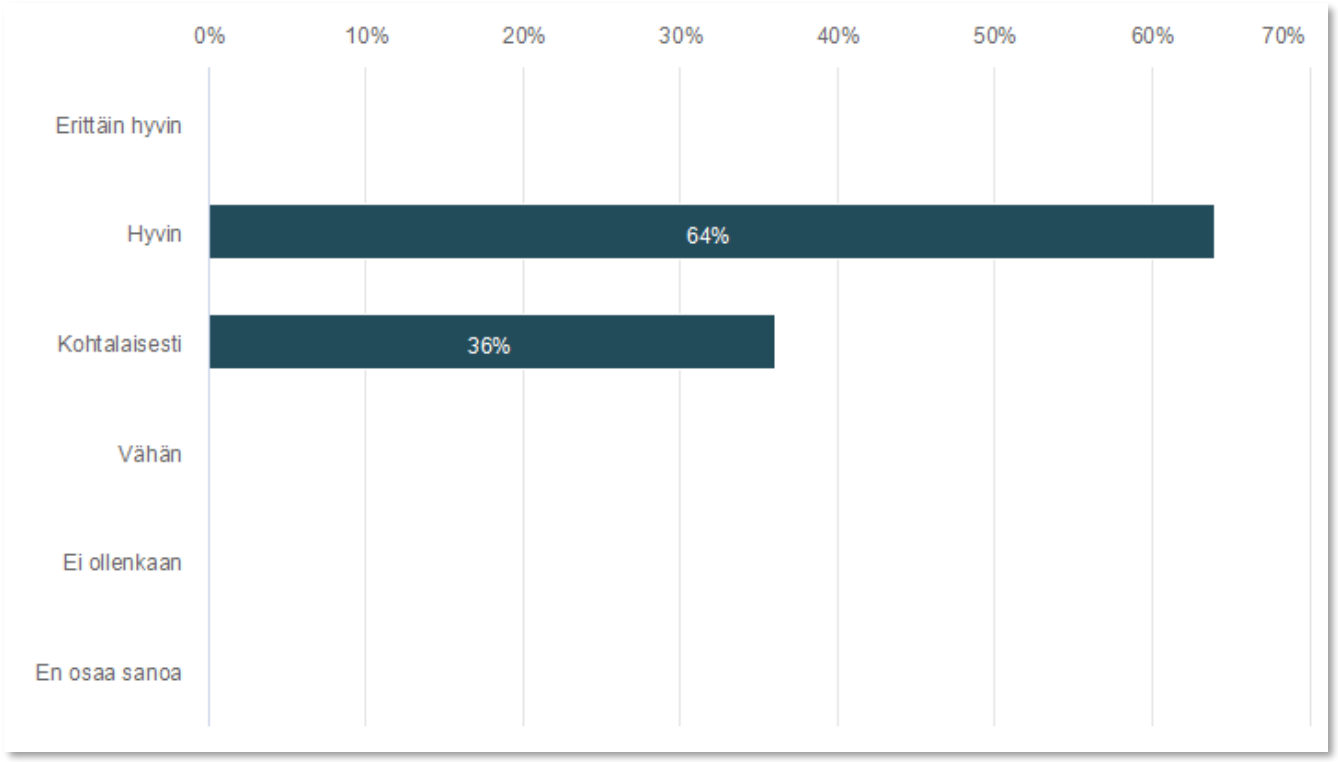
Kuvio 7. Etätyön mahdollistaminen vastaajayrityksissä.

Positiivista oli, että kaikissa kyselyyn vastanneista yrityksissä oli mahdollistettu etätyötä. Yli puolet (57 %) vastaajayrityksistä oli mahdollistanut osittain joista 29 prosenttia toimihenkilöille ja 36 prosenttia esihenkilöille ja johtajille, kun taas 43 prosentilla vastaajayrityksistä etätyö oli mahdollistettu koko henkilöstölle.

5.2 Kysymykset tietoturvan ja tietosuojan huomioimisesta

Kolmannesta kysymyksestä alkaen keskityttiin yrityksen tietoturvan ja tietosuojan tilanteen kartoittamiseen. Kyselyn kolmannessa kysymyksessä kartoitettiin, kuinka hyvin tietoturva oli huomioitu etätyössä.

Kysymys 3. Kuinka hyvin tietoturva on huomioitu etätyössä?

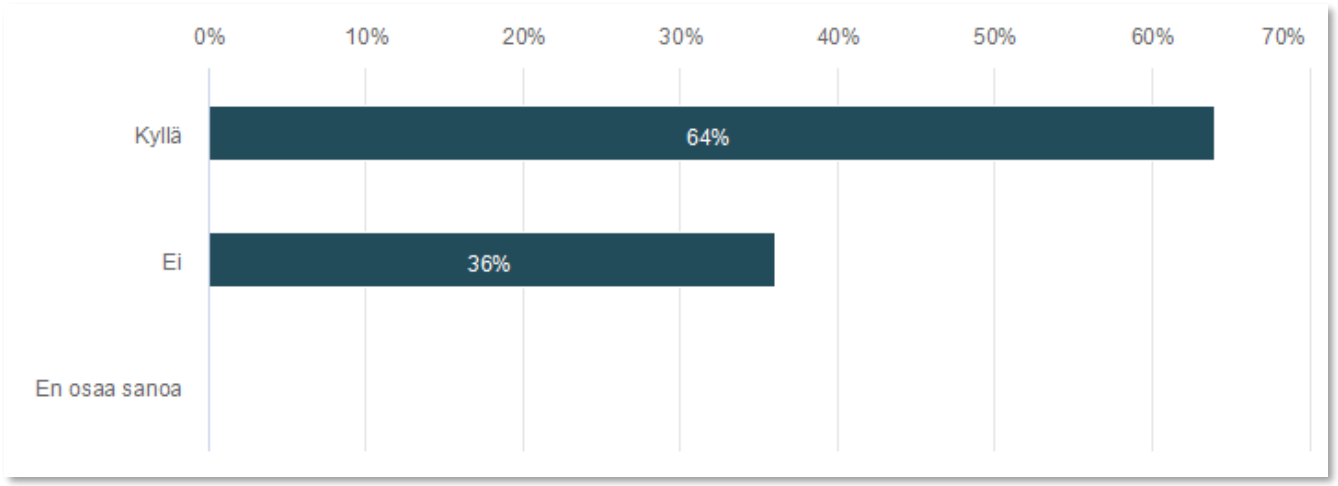


Kuvio 8. Tietoturvan huomioiminen etätyössä vastaajayrityksissä.

Suurin osa eli 64 prosenttia vastaajista koki, että etäyön tietoturva oli huomioitu hyvin yrityksessä, ja 36 prosenttia koki, että vähintään kohtalaisesti. Vastauksista positiivista oli, se että kukaan ei kokenut etätyön tietoturvan jääneen huomioimatta yrityksessä. Vastauksista voi myös päätellä, että etätyön tietoturvassa on kuitenkin parantamisen varaa, koska kukaan vastaajista ei kokenut etätyön tietoturvan tilan olevan huomioitu erittäin hyvin.

Neljännessä kysymyksessä kysyttiin, onko yrityksessä käytössä ohjeistusta etätyön käytännöistä ja tietoturvasta. Vastausvaihtoehdot olivat tässä kysymyksessä: kyllä, ei tai en osaa sanoa.

Kysymys 4. Onko yrityksessä käytössä ohjeistusta etätyön käytännöistä ja tietoturvasta?

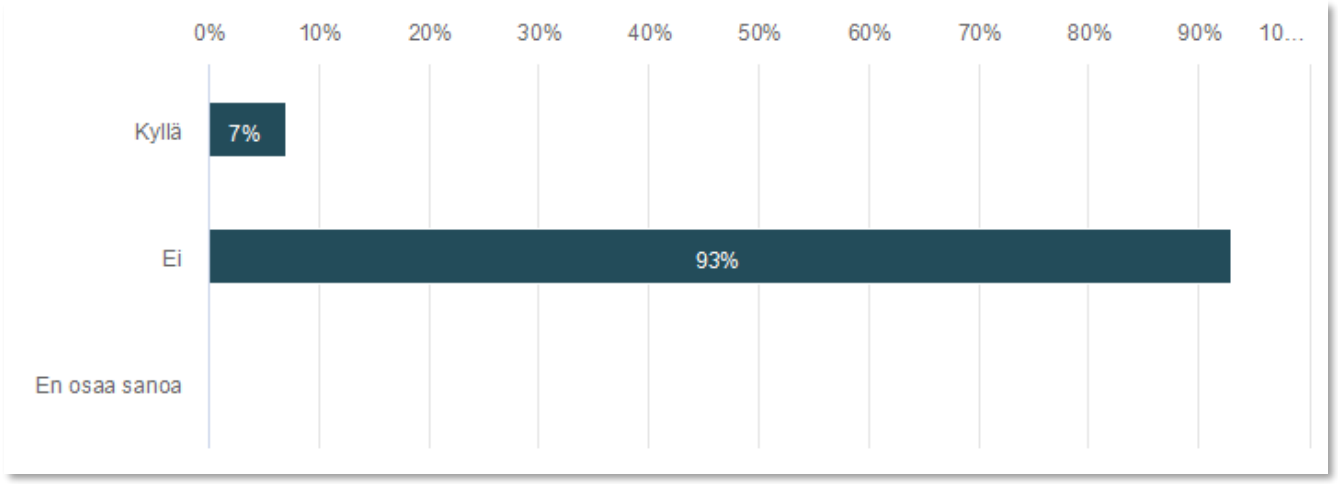


Kuvio 9. Ohjeistuksen käyttö etätyön käytännöistä ja tietoturvasta vastaajayrityksissä.

Suurin osa vastaajista oli sitä mieltä, että yrityksessä oli käytössä ohjeistus etätyön käytännöistä ja tietoturvasta, joka oli positiivinen yllätys. Toki 36 prosentilla vastanneista ei ollut ohjeistusta käytössä ollenkaan. Kuten aikaisemmin luvussa 2.8 mainittiin, on erittäin tärkeää, että ohjeistus on laadittu ja käytössä.

Viidennessä kysymyksessä tiedusteltiin tietoturvatietämyksen testaamista säännöllisesti esimerkiksi henkilöstön tietoturvatesteillä. Kysymykseen oli myös lisätty selite, jossa täsmennettiin tietoturvatestin olevan esimerkiksi simuloitu tietojenkalasteluviesti tai vastaava.

Kysymys 5: Testataanko käyttäjien tietoturvatietämystä säännöllisesti, esimerkiksi henkilöstön tietoturvatesteillä?

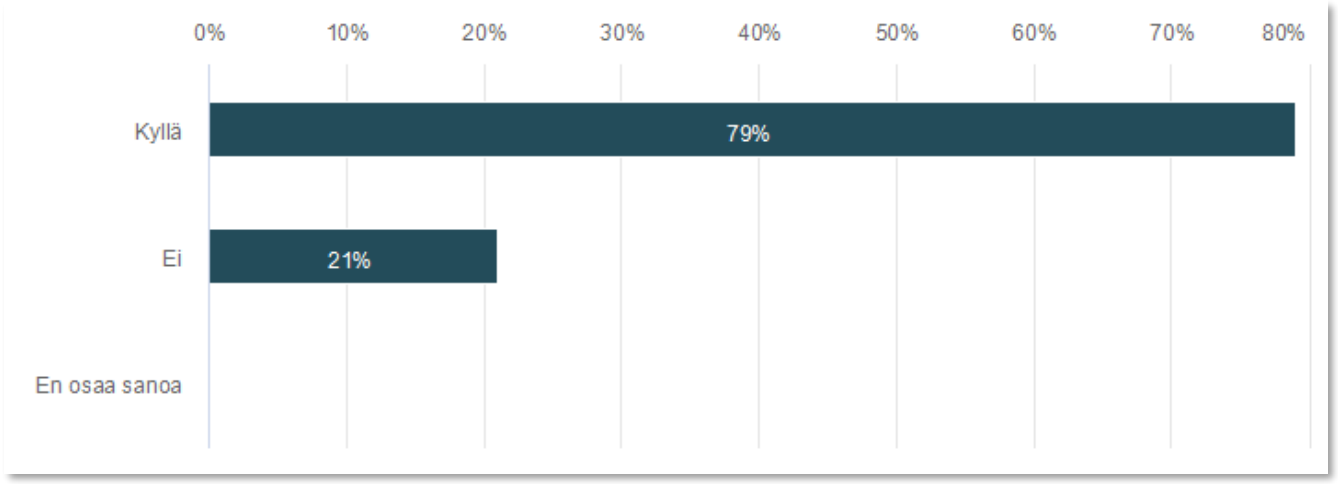


Kuvio 10. Säännöllinen henkilöstön tietoturvatietämyksen testaaminen tietoturvatesteillä vastaajayrityksissä.

Vain seitsemässä prosentissa vastanneista yrityksistä oli käytössä tietoturvatesti, jolla testattiin henkilöstön tietoturvatietämystä säännöllisesti. Vastanneista jopa 93 prosenttia ei testaa henkilöstöä säännöllisesti.

Kuudennessa kysymyksessä kysyttiin uuden työntekijän perehdyttämisestä myös tietoturvan ja tietosuojan käytännöistä etätyössä.

Kysymys 6: Huomioidaanko uuden työntekijän perehdytyksessä myös tietoturvan ja tietosuojan käytännöistä etätyössä?

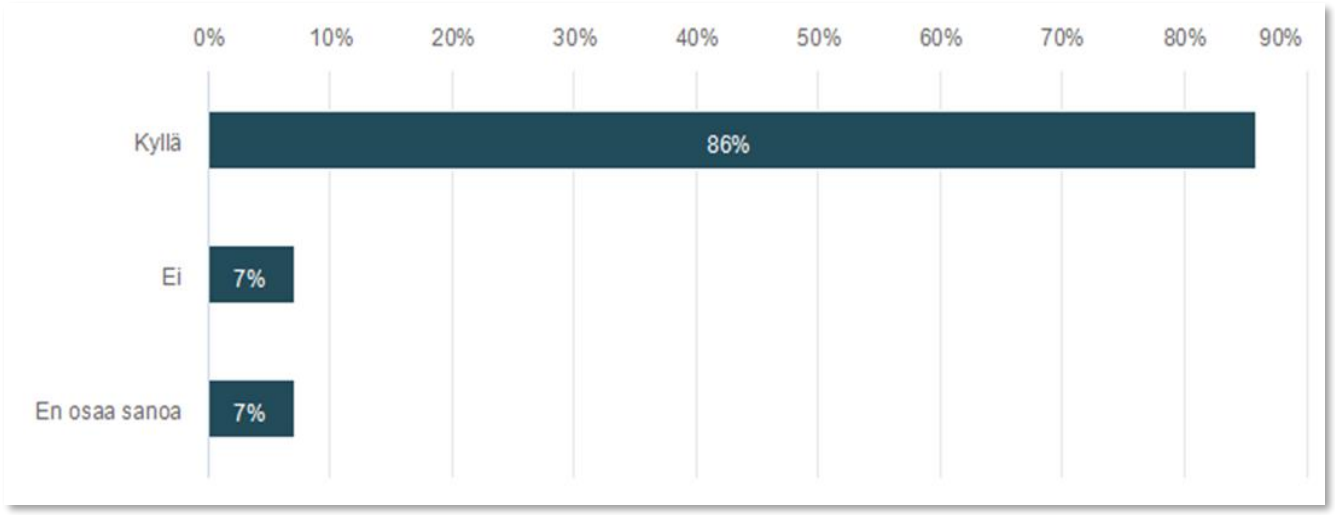


Kuvio 11. Tietoturvan ja tietosuojan huomioiminen uuden työntekijän perehdytyksessä vastaajayrityksissä.

Suurimmassa (79 %) osassa vastanneista yrityksistä uuden työntekijän perehdytys etätyön tietoturvan ja tietosuojan osalta oli kunnossa. Lopuilla vastaajayrityksistä ei ollut asiaa huomioitu.

Seitsemännessä kysymyksessä täsmennettiin tietosuojan huomioon ottamista myös etätyössä. Kysymystä tarkennettiin selitteellä, jossa annettiin esimerkiksi henkilötietosuoja ja GDPR. Selitteellä haluttiin kysymyksen keskittyvän näihin käsitteisiin.

Kysymys 7: Onko tietosuoja otettu huomioon myös etätyössä?

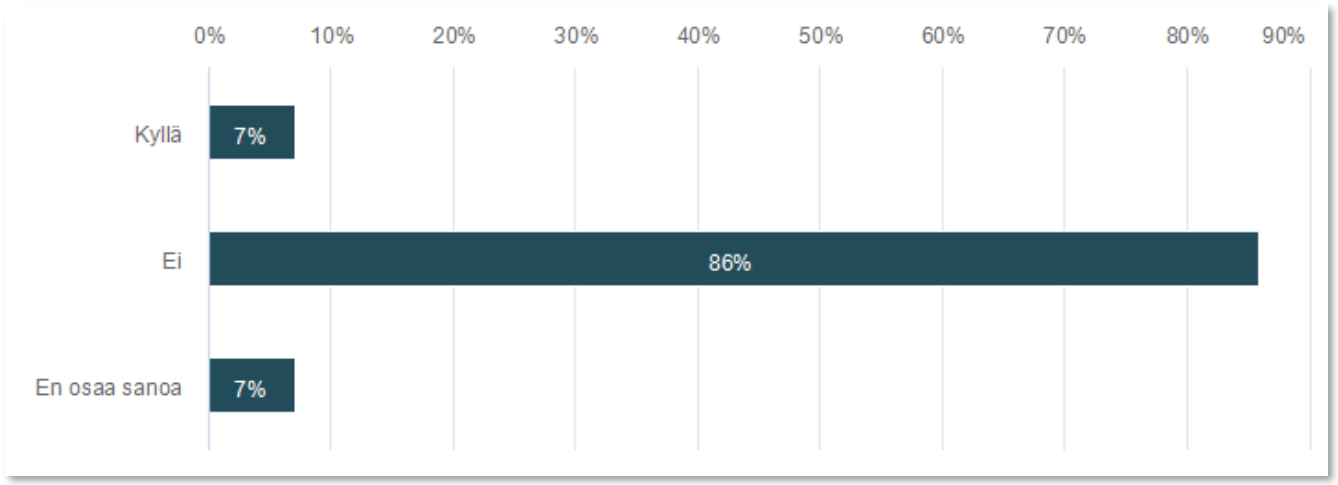


Kuvio 12. Vastaajayritysten tietosuojan huomioiminen myös etätyössä.

Tietosuoja oli otettu huomioon myös etätyössä suurimmassa osassa (86 %) vastanneista yrityksistä. Vain seitsemässä prosentissa vastanneista yrityksistä ei ollut otettu tietosuojaa huomioon etätöissä, ja toiset seitsemän prosenttia ei osannut sanoa.

Kahdeksannessa kysymyksessä pyrittiin selvittämään, onko yrityksessä laadittu kyberturvallisuusstrategiaa.

Kysymys 8. Onko yrityksessänne laadittu kyberturvallisuusstrategia?



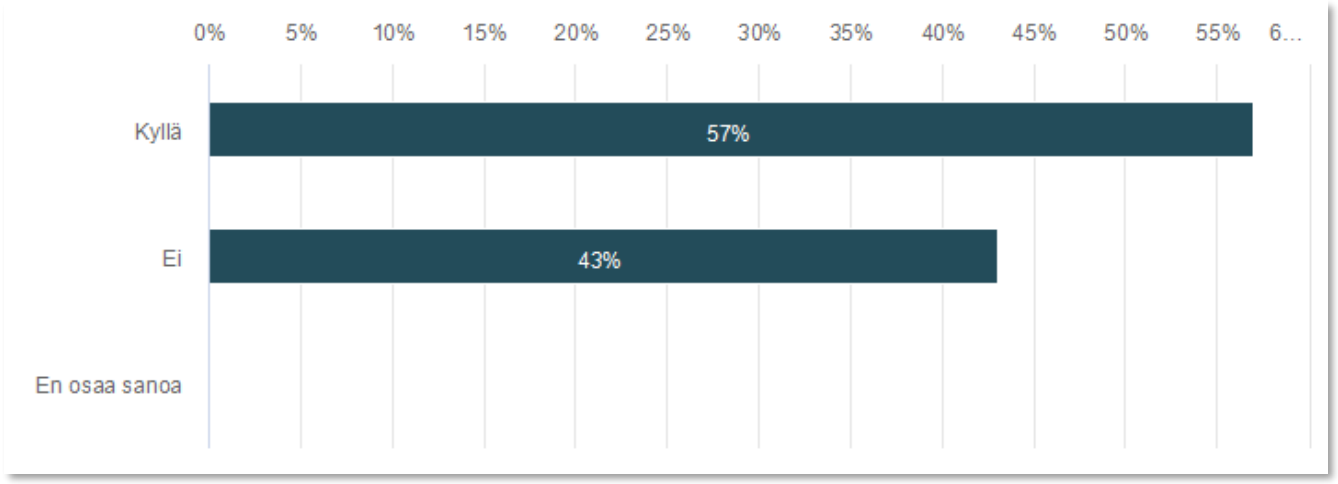
Kuvio 13. Kyberturvallisuusstrategian laadinta vastaajayrityksessä.

Kysymyksen vastaukset olivat odotettuja. Kyberturvallisuusstrategiaa ei ole yleensä laadittu pk-yrityksissä, vaan se on yleensä käytössä julkishallinnossa tai valtion eri toiminnoissa. Esimerkiksi Suomen valtiolla ja puolustusvoimilla on oma kyberturvallisuusstrategia. (Ulkoministeriö, [viitattu 24.10.2022].)

Vain seitsemällä prosentilla vastanneista yrityksistä oli jo käytössä kyberturvallisuusstrategia. Suurimmalla osalla (86 %) ei ollut käytössä, ja seitsemän prosenttia vastaajayrityksistä ei osannut sanoa.

Yhdeksännessä kysymyksessä tiedusteltiin, onko yrityksessä nimettyä tietosuojavastaavaa joko sisäisesti, ulkoistettuna tai tietosuojavastaavaa ei ole nimetty ollenkaan.

Kysymys 9: Onko yrityksessänne nimettyä tietosuojavastaavaa yrityksen sisältä tai ulkoistettuna?



Kuvio 14. Tietosuojavastaavan nimeäminen vastaajayrityksissä.

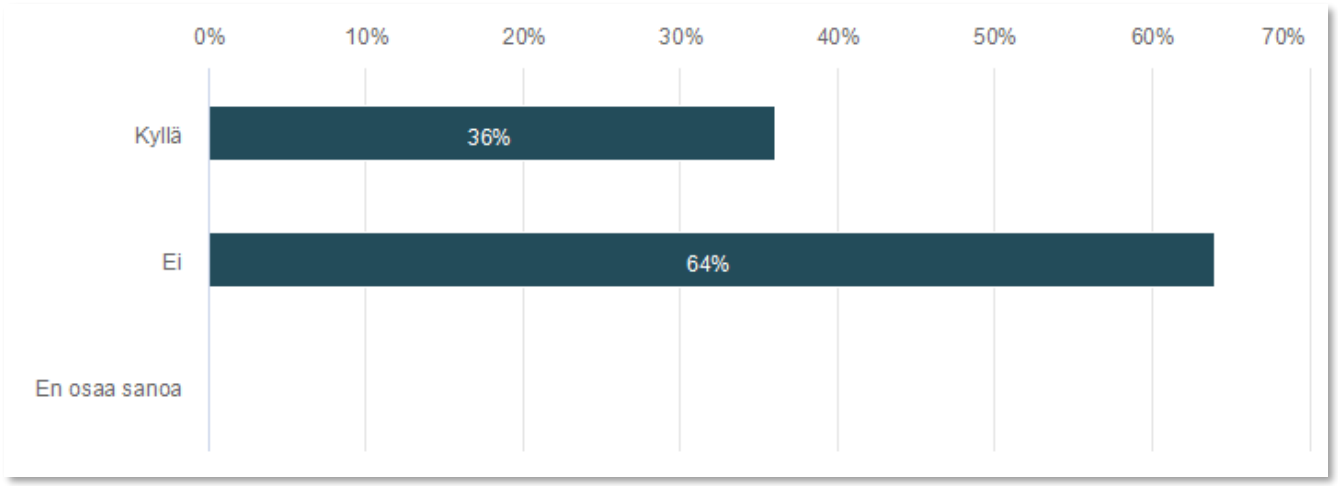
EU:n yleisen tietosuoja-asetuksen mukaan tietosuojavastaavan nimeämisessä tulee ottaa huomioon henkilön pätevyys tehtävään ja muut tarvittavat resurssit. Jos organisaatiosta ei löydy sopivaa henkilöä, voidaan tietosuojavastaavan tehtävät ulkoistaa ja ostaa palveluna. (Andreasson ym. 2019, 99). Vastanneista yrityksistä 57 prosentilla oli nimetty tietosuojavastaava sisäisesti tai ulkoistettuna. Vähän alle puolella, eli 47 prosentilla, tietosuojavastaavaa ei ollut nimetty.

Tietosuojavastaavan tehtävä perustuu vapaaehtoisuuteen, jos organisaatiolla ei ole siihen velvoitetta. Velvoite tulee kyseeseen seuraavissa tapauksissa

- Jos toimija on julkisen sektorin toimija, mutta ei tuomioistuin.
- Jos toimijan ydintehtävät muodostuvat henkilötietojen käsittelytoimista, jota edellyttävät rekisteröityjen laajamittaista, säännöllistä ja järjestelmällistä seurantaa.
- Jos toimijan ydintehtävät muodostuvat henkilötietojen laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin tai rikostuomiota tai rikkomuksia koskeviin tietoihin. (Andreasson ym. 2019, 90.)

Kymmenennessä kysymyksessä kartoitettiin, oliko yritysten henkilöstölle toteutettu säännöllisesti tietoturvakoulutusta esimerkiksi vähintään kerran vuodessa.

Kysymys 10: Onko henkilöstölle toteutettu tietoturvakoulutusta säännöllisesti, esim. vähintään kerran vuodessa?

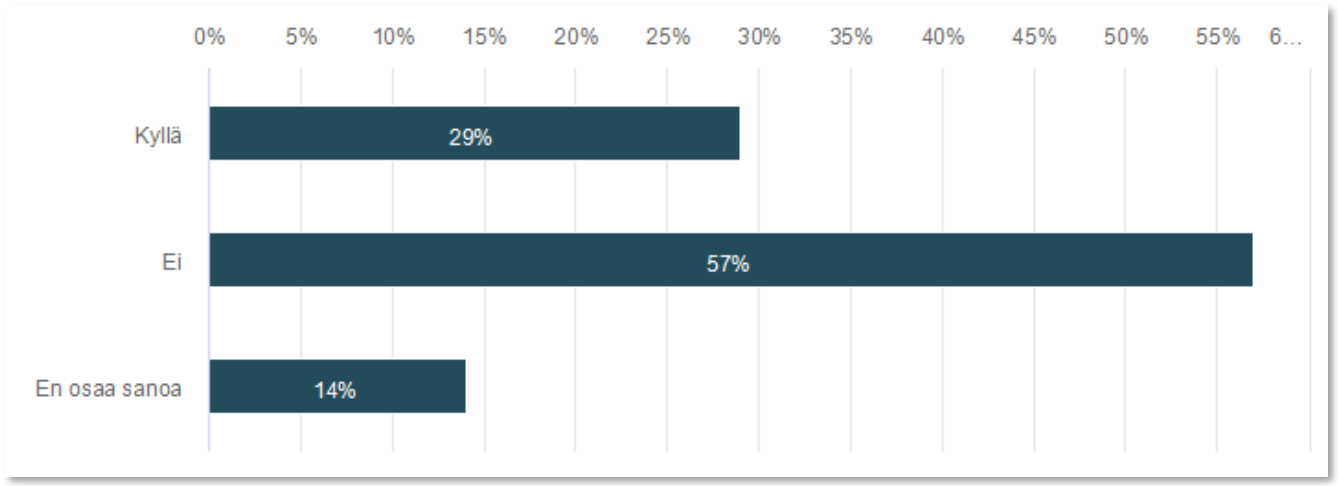


Kuvio 15. Säännöllisen tietoturvakoulutuksen toteuttaminen vastaajayrityksissä.

Suurin osa vastaajayrityksistä ei ollut toteuttanut tietoturvakoulutusta säännöllisesti vähintään kerran vuodessa. Vastaajayrityksistä 36 prosenttia oli toteuttanut tietoturvakoulutuksia säännöllisesti, vaikka kuitenkin uuden työntekijän perehdytyksessä tietosuojan ja tietoturvan käytännöt oli käyty läpi jopa 79 prosentissa kyselyyn vastanneista yrityksistä.

Kysymyksessä 11 tiedusteltiin Zero Trust -suojausmallin käyttöä tai sen suunniteltua käyttöä. Kysymyksen ohessa annettiin selite, jossa kuvattiin mitä Zero Trust -suojausmalli tarkoittaa.

Kysymys 11: Onko yrityksessänne käytössä tai suunnitteilla ottaa käyttöön ns. "Zero Trust" -suojausmalli?

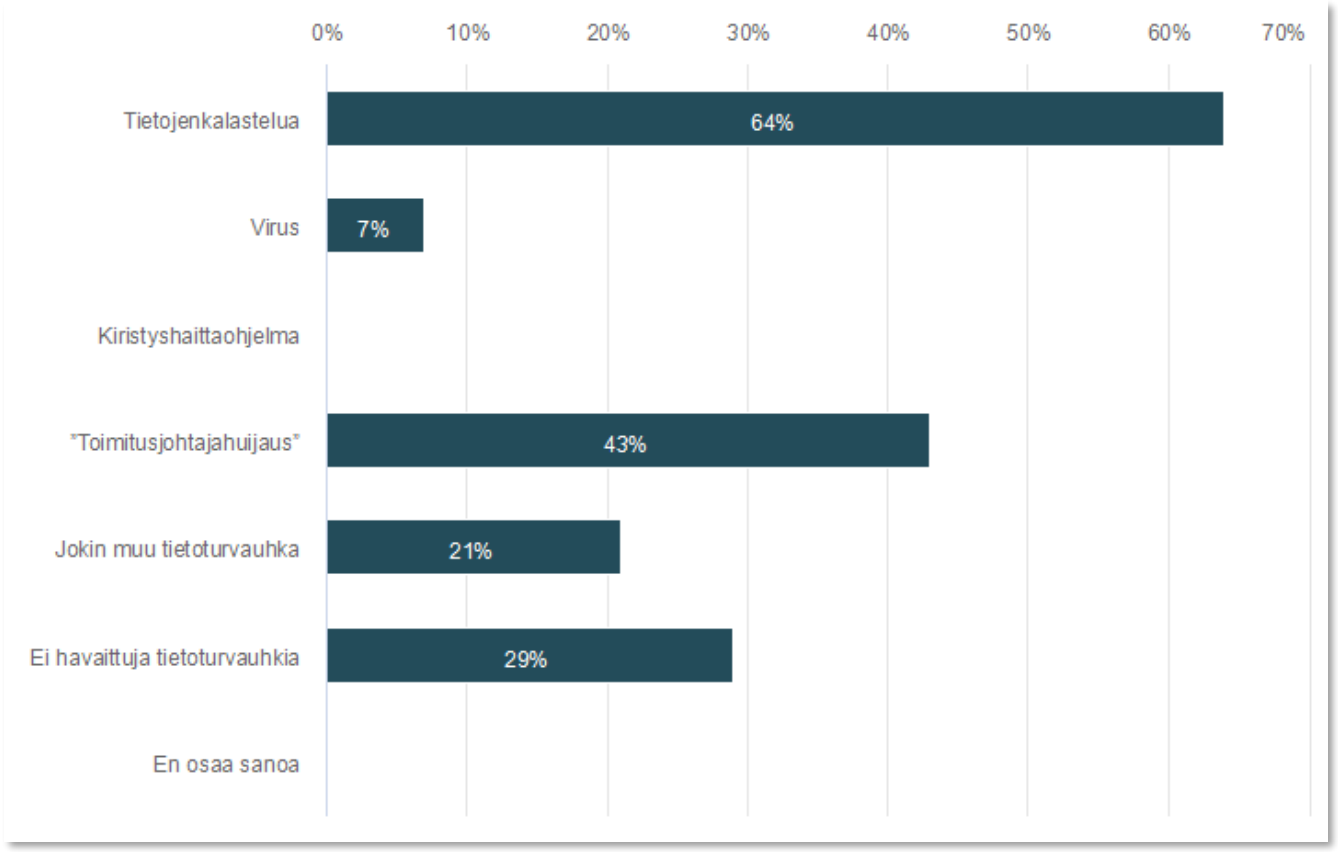


Kuvio 16. Zero Trust -suojausmallin käyttö tai suunniteltu käyttö vastaajayrityksissä

Kuten aikaisemmin luvussa 3.3 kerrottiin, Zero Trust -suojausmallista on tullut yksi suosituimmista nykyaikaisista kyberturvallisuuden rajapinnoista. Vastauksista voi kuitenkin todeta, että ehkä pk-yrityksissä Zero Trust -suojausmalli ei ole vielä useimmilla käytössä. 29 prosenttia vastaajista kertoi sen olevan käytössä tai suunnittelee sen käyttöönottoa. Yli puolet yrityksistä (57 %) ei ole ottanut sitä käyttöön tai ei suunnittele sen ottamista käyttöön. 14 prosenttia vastaajista ei osannut sanoa, onko suojausmalli käytössä tai suunnitteilla.

Kysymyksessä 12 kysyttiin yrityksiltä tietoturvauhista viimeisimmän kahden vuoden aikana. Kysymyksessä lueteltiin yleisimpiä tietoturvauhkia ja annettiin vaihtoehdoksi vastata myös ”jokin muu tietoturvauhka” tai ”en osaa sanoa” -vaihtoehdot

Kysymys 12: Onko yritykseenne kohdistunut mitään seuraavista yleisimmistä tietoturvauhista viimeisen kahden vuoden aikana?



Kuvio 17. Vastaajayrityksiin kohdistuneet tietoturvauhat viimeisimmän kahden vuoden aikana.

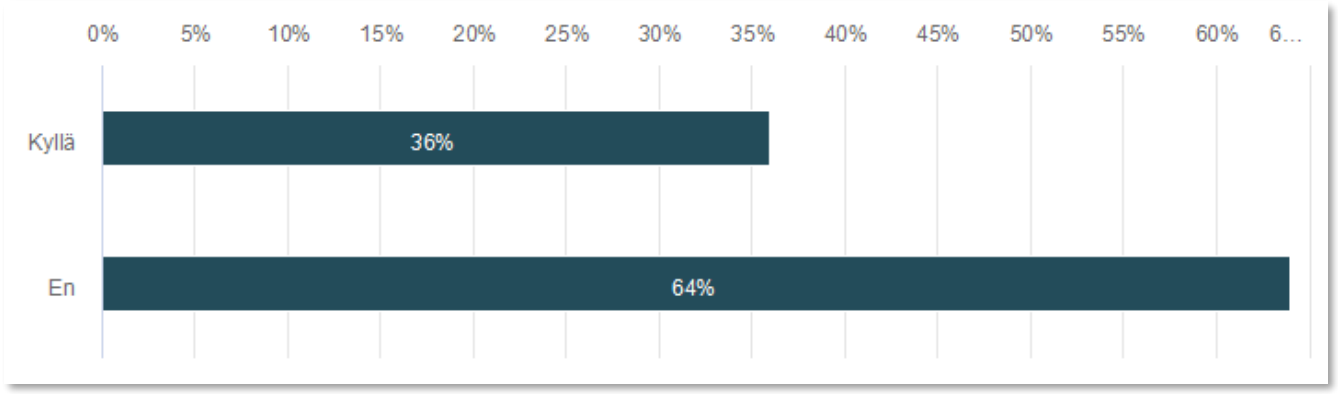
Taulukko 2. Vastanneiden määrä ja vastausvaihtoehtojen jakautuminen kysymyksessä 12

Vaihtoehto	**vastanneiden määrä**
Tietojenkalastelua	9
Virus	1
Kiristyshaittaohjelma	0
”Toimitusjohtajahuijaus”	6
Jokin muu tietoturvauhka	3
Ei havaittuja tietoturvauhkia	4
En osaa sanoa	0

Kysymykseen saatiin yhteensä 23 vastausta 14 eri vastaajayrityksestä. Tietoturvauhkia kohdistui kymmeneen eri yritykseen viimeisimmän kahden vuoden aikana, ja niistä suurimmassa osassa tietoturvauhat olivat tietojenkalastelua ja ns. toimitusjohtajahuijauksia. 21 prosenttia vastaajista oli kohdannut jonkin muun tietoturvauhan ja yllättäen jopa 29 prosenttia vastaajista ei ollut havainnut yhtään tietoturvauhkaa viimeisimmän kahden vuoden aikana.

Kysymyksessä 13 kysyttiin vastaajan aktiivisuutta seurata Kyberturvallisuuskeskuksen tietoturvauutisia viimeisen kahden vuoden aikana. Kyberturvallisuuskeskus tarjoaa mm. tietoturvajulkaisuja ja -uutisia, kuten ”Tietoturva nyt!”, joka koostaa Kyberturvallisuuskeskuksen ajankohtaisia uutisia ja raportteja. Lisäksi joka kuukausi, julkaistaan ns. ”Kybersää”, jossa käydään läpi edellisen kuukauden tietoturvan yleinen tilanne.

Kysymys 13. Oletko seurannut aktiivisesti kyberturvallisuuskeskuksen tietoturvauutisia viimeisen kahden vuoden aikana?

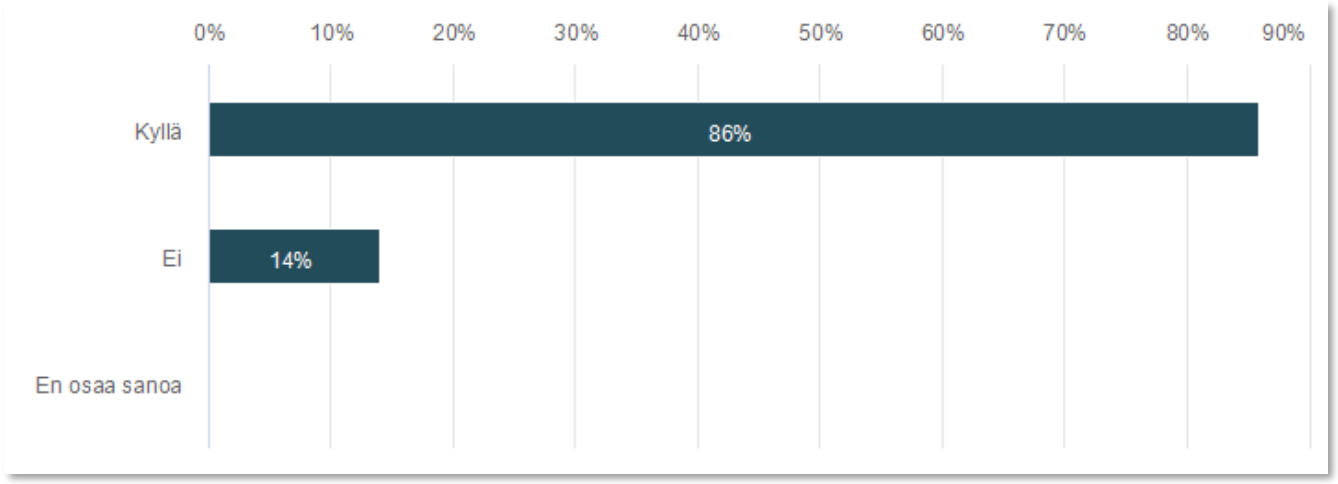


Kuvio 18. Kyberturvallisuuskeskukset tietoturvauutisten aktiivinen seuranta vastaajayrityksissä.

Suurin osa vastaajista ei ollut aktiivisesti seurannut Kyberturvallisuuskeskuksen tietoturvauutisia viimeisen kahden vuoden aikana. Vain 36 % vastaajista oli seurannut aktiivisesti Kyberturvallisuuden ajankohtaisia tietoturvauutisia.

Kysymyksessä 14 kysyttiin tietoturvan parantamisen toimenpiteistä ja investoinneista viimeisen kahden vuoden aikana.

Kysymys 14: Onko yrityksenne tehnyt selvästi enemmän toimenpiteitä tai investointeja tietoturvan parantamiseen viimeisen kahden vuoden aikana?



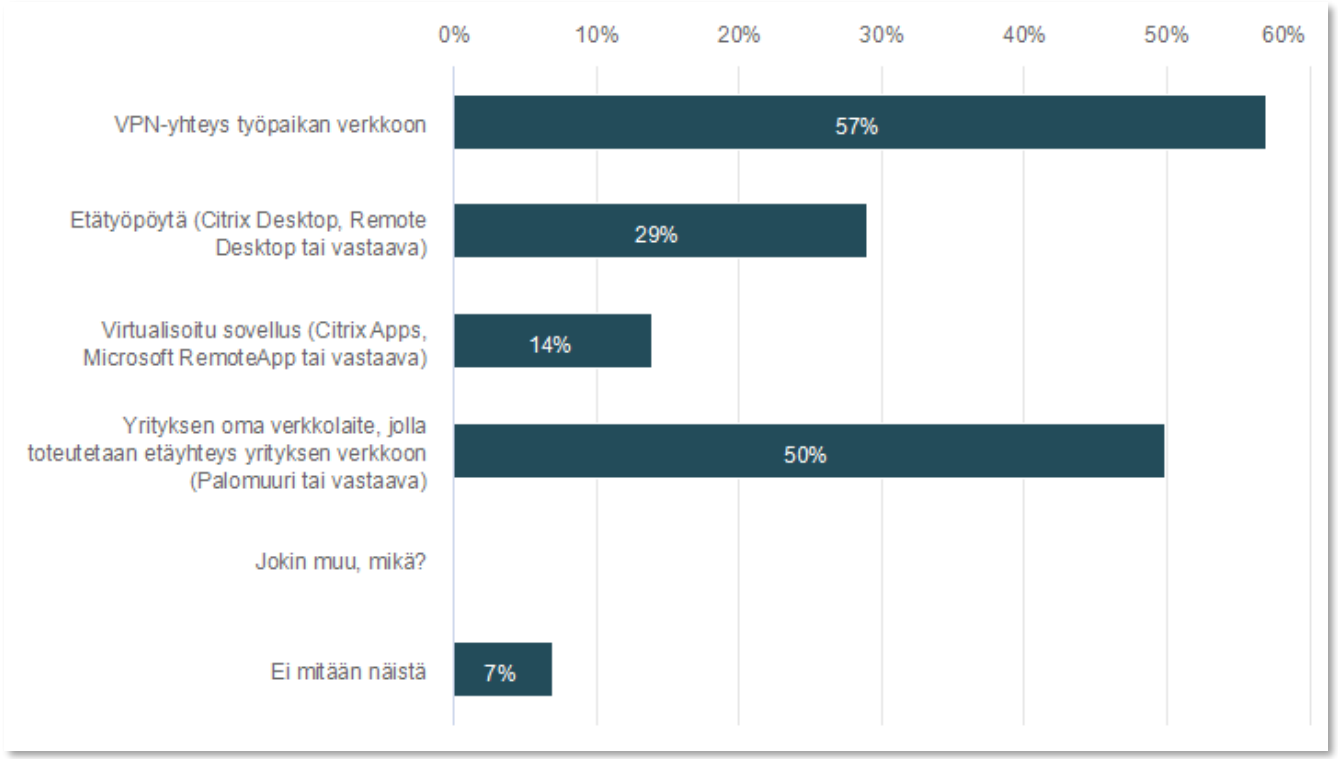
Kuvio 19. Tietoturvan parantamisen toimenpiteiden ja investointien kasvu vastaajayrityksissä.

Tämä tulos oli odotettu varsinkin, kun ottaa huomioon etätyön tarpeen kasvun ja lisääntyneiden tietoturvauhat yleisesti. Jopa 86 % vastanneista oli tehnyt selvästi enemmän toimenpiteitä ja investointeja tietoturvan parantamiseen viimeisen kahden vuoden aikana. Vain 14 % ei ollut tehnyt selkeitä toimenpiteitä ja investointeja tietoturvan parantamiseen ko. ajanjakson aikana.

Kysymyksessä 15 kysyttiin tarkemmin, mitä kysymyksen eri etäyhteysratkaisuja tai etätyökaluja vastaajayrityksessä oli käytössä. Tässä kysymyksessä oli myös vastaajalla vaihtoehtona valita ”jokin muu, mikä?” ja mahdollisuus kertoa vapaakenttään, mikä jokin muu ratkaisu vastaajayrityksessä oli käytössä.

5.3 Kysymykset käytössä olevista tietoturvaratkaisuista

Kysymys 15: Mitä seuraavista etäyhteysratkaisuista tai etätyökaluista on käytössä etätöissä yrityksessänne?



Kuvio 20. Käytössä olevat etäyhteysratkaisut ja etätyökalut vastaajayrityksissä.

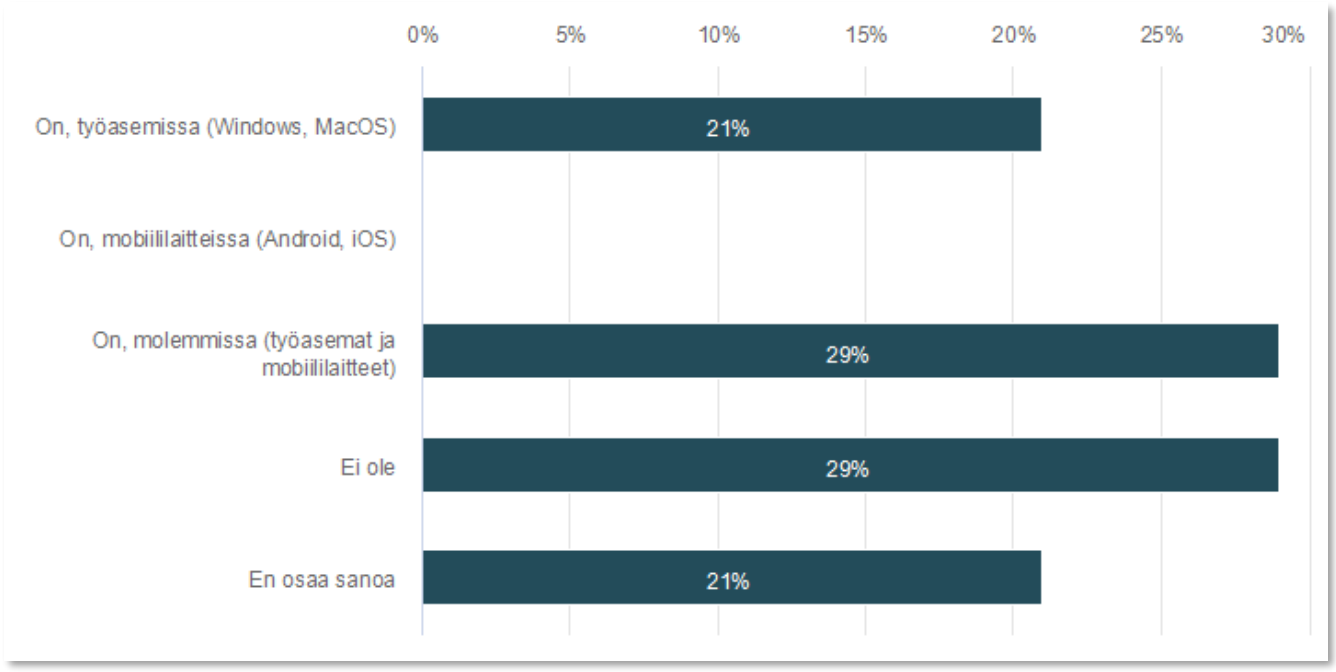
Taulukko 3. Vastanneiden määrä ja vastausvaihtoehtojen jakautuminen kysymyksessä 15.

Vaihtoehto	Vastanneiden määrä
VPN-yhteys työpaikan verkkoon	8
Etätyöpöytä (Citrix Desktop, Remote Desktop tai vastaava)	4
Virtualisoitu sovellus (Citrix Apps, Microsoft RemoteApp tai vastaava)	2
Yrityksen oma verkkolaite, jolla toteutetaan etäyhteys yrityksen verkkoon (Palomuuri tai vastaava)	7
Jokin muu, mikä?	0
Ei mitään näistä	1

Vastauksia annettiin yhteensä 22 kappaletta 14 vastanneen vastaajayrityksen kesken. Vastaukset jakautuivat siten, että suosituin vaihtoehto oli VPN-yhteys työpaikan verkkoon, ja se oli käytössä jopa kahdeksalla vastaajista. Toiseksi suosituin oli yrityksen oma verkkolaite, jolla etäyhteys yrityksen verkkoon oli toteutettu. Sitä käytti seitsemän vastaajaa neljästätoista vastaajasta. Etätyöpöytää käytti 29 % vastaajista, ja sovellusvirtualisointia käytti 14 prosenttia vastaajista. Vain yhdellä vastaajista ei ollut mitään näistä etäyhteysratkaisuista tai etätyökaluista käytössä tai niille ei ollut tarvetta.

Kysymyksessä 16 kysyttiin keskitetystä päätelaitehallinnan ratkaisusta. Selitteeseen annettiin esimerkkinä Microsoftin Endpoint Manager eli Intune ja Upkeeper. Molemmat ovat työkaluja ja ratkaisuja päätelaitehallintaan. Jos vastaajalla oli käytössään keskitetty päätelaitehallinta, kysymyksessä annettiin vaihtoehdoksi valita joko työasemissa tai mobiililaitteissa tai tarjottiin erikseen vaihtoehtona molemmissa eli sekä työasemissa että mobiililaitteissa.

Kysymys 16: Onko yrityksessänne käytössä keskitettyä päätelaitehallintaa?

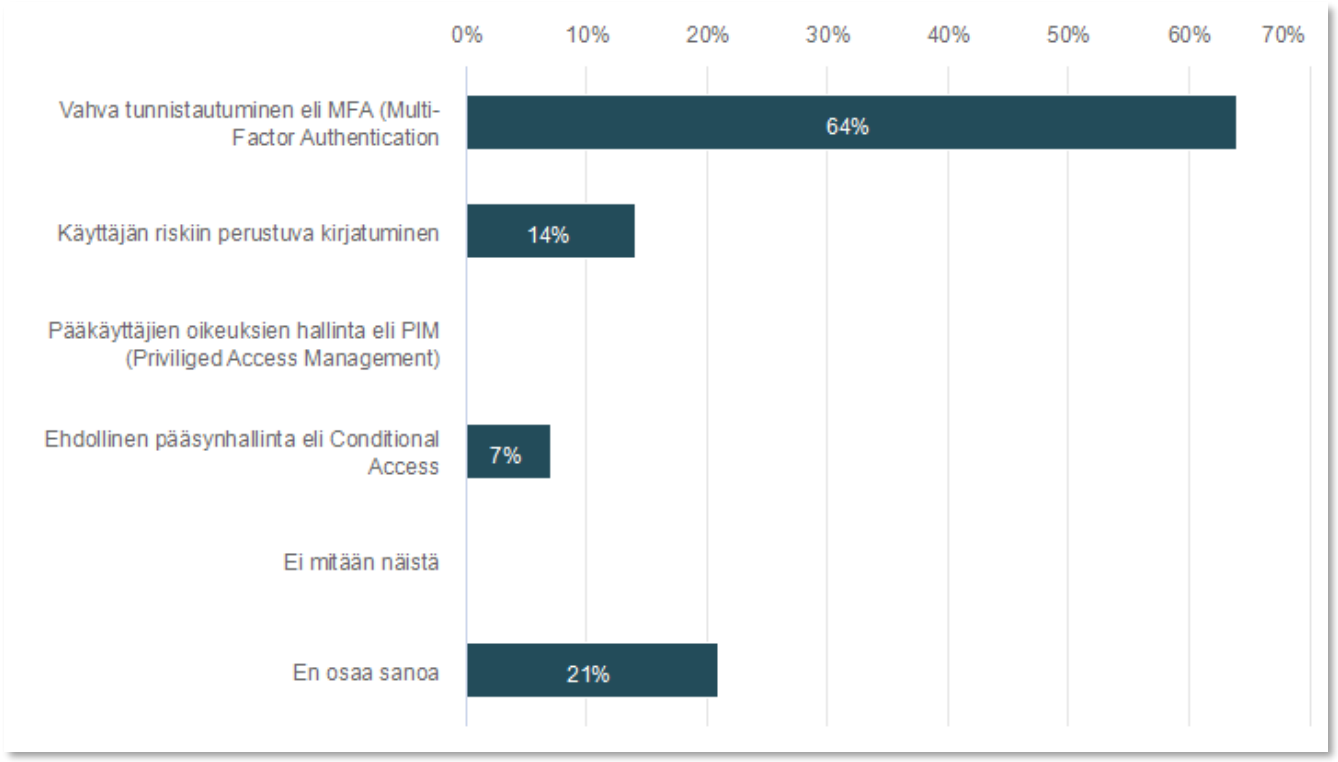


Kuvio 21. Keskitetty päätelaitehallinta vastaajayrityksessä

Yhteensä puolet vastaajista kertoi käyttävänsä keskitettyä päätelaitehallintaa joko työasemissa tai molemmissa eli työasemissa sekä mobiililaitteissa. Loput vastaajayrityksistä ei käyttänyt tai ei osannut sanoa käyttäneensä keskitettyä päätelaitehallintaa. Näistä 29 prosenttia ei käyttänyt ja 21 prosenttia ei osannut sanoa.

Kysymyksessä 17 kysyttiin käytössä olevista pääsynhallintatekniikoista Microsoft 365 ja Azure -palveluissa. Vastaajille annettiin valmiit vaihtoehdot eri tekniikoihin.

Kysymys 17. Mitä pääsynhallintatekniikoita yrityksessä on käytössä Microsoft 365 ja/tai Azure -palveluissa?



Kuvio 22. Microsoft 365 ja Azure-palveluiden pääsynhallintatekniikoiden käyttö vastaajayrityksissä

Taulukko 4. Vastanneiden määrä ja vastausvaihtoehtojen jakautuminen vastaajayrityksessä

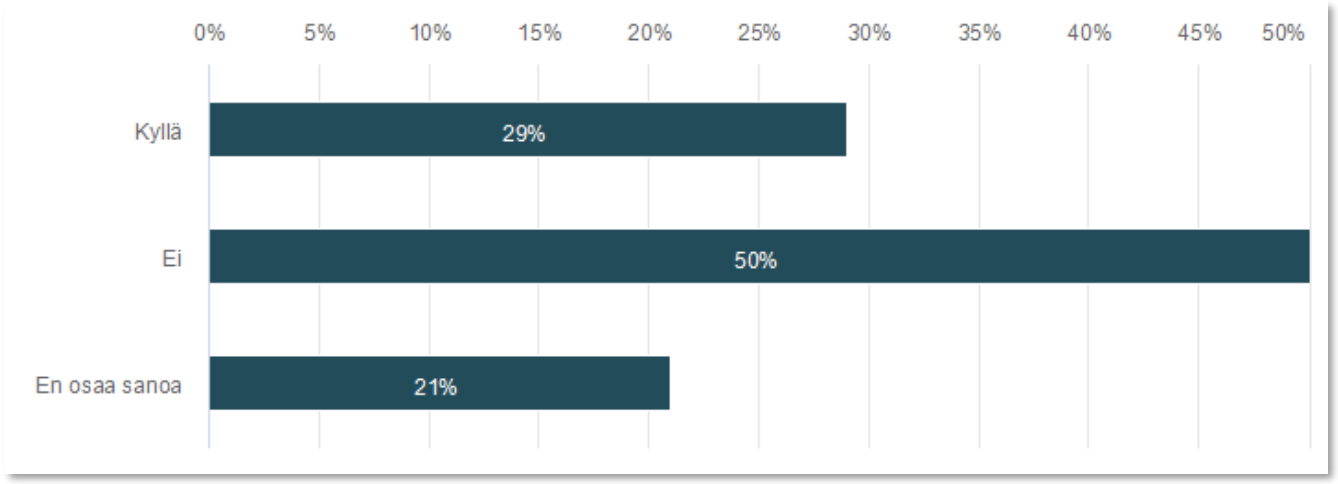
Vaihtoehto	Vastanneiden määrä
Vahva tunnistautuminen eli MFA (Multi-Factor Authentication	9
Käyttäjän riskiin perustuva kirjautuminen	2
Pääkäyttäjien oikeuksien hallinta eli PIM (Priviliged Access Management)	0
Ehdollinen pääsynhallinta eli Conditional Access	1
Ei mitään näistä	0
En osaa sanoa	3

Vastausten perusteella yhdeksässä eli suurimmassa osassa yrityksissä oli käytössä vahva tunnistautuminen eli monimenetelmäinen tunnistautuminen (MFA). Se mahdollistaa perinteisen käyttäjätunnus ja salasana -yhdistelmän lisäksi erikseen tehtävän lisätarkistuksen. Lisätarkistus voi olla kertakäyttöinen koodi puhelun tai tekstiviestin kautta, mobiilisovelluksen kautta tehtävä hyväksyminen tai vaihtuva numerokoodi. (Traficom 2019.)

Kolmessa vastaajayrityksessä oli käytössä kehittyneempiä pääsynhallintatekniikoita, kuten käyttäjän riskiin perustuva kirjautuminen ja ehdollinen pääsynhallinta (englanniksi Conditional Access). Kolme vastaajaa ei osannut sanoa onko yrityksessä pääsynhallintatekniikoita käytössä.

Kysymyksessä 18 kysyttiin EDR eli Endpoint Detection and Response -ratkaisuiden käytöstä yrityksessä. Selitteessä avattiin vastaajalle mitä EDR tarkoittaa, jos se ei ollut aikaisemmin tuttu termi.

Kysymys 18: Onko yrityksessänne käytössä Endpoint Detection and Response (EDR) -ratkaisuja?

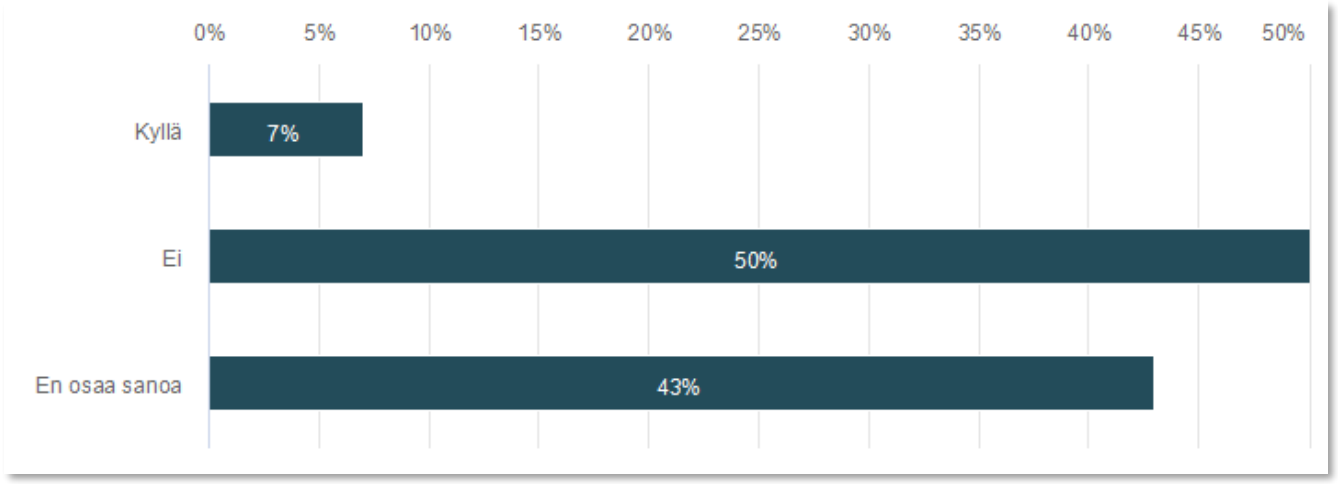


Kuvio 23. EDR eli Endpoint Detection and Response -ratkaisuiden käyttö vastaajayrityksissä.

EDR eli Endpoint Detection and Response on yleisesti käytetty termi ratkaisusta, jossa reaaliaikaisesti ja tekoälyn avustuksella suojataan päätelaitteita automaattisesti. Se kerää dataa jatkuvasti ja analysoi sen lennosta. Eri signaalien ja algoritmien avulla se voi tunnistaa ja jopa estää haitallisia tai epäilyttäviä käytäntöjä päätelaitteessa (IBM Corporation 2022c). Suurimmalla osalla ei ollut kyseistä ratkaisua käytössä. Vain 29 prosentilla sellainen oli käytössä. 21 prosenttia vastaajista ei osannut sanoa, onko yrityksessä EDR-ratkaisu käytössä.

Toiseksi viimeisessä eli 19. kysymyksessä kartoitettiin SIEM eli Security Information and Event Management -ratkaisun käyttöä yrityksissä. Vastaajille kerrottiin selitteessä kuvaus, mitä SIEM tarkoittaa.

Kysymys 19: Onko yrityksessänne käytössä SIEM (Security Information and Event Management) -ratkaisua?

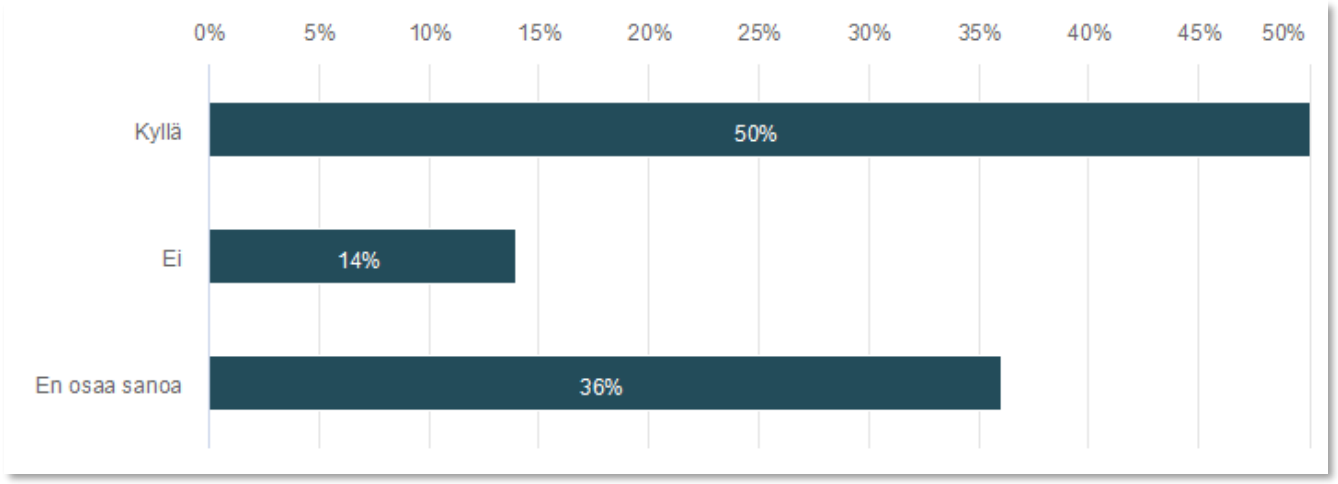


Kuvio 24. SIEM-ratkaisujen käyttö vastaajayrityksissä.

SIEM eli Security Information and Event Management tarkoittaa tietoturvaratkaisua, jonka avulla siihen keskitetysti ohjatuista lokitiedoista ja valvontatapahtumista tunnistetaan potentiaalisia tietoturvauhkia ja haavoittuvuuksia ennen kuin ne voivat häiritä liiketoimintaa. Sitä käytetään moderneissa tietoturvakeskuksissa (SOC eli Security Operations Center) yleisesti keskitettyyn valvontaan ja hälytyksiin. Se on myös työkalu tietoturvaloukkausten tutkinnassa (IBM 2022d). SIEM voi olla uusi käsite monille pk-yrityksissä ja tämän voi myös havaita vastauksissa. Suurin osa vastaajista ei osannut sanoa tai kertoa suoraan, että kyseistä ratkaisua ei ole käytössä. Vain yhdellä vastanneista yrityksistä oli käytössä jokin SIEM-ratkaisu.

Viimeisenä kysymyksenä oli elintärkeiden palveluiden tai järjestelmien varmuuskopioiden toimivuuden ja eheyden säännöllinen testaus. Selitteessä avattiin kysymystä ja esimerkkinä käytettiin tietokantojen ja palvelimien säännölliset testipalautukset ja toimivuuden tarkistukset omasta tai palveluntarjoajan puolesta.

Kysymys 20: Varmistetaanko yrityksenne liiketoiminalle elintärkeiden palveluiden tai järjestelmien varmuuskopioiden toimivuus ja eheys säännöllisesti?



Kuvio 25. Varmuuskopioiden toimivuuden ja eheyden säännöllinen varmistus vastaajayrityksessä.

Varmuuskopiot ovat paras vakuutus yritykselle varsinkin kiristyshaittaohjelmia vastaan tai niistä palautumiseen. Varmuuskopioiden toimivuuden eheyden tarkistus on tärkeää varsinkin liiketoiminalle elintärkeiden palveluiden tai järjestelmien osalta. (IBM 2022a.)

Vastausten perusteella on huolestuttavaa, että jopa 36 prosenttia vastanneista yrityksistä ei osannut sanoa tai 14 prosentilla ei varmistettu varmuuskopioiden toimivuutta ja eheyttä säännöllisesti. Puolella vastaajayrityksistä tämä asia oli jo kunnossa.

6 JOHTOPÄÄTÖKSET JA KEHITYSEHDOTUKSET

6.1 Etätyön yleistymisen haasteet

Etätyön tarve on selvästi muuttunut viimeisen kahden vuoden aikana. Suurelta osin tämän voi selittää COVID-19-taudin aiheuttama pandemia ja sitä kautta väkisinkin muuttuneet tavat tehdä töitä. Tämänkin työn tutkimuksen kaikissa vastaajayrityksissä etätyö oli mahdollistettu kaikille työntekijöille. Tänä päivänä työntekijät, joille etätyö on mahdollista, voivat dynaamisesti päättää, missä tehdä töitä. Myös hybridityö on tullut ehkä jäädäkseen.

Toimenpiteet ovat aiheuttaneet painetta parantaa tietoturvaa ja investointeja pk-yrityksissä. IBM:n X-Force Threat Intelligence Index -raportin mukaan työn tekemisen paikan dynaamisuus aiheuttaa haasteita tietoturvaan ja sitä kautta tietoturvan johtamiseen. (IBM 2022d). Innolinkin tekemän tutkimuksen mukaan COVID-19-taudin pandemia-ajan myötä vain 14 prosentille yrityksille syntyi uusia tarpeita tai kehityshankkeita IT-ratkaisuiden osalta (Innolink 2020). Tämän tutkimuksen otannan mukaan uudet tarpeet ja investoinnit ovat kasvaneet huomattavasti vastaajayrityksissä.

6.2 Ohjeistus ja perehdyttäminen

Vastaajayritysten vastausten perusteella etätyön tietoturvaa oli perehdytetty hyvin uudelle työntekijälle, mutta tietoturvakoulutusta tai testausta ei ollut toteutettu säännöllisesti. Ohjeistus etätyön käytännöistä ja tietoturvasta löytyi 64 prosentilta vastaajayrityksiltä, ja lopuilta vastaajayrityksiltä se puuttui.

Tietoturvallisuuden järjestäminen on työnantajan vastuulla, mutta myös työntekijällä on oma vastuunsa. Etätyön tietoturvallisuus tulee perustua työnantajan tietoturvaohjeisiin ja etätyössä etenkin etätyötä koskeviin lisäohjeisiin. Työntekijän vastuu tarkoittaa myös käytännössä annettujen ohjeiden noudattamista. Mikäli etätyöntekijät eivät ole tietoisia yrityksen menettelytavoista ja ohjeista, oikeat toimintatavat eivät ole mahdollisia. (Helle 2004, 192.)

Etätyön tietoturvallisuusohjeissa tulisi kiinnittää huomiota

- tietoturvapolitiikkaan (Andreasson ym. 2019, 115)
- tiedostojen suojaukseen
- käyttöoikeuksien hallintaan
- tietoliikenneyhteyksien suojaamiseen
- luottamuksellisen tiedon käsittelyyn
- virustorjuntaan
- tietojen tallentamiseen
- työvälineiden käyttötarkoitukseen
- asiakirjojen käyttöön, säilyttämiseen ja hävittämiseen
- työpisteen fyysiseen suojaamiseen
- toimenpiteisiin etätyön päättyessä. (Helle 2004, 196.)

Perehdytyksessä tietosuoja- ja tietoturva-asiat pitäisi olla itsestään selviä, ja niiden jatkuvaan kehittämiseen kannattaisi panostaa. Uudelle työntekijälle olisi tärkeää antaa sellaista tukea, että hän kokisi saavansa apua tarvittaessa esimerkiksi salassa pidettävien tai muuten arkaluontoisten tietojen käsittelyssä. Poikkeamia ja ongelmatilanteita tulee pakostakin vastaan ICT-välineiden ja ohjelmistojen hallinnassa. (Andreasson ym. 2019, 118.)

Tietoturva vaatii säännöllistä perehdyttämistä henkilöstölle. Andreasson ym. (2019, 118–120) suosittelee käyttämään apuna esimerkiksi seuraavia asioita:

- henkilöstön tietoturva- ja tietosuojaopas
- tietosuojavastaavan säännölliset tiedotukset
- yrityksen sisäinen intranet
- tietoturvallisuuden ja tietosuojan verkkokurssit
- erilaiset luennot aiheesta
- käyttökoulutukset
- säännölliset pikaohjeet ja tiedotteet
- lyhyet videot

- tietoturvaan ja tietosuojaan kytketyt teemapäivät tai -viikot
- tietoturvauutiset, kuten Kyberturvallisuuskeskuksen ajankohtaiset uutiset (Tietoturva nyt!) ja Kybersää (Traficom 2022b).

Esimerkki Kyberturvallisuuskeskuksen Kybersäästä:

Kuvio 26. Kyberturvallisuuskeskuksen Kybersää syyskuu 2022 (Traficom 2022b).

Yksi hyvä tapa lisätä henkilöstön tietoturvatietoisuutta on erilaiset testit. Microsoft tarjoaa hyökkäyssimulaatiokoulutusta Defender for Office 365-tuotteessa. Siinä voidaan simuloida esimerkiksi tietojenkalasteluhyökkäystä käyttämällä erilaisia social engineering -huijaustapoja. (Microsoft 2022b.)

6.3 Tietosuojan huomiointi

Kyselytutkimuksessa kysyttiin vastaajayrityksiltä tietosuojan huomioonottamisesta myös etätyössä. Vastaajayrityksistä melkein kaikki olivat ottaneet tietosuojan huomioon, mutta vain noin puolella vastaajayrityksistä oli nimetty tietosuojavastaava. Tietosuojatyön organisoiminen koko

henkilöstölle ja tietosuojatyön kehittäminen tuovat yrityksille etuja ja hyötyjä. Asiakkaan luottamuksen lisäksi toiminta- ja asiakasprosessit muuttuvat lainmukaisiksi ja joustaviksi. Etuja ovat myös työntekijän oman oikeusturvan parantaminen, tietosuojan epävarmuuden poistaminen ja työviihtyvyyden lisääminen. Yritykselle etuja tuovat osaavammat ja työssä viihtyvämmät työntekijät, ja se myös tuo työhön tehokkuutta. Näin myös yrityksen tuottavuus kasvaa ja kustannukset vähenevät. Tietosuojatyöhön panostaminen on siis kannattava investointi, joka voi tuottaa itsensä takaisin. (Andreasson ym. 2019, 49–50.)

Menestyksekästä tietosuojatyötä voi toteuttaa esimerkiksi organisoimalla tietosuojatyö nimeämällä yritykselle tietosuojavastaava ja hyödyntämällä sitä työarjessa. Lisäksi kannattaa varmistaa koko henkilöstön tietosuojaosaaminen seuraavasti: Laadi käsittelyohjeet asiakastiedoille ja kouluta ne koko henkilöstölle. Testaa koko henkilöstön tietosuojaosaaminen ja seuraa, kehitä ja puutu tietosuojan poikkeamiin (Andreasson ym. 2019, 49–50.)

Johdon rooli on tietosuojatyön onnistumisen ytimessä. Sen velvoitteisiin ja vastuisiin voidaan lukea

- tietosuojan nykytilan kartoitus
- rekisterihallinnon järjestäminen, esim. rekisteriselosteet
- kirjalliset politiikat, periaatteet ja ohjeet
- riittävät resurssit tietosuojavastaavalle ja mahdolliselle tietosuojaryhmälle
- riskienhallinta, kuten riskien tunnistaminen, luokittelu, analyysit ja toimintaohjeet
- seuraamuskäytännöt tietosuojarikkomuksia varten
- tietosuojattavien asiakirjojen hävitysprosessit
- tietoturvan ja tietosuojan omavalvontasuunnitelma tarvittaessa (pakollinen vain sosiaali- ja terveydenhuollossa)
- tietotilinpäätös osana raportointia. (Andreasson ym. 2019, 87–88.)

Tietosuojavastaava on pakko nimittää EU:n yleisen tietosuoja-asetuksen mukaan julkisella sektorilla, lukuun ottamatta tuomioistuimia. Myös siinä tapauksessa, jos yrityksessä käsitellään laajasti henkilötietoja tai sen ydintoiminnassa käsitellään laajasti arkaluonteisia tietoja, velvoittaa asetus nimittämään yritykseen tai organisaatioon tietosuojavastaavan. Rekisterinpitäjien ja

henkilötietojen käsittelijöiden on varmistuttava siitä, onko yritykseen nimettävä tietosuojavastaava asetuksen mukaan. Tietosuojavastaava toimii yrityksen erityisasiantuntijana rekisterinpitäjän apuna ja auttaa saavuttamaan korkean tietosuojan tason yrityksessä. Näin ollen tietosuojavastaavaksi tulee valita aina lähtökohtaisesti asiantuntija. Tietosuojavastaavalle tulee antaa mahdollisuudet ja resurssit työaikaan, kouluttautumiseen ja työvälineisiin. (Andreasson ym. 2019, 14–15, 90, 92.)

Tietosuojavastaavan tehtävät määritellään EU:n yleisen tietosuoja-asetuksen 39 artiklassa seuraavasti:

1. EU:n yleisen tietosuoja-asetuksen, muun lainsäädännön ja ohjeistuksen vaatimusten täytäntöönpano ja soveltaminen organisaatiossa
2. tietosuojavaatimusten noudattamisen ja oikeuksien toteutumisen seuranta ja valvonta
3. neuvonta ja ohjaus kaikissa tietosuojakysymyksissä
4. dokumentaation laatimisen, saatavuuden ja säilyttämisen valvonta
5. vaikutustenarviointien tuki ja valvonta
6. tietosuojariskien asianmukainen huomioiminen
7. tietosuojan tietoisuusohjelman rakentaminen ja kouluttaminen henkilöstölle
8. yhteistyö valvontaviranomaisten kanssa
9. ilmoitusvelvollisuuden toteutumisen seuranta ja mahdollisesti myös hoitaminen
10. rekisteröityjen oikeuksien toteuttamisen tukeminen. (Andreasson ym. 2019, 92–93.)

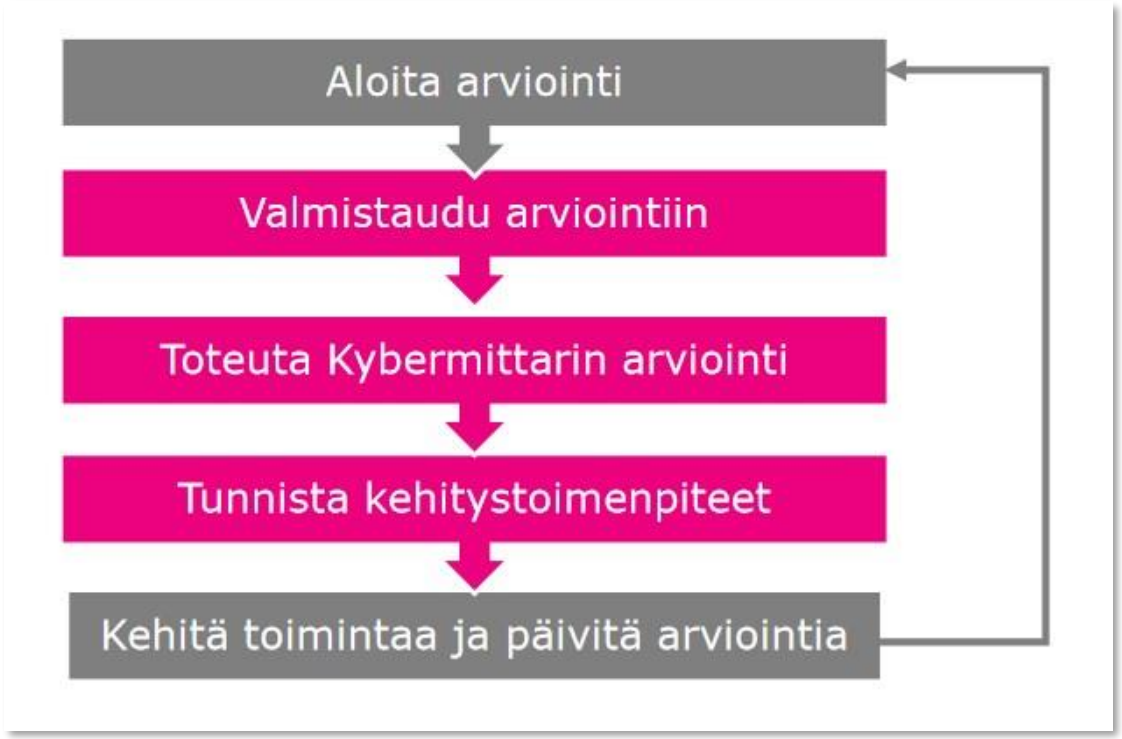
6.4 Tietoturvan suositukset ja parantaminen

IBM:n X-Force Threat Intelligence -raportin suosituksena on käyttää Zero Trust -suojausmallia yleisimpiä hyökkäyksiä vastaan. Se vaikeuttaa huomattavasti rikollisen etenemistä yrityksen verkossa. Koska kaikki verkkoliikenne todennetaan, vain oikeilla henkilöillä on pääsy kriittiseen dataan. Raportin mukaan monivaiheisen tunnistautumisen lisäksi tulisi huomioida myös käyttöoikeuksin pienimmän valtuuden periaate, joka erityisesti auttaa luomaan esteitä kiristyshaittaohjelmien leviämiseen yrityksessä. Raportti suosittelee ottamaan käyttöön tietoturvan automaatiota tieturvatapausten vastaamiseen. Näitä ovat mm. SIEM-ratkaisut. Myös EDR-ratkaisut tuovat yrityksille huomattavaa etua tunnistamaan ja hävittämään hyökkääjät yrityksen verkosta

ennen kuin ne saavuttavat viimeisen tavoitteen, kuten datan varastamisen yrityksestä. (IBM 2022a.)

Yksi tietoturvan arviointityökalu on Kyberturvallisuuskeskuksen tietoturvan arviointityökalu nimeltään ”Kybermittari”, jolla voidaan arvioida liiketoiminnan kriittiset toiminnot, kattaa yleisimmät kyberturvallisuuden riskienhallinnan osa-alueet ja parhaat käytännöt. Kybermittari koostuu osioista, tavoitteista ja käytännöistä, jotka edustavat tyypillisiä ja hyväksi havaittuja tietoturvan menettelytapoja. Kybermittari laskee kypsyystason kolmessa vaiheessa ja antaa kypsyysraportin, jossa kerrotaan eri kypsyystasoille vaadittavat käytännöt. Kun vaadittavat käytännöt ovat kunnossa, kypsyystaso nousee. Parhaan hyödyn työkalusta saa, kun sitä käytetään osana viisivaiheista arviointiprosessia ja se tuodaan osaksi jatkuvaa toiminnan kehittämistä. (Traficom 2022c.)

Kybermittarin viisivaiheinen arviointiprosessi:



Kuvio 27. Kybermittarin viisivaiheinen arviointiprosessi (Traficom 2022c).

Kybertuvallisuuskeskus suosittelee tavanomaisiksi suojaustoimenpiteiksi käytännössä seuraavaa:

1. Ota käyttöön monivaiheinen tunnistautuminen (MFA).
2. Huolehdi tietoturvapäivityksien asentamisesta viipymättä.
3. Huolehdi varmuuskopioinnista ja niiden toimivuudesta.
4. Varmista etäyhteyksien turvallisuus.
5. Tarjoa henkilöstölle koulutusta, jotta he osaavat toimia työssään tietoturvallisesti. (Traficom 2020a.)

Suosittelenkin tämän työn tuloksena pk-yrityksiä huomioimaan tietoturvaa ja tietosuojaa erityisesti etätyössä sekä noudattamaan edellä mainittuja Kyberturvallisuuskeskuksen suosituksia.

LÄHTEET

Andreasson, A., Riikonen, J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki: Tietosanoma.

Eduskunta. 21.12.2018. EU:n tietosuojauudistuksen kansallinen täytäntöönpano. [Verkkosivu]. [Viitattu 23.10.2022]. Saatavana: https://www.eduskunta.fi/FI/naineduskuntatoimii/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx.

Etätyötä koskeva puitesopimus.16.7.2002. Framework agreement on telework. [Verkkojulkaisu]. [Viitattu 20.10.2021]. Saatavana: https://www.kt.fi/sites/default/files/media/document/etatyo-puitesopimus.pdf.

HE 158/2018 vp. Hallituksen esitys eduskunnalle työaikalaiksi ja eräiksi siihen liittyviksi laiksi.

Heikkilä, T. 2014a. Tilastollinen tutkimus. Porvoo: Bookwell.

Heikkilä, T. 2014b. Webropol-kyselyt. [Verkkojulkaisu]. [Viitattu 11.10.2021]. Saatavana: http://www.tilastollinentutkimus.fi/6.WEBROPOL/Webropol-kysely.pdf.

Helle, M. 2004. Etätyö. Helsinki: Edita Publishing.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Hämeenlinna: Tammi.

IBM. 2022a. X-Force Threat Intelligence Index 2022. [Verkkojulkaisu]. [Viitattu 23.10.2022]. Saatavana: https://www.ibm.com/downloads/cas/ADLMYLAZ.

IBM. 2022b. Cost of a data breach 2022. [Verkkojulkaisu]. [Viitattu 23.10.2022]. Saatavana: https://www.ibm.com/reports/data-breach. Vaatii rekisteröinnin.

IBM. 2022c. EDR (Endpoint Detection and Reponse). [Verkkosivu]. [Viitattu 24.10.2022]. Saatavana: https://www.ibm.com/topics/edr.

IBM. 2022d. What is SIEM? [Verkkosivu]. [Viitattu 24.10.2022]. Saatavana: https://www.ibm.com/topics/siem.

Innolink. 2020. Kuinka korona haastoi yritysten digivalmiuden? [Verkkojulkaisu]. [Viitattu 5.10.2021]. Saatavana: https://www.innolink.fi/case/arrow-ecs-2020/.

L 738/2002. Työturvallisuuslaki.

L 872/2019. Työaikalaki.

L 55/2001. Työsopimuslaki.

Microsoft. 2022a. Mitä haittaohjelmat ovat? [Verkkosivu]. [Viitattu 19.10.2022]. Saatavana: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-malware.

Microsoft. 12.10.2022b. Simulate a phishing attack with Attack simulation training in Defender for Office 365. [Verkkosivu]. [Viitattu 24.10.2022]. Saatavana: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training?view=o365-worldwide.

Microsoft. 2022c. Suhtaudu tietoturvaan aktiivisesti Zero Trust -suojausmallilla. [Verkkosivu]. [Viitattu 19.10.2022]. Saatavana: https://www.microsoft.com/fi-fi/security/business/zero-trust.

Microsoft. 2022d. Tietojen kalastelulta suojautuminen. [Verkkosivu]. [Viitattu 19.10.2022]. Saatavana: https://support.microsoft.com/fi-fi/windows/tietojen-kalastelulta-suojautuminen-0c7ea947-ba98-3bd9-7184-430e1f860a44.

Mitre Co. 4.1.2022. Att&ck Phishing. [Verkkosivu]. [Viitattu 19.10.2022] Saatavana: https://attack.mitre.org/techniques/T1566/.

Priyanka, N. 2018. Malware Detection. Hamburg: Anchor Academic Publishing

Tietosuojavaltuutetun toimisto. 2022a. Henkilötietojen käsittely. [Verkkosivu]. [Viitattu 23.10.2022]. Saatavana: https://tietosuoja.fi/henkilotietojen-kasittely.

Tietosuojavaltuutetun toimisto. 2022b. Osoita noudattavasi tietosuojasäännöksiä. [Verkkosivu]. [Viitattu 23.10.2022]. Saatavana: https://tietosuoja.fi/osoitusvelvollisuus.

Tivi. 30.11.2016. Varjo-IT on myrkkyä digitalisaatiolle. [Verkkoartikkeli]. Alma Media. [Viitattu 27.10.2022]. Saatavana: https://www.tivi.fi/kumppaniblogit/salesforce/varjo-it-on-myrkkya-digitalisaatiolle/623e32d9-fa6f-3c0e-ab03-b7f4cca0d041.

Tilastokeskus. 2021. Käsitteet. [Verkkosivu]. [Viitattu 02.11.2021] Saatavana: https://www.stat.fi/meta/kas/pk_yritys.html.

TIVIA. 2022. Maksuton kyberturvallisuusstrategiaesityspohja yrityksille. [Verkkojulkaisu]. [Viitattu 24.10.2022]. Saatavana: https://tivia.fi/uutiset/uutiset-3/maksuton-kyberturvallisuus-strategia-esityspohja-yrityksille-1628.

Traficom. 2019. Suojautuminen Microsoft Office 365 -tunnusten kalasteluilta ja tietomurroilta. [Verkkojulkaisu]. [Viitattu 19.10.2022] Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Suojautuminen%20Microsoft%20Office%20365%20-tunnusten%20kalastelulta%20ja%20tietomurroilta%20web.pdf.

Traficom. 2020a. Pienyritysten kyberturvallisuusopas. [Verkkojulkaisu]. [Viitattu 5.10.2021] Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf.

Traficom. 2020b. Kyberturvallisuus ja yrityksen hallituksen vastuu. [Verkkojulkaisu]. [Viitattu 20.10.2022]. Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf.

Traficom. 2022a. Toimintaohje - Vuotaneet tunnukset. [Verkkojulkaisu]. [Viitattu 19.10.2022] Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuotaneet%20tunnuksetToimintaohje.pdf.

Traficom. 13.10.2022b. Kybersää syyskuu 2022. [Verkkojulkaisu]. [Viitattu 24.10.2022] Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%2C%20syyskuu%202022.pdf.

Traficom. 10.10.2022c. Kybermittari: perusperiaatteet. [Verkkojulkaisu]. [Viitattu 24.10.2022]. Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_esittely_V2.0.pdf.

Traficom. 2022d. Toimintaohje - Tietomurto. [Verkkojulkaisu]. [Viitattu 24.10.2022]. Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf.

Traficom. 2022e. Toimintaohje - Kiristyshaittaohjelma. [Verkkojulkaisu]. [Viitattu 24.10.2022]. Saatavana: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/KiristyshaittaohjelmaToimintaohje.pdf.

Työsuojeluhallinto. 15.9.2020. Etätyö. [Verkkosivu]. [Viitattu 21.10.2022]. Saatavana: https://www.tyosuojelu.fi/tyoolot/tyoymparisto/etatyo.

Työturvallisuuskeskus. 2017. Etätyössä turvallisesti. [Verkkojulkaisu]. [Viitattu 05.10.2021] Saatavana: https://ttk.fi/julkaisu/etatyossa-turvallisesti/.

Ulkoministeriö. Ei päiväystä. Kyberturvallisuus ja kybertoimintaympäristö. [Verkkojulkaisu]. [Viitattu 24.10.2022]. Saatavana: https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto.

Varonis. 2022. What Is Zero Trust? A Comprehensive Guide & Security Model. [Verkkosivu]. [Viitattu 20.10.2022] Saatavana: https://www.varonis.com/blog/what-is-zero-trust/.

Vilkman, U. 2016a. Etäjohtaminen: tulosta joustavalla työllä. Helsinki: Talentum Pro.

Vilkman, U. 16.2.2016b. Etätyön hyödyt ja haasteet johtamisen näkökulmalta. [Verkkojulkaisu]. [Viitattu 21.10.2022]. Saatavana: https://etajohtaminen.fi/etatyohon-siirtyminen-johtamisennakokulmasta/

LIITTEET

Liite 1. Kyselytutkimuksen kysymykset

Liite 1. Kyselytutkimuksen kysymykset

1. Onko etätyön tarve kasvanut pysyvästi yrityksessänne viimeisen kahden vuoden aikana?

- ○ Erittäin paljon
- ○ Huomattavasti
- ○ Kohtalaisesti
- ○ Vähän
- ○ Ei ollenkaan
- ○ En osaa sanoa

2. Miten laajasti yrityksessänne on mahdollistettu etätyötä?

- ☐ Ei ole mahdollistettu ollenkaan
- ☐ Osittain
- ☐ Toimihenkilöille
- ☐ Esihenkilöille ja johtajille
- ☐ Koko henkilöstölle

4. Kuinka hyvin tietoturva on huomioitu etätyössä?

- ◯ Erittäin hyvin
- ◯ Hyvin
- ◯ Kohtalaisesti
- ◯ Vähän
- ◯ Ei ollenkaan
- ◯ En osaa sanoa

5. Onko yrityksessä käytössä ohjeistusta etätyön käytännöistä ja tietoturvasta?

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

6. Testataanko käyttäjien tietoturvatietämystä säännöllisesti, esimerkiksi henkilöstön tietoturvatesteillä?
   Tietoturvatesti voi olla esimerkiksi simuloitu tietojenkalasteluviesti tai vastaava.

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

8. Huomioidaanko uuden työntekijän perehdytyksessä myös tietoturvan ja tietosuojan käytännöistä etätyössä?

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

9. Onko tietosuoja otettu huomioon myös etätyössä?
   Esimerkiksi henkilötietosuoja ja GDPR

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

10. Onko yrityksessänne laadittu kyberturvallisuusstrategia?

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

11. Onko yrityksessänne nimettyä tietosuojavastaavaa yrityksen sisältä tai ulkoistettuna?

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

13. Onko henkilöstölle toteutettu tietoturvakoulutusta säännöllisesti, esim. vähintään kerran vuodessa?

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

14. Onko yrityksessänne käytössä tai suunnitteilla ottaa käyttöön ns. "Zero Trust" -suojausmalli?

"Zero Trust" on nimi suojausmallille, jossa pääsynhallinnassa ja verkkoliikenteessä kaikki on ei-luotettua. Kaikki kirjautumiset ja verkkoliikenne pyritään varmistamaan oikeaksi.

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

15. Onko yritykseenne kohdistunut mitään seuraavista yleisimmistä tietoturvauhista viimeisen kahden vuoden aikana?

- ☐ Tietojenkalastelua
- ☐ Virus
- ☐ Kiristyshaittaohjelma
- ☐ ”Toimitusjohtajahuijaus”
- ☐ Jokin muu tietoturvauhka
- ☐ Ei havaittuja tietoturvauhkia
- ☐ En osaa sanoa

16. Oletko seurannut aktiivisesti kyberturvallisuuskeskuksen tietoturvauutisia viimeisen kahden vuoden aikana?
Esimerkiksi ”Tietoturva nyt!” tai ”Kybersää”

○ Kyllä

○ En

17. Onko yrityksenne tehnyt selvästi enemmän toimenpiteitä tai investointeja tietoturvan parantamiseen viimeisen kahden vuoden aikana?

○ Kyllä

○ Ei

○ En osaa sanoa

18. Mitä seuraavista etäyhteysratkaisuista tai etätyökaluista on käytössä etätöissä yrityksessänne?

☐ VPN-yhteys työpaikan verkkoon

☐ Etätyöpöytä (Citrix Desktop, Remote Desktop tai vastaava)

☐ Virtualisoitu sovellus (Citrix Apps, Microsoft RemoteApp tai vastaava)

☐ Yrityksen oma verkkolaite, jolla toteutetaan etäyhteys yrityksen verkkoon (Palomuuri tai vastaava)

☐ Jokin muu, mikä? _____

☐ Ei mitään näistä

20. Onko yrityksessänne käytössä keskitettyä päätelaitehallintaa?

Esim. Microsoft Endpoint Manager (Intune), Upkeeper tai jokin muu vastaava.

- ○ On, työasemissa (Windows, MacOS)
- ○ On, mobiililaitteissa (Android, iOS)
- ○ On, molemmissa (työasemat ja mobiililaitteet)
- ○ Ei ole
- ○ En osaa sanoa

21. Mitä pääsynhallintatekniikoita yrityksessä on käytössä Microsoft 365 ja/tai Azure -palveluissa?

- ☐ Vahva tunnistautuminen eli MFA (Multi-Factor Authentication
- ☐ Käyttäjän riskiin perustuva kirjautuminen
- ☐ Pääkäyttäjien oikeuksien hallinta eli PIM (Priviliged Access Management)
- ☐ Ehdollinen pääsynhallinta eli Conditional Access
- ☐ Ei mitään näistä
- ☐ En osaa sanoa

23. Onko yrityksessänne käytössä Endpoint Detection and Response (EDR) ratkaisuja?
EDR on esimerkiksi päätelaitteisiin asennettava agentti, jolla voidaan tunnistaa tai analysoida kehittyneitä kyberuhkia ja niiden toimintamalleja. Tuotteita ovat mm. WithSecure Elements Endpoint Detection and Response tai Microsoft Defender for Endpoint

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

24. Onko yrityksessänne käytössä SIEM (Security Information and Event Management) -ratkaisua?
SIEM on yleinen nimi tietoturvan seurantatyökalulle, joka kerää lokitietoa kaikesta yrityksen kyberturvallisuuteen liittyvästä

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

25. Varmistetaanko yrityksenne liiketoiminalle elintärkeiden palveluiden tai järjestelmien varmuuskopioiden toimivuus ja eheys säännöllisesti?
Esimerkiksi säännölliset tietokantojen tai palvelimien testipalautukset ja toimivuuden tarkistukset omasta tai palveluntarjoajan toimesta

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa