Tampereen ammattikorkeakoulu

# Etätyöskentelyn tietoturva

Kristian Rintala

Taavi Pelkonen

OPINNÄYTETYÖ
Huhtikuu 2021

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

**TIIVISTELMÄ**

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikan tutkinto-ohjelma
Tietoliikennetekniikka ja tietoverkot

RINTALA, KRISTIAN & PELKONEN, TAAVI:
Etätyöskentelyn tietoturva

Opinnäytetyö 52 sivua, joista liitteitä 1 sivu
Huhtikuu 2021

---

Tietoturva on noussut yhteiskunnassa ajankohtaiseksi puheenaiheeksi yhä useampiin yrityksiin ja yksityishenkilöihin kohdistuneiden tietomurtojen sekä niistä nousseen mediahuomion seurauksena. Vuonna 2019 puhjennut COVID-19-pandemia on lisäksi pakottanut yhä useammat työskentelemään etäyhteyksien avulla. Tämä opinnäytetyö tehtiin selvittämään etätyöskentelyn tietoturvaa sekä tietoturvaan kohdistuvaa asennoitumista työntekijän näkökulmasta erilaisissa yrityksissä. Eri alojen yrityksissä toimivien työntekijöiden etätyöskentelyyn liittyvästä toiminnasta etsittiin mahdollisia puutteita ja niihin rakennettiin korjausehdotuksia.

Opinnäytetyö toteutettiin verkkokyselyn ja haastatteluiden avulla mahdollisimman suuren otannan saavuttamiseksi. Tutkimuksesta saatujen tulosten mukaan työntekijät pitivät kohdalleen sattuvaa tietoturvamurtoa hyvin pelottavana ajatuksena, mutta samalla vastaajat eivät pitäneet tätä aidosti todennäköisenä. Lisäksi tietoturvakoulutuksen taso on liian matalaa. Varsinkin pandemian vuoksi etätyönsä nopealla aikataululla aloittaneet työntekijät saivat liian vähän etätyöhön ja sen tietoturvaan liittyvää koulutusta siirtymän yhteydessä. Tietämys tietoturvaan liittyvistä asioista on siis liian vähäistä takaamaan turvallista työskentelyä, sillä usein suurin riski tietoturvalle on työntekijän omat toimintatavat.

Suurin osa työssä löydetyistä tietoturvaongelmista olisi ratkaistavissa kouluttamalla henkilökuntaa enemmän. Myös mahdollinen tarkennettu kouluttaminen voisi olla hyödyksi niin työntekijöille kuin yrityksille. Lisäksi tietoturvaosaamisen testaaminen ja varmentaminen olisi tarpeen arkaluontoista materiaalia käsittelevien henkilöiden kohdalla. Tietoturvan tärkeyttä tulisi painottaa kaikissa etätyötä hyödyntävissä yrityksissä ja opinnäytetyön käsittelemiä teemoja tulisi pohtia yhdessä työyhteisön kesken.

---

Asiasanat: tietoturva, tietomurto, etätyö, digitalisaatio

## ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Telecommunications and Networks

RINTALA, KRISTIAN & PELKONEN, TAAVI:
Information Security in Remote Work

Bachelor's thesis 52 pages, appendices 1 page
April 2021

---

Information and cyber security have recently become one of the most discussed topics around the world due to massive data breaches against companies and many individuals. The COVID-19 pandemic forced multiple companies to adapt to the difficult situation by working remotely. The purpose of this thesis was to determine the main security risks at remote working and to find out employees' attitude in a variety of different companies towards information security.

The data for this study was collected mainly via interviews and online surveys to get as large a sample size as possible. The results suggest that remote workers find data breaches very scary, but extremely unlikely for them to happen. It was also very clear that information security training was being done too infrequently and multiple employees had never been in one.

Most of the problems discovered during this thesis study can be solved by adding more information security training in the companies. It would also be beneficial to test employees' knowledge from regularly, especially if they handle sensitive data. Companies that allow remote working should also highlight the importance of IT security and discuss the topic within the company.

---

Key words: information security, cyber security, remote work, digitalization

**SISÄLLYS**

**ERITYISSANASTO**

| | |
|---|---|
| Digitalisaatio | Digitaalisen tietotekniikan yleistyminen arkielämän toiminnoissa |
| GDPR | EU:n yleinen tietosuoja-asetus |
| Penetraatiotestaus | Järjestelmän testaamista tietoturvariskien varalta hyökkääjien näkökulmasta |
| VPN | Virtual Private Network, virtuaalinen erillisverkko |

# 1 JOHDANTO

Tämä opinnäytetyö käsittelee etätyöskentelyn tietoturvaa työntekijän näkökulmasta. Työ pyrkii selvittämään tietoturvaan liittyviä ongelmakohtia, luomaan näihin ratkaisuja ja korostamaan tietoturvan tärkeyttä.

Kiihtynyt digitalisaatio on lisännyt etätöinä työskentelevien henkilöiden määrää huomattavasti viime vuosina. Tämän seurauksena myös tietoturvaongelmat ovat nousseet yhä ajankohtaisemmiksi ja yhä useammat henkilöt ja yritykset ovat joutuneet tietomurtojen kohteiksi.

Vuonna 2019 puhjennut COVID-19-pandemia pakotti yhä useammat henkilöt etätöihin. Siirto etätyönä työskentelyyn tapahtui hyvin nopeasti pandemian aiheuttamien liikkumisrajoitusten vuoksi. Useille yrityksille ja organisaatioille henkilökunnan siirto etätyöhön tuli yllättäen, eivätkä monet työnantajat olleet käyttäneet etätyömuotoa lainkaan aikaisemmin. Yrityksillä ei ollut myöskään välttämättä aikaa ja resursseja valmistautua siirtymiseen tai valmistaa työntekijöitään turvalliseen etätyöhön.

Opinnäytetyö rajautui etätyöskentelyn tietoturvaan ajankohtaisuuden vuoksi. Lähtöolettamuksena oli, että tärkein ja suurin heikkous tietoturvaa tarkasteltaessa on työntekijä itse.

Tällä tutkimuksella pyritään selvittämään yleisimpiä tietoturvaongelmia sekä kartoittamaan työntekijöiden tietämystä ja annetun tietoturvakoulutuksen tasoa.

# 2 TIETOTURVA

## 2.1 Tietoturvan määritelmä

Tietoturvalla tarkoitetaan yleensä tietojen ja niitä kuljettavan tietoliikenteen oikeanlaista suojaamista (Helsingin yliopisto n.d.). Käsitteenä tietoturva on kuitenkin tätä määritelmää paljon laajempi, sillä siihen sisältyy useita osa-aluetta. Tietoturvan tärkeys lisääntyy jatkuvasti teknologian kehittyessä. Teknologia kehittyy ajassamme kiihtyvällä tahdilla, mikä aiheuttaa jatkuvasti myös uusia tietoturvariskejä. Tästä syystä yksityishenkilöiden, yritysten ja organisaatioiden, kaikkien teknologiaa hyödyntävien käyttäjien, on pysyttävä ajan tasalla myös tietoturvaan liittyvissä asioissa.

Useat käyttäjät osaavat yhdistää tietoturvaan virukset ja haittaohjelmat, mutta tietoturvaan kuuluu kuitenkin myös useita vähemmän tunnettuja osa-alueita. Taulukossa 1 on esitetty Turun ammattikorkeakoulun tietoturvavastaavan Matti Laakson jaottelu tietoturvan osa-alueista (Laakso n.d). Liikenne- ja viestintävirasto Traficom määrittelee tietoturvan hallinnollisina ja teknisinä toimina, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys (Traficom 2020c). Luottamuksen, eheyden ja käytettävyyden lisäksi tietoturvan osa-alueeksi lisätään usein myös todentaminen, sillä kaikki nämä neljä tietoturvan osa-aluetta kytkeytyvät toisiinsa.

Tietoturvasta käytetään sanontaa ”mukavuus kertaa turvallisuus on vakio” (Järvinen, 2012, s. 24). Sanonta kuvaa ristiriitaista suhdetta käyttömukavuuden ja tietoturvallisuuden välillä. Mikäli laitteiden käyttäminen on erittäin helppoa, on järjestelmän tietoturvallisuudessa usein puutteita. Sama toimii myös toisinpäin; mitä turvallisempi järjestelmä on, sitä vaikeampaa sen käytöstä tulee. Yrityksen näkökulmasta on vaikeaa löytää täydellinen tasapaino näiden kahden välillä. Työ halutaan suorittaa mahdollisimman tehokkaasti, mutta samalla tietoturvasta on huolehdittava. Hyvällä järjestelmäsuunnittelulla voidaan kuitenkin parantaa sekä tietoturvaa että käyttömukavuutta. (Järvinen, 2012, s. 24–25.)

TAULUKKO 1. Tietoturvan osa-alueet (Laakso n.d.)

| **Tietoturvan osa-alue** | **Lyhyt selitys** |
|---|---|
| Hallinnollinen tietoturva | Tietoturvan johtaminen ja hallinnointi |
| Fyysinen tietoturva | Toimitilojen ja laitteiden fyysinen suojaaminen |
| Laitteistoturvallisuus | Esimerkiksi tietokoneiden yleinen suojaaminen |
| Ohjelmistoturvallisuus | Ohjelmistojen tietoturvaan liittyvät asiat |
| Tietoaineiston turvallisuus | Sähköisten ja paperisten dokumenttien käsittely ja suojaaminen |
| Tietoliikenneturvallisuus | Esimerkiksi tiedonsiirtoon liittyvät tietoturvamekanismit |
| Henkilöstöturvallisuus | Rooleihin, vastuihin ja tietoturvaohjeistuksiin liittyvät asiat |
| Käyttöturvallisuus | Esimerkiksi salasanoihin liittyvät asiat. Yleensä ”ylimääräinen” kahdeksas osa-alue. Salasanakäytännöt voidaan yhdistää esimerkiksi ohjelmistoturvallisuuteen. |

## 2.2 Luottamuksellisuus

Luottamuksellisuus on sitä, että käytettävät tiedot ovat vain niiden saatavilla, joilla niihin on oikeus (Traficom 2020c). Luottamuksellisia tietoja voivat olla esimerkiksi tunnistetiedot, henkilötiedot tai terveystiedot. Näitä tietoja ei saa jakaa, lainata tai antaa ulkopuolisille nähtäväksi tai käytettäväksi.

Terveydenhuolto on hyvä esimerkki luottamuksellisuuden tärkeydestä. Terveydenhuollon asiakkaat jakavat omia arkaluontoisia asioitaan, jotka kirjataan ylös. Asiakkaan pitää pystyä luottamaan siihen, että näitä tietoja ei jaeta tai näytetä

kuin niille terveydenhuollon ammattilaisille, jotka niitä hoitotyössään tarvitsevat. Samalla nämä tiedot pitää pystyä suojaamaan tietoturvamurroilta.

Suuri luottamuksellisuuden rikkoutuminen tuli Suomessa julki lokakuussa 2020, kun psykoterapiakeskus Vastaamolle sattuneet tietoturvamurrot paljastuivat. Vastaamon tietokantaan tehtiin kaksi tietomurtoa (2018 ja 2019), joissa onnistuttiin varastamaan henkilö- ja potilastietoja. Vastaamon toimitusjohtaja salasi tietomurtoa 1,5 vuoden ajan. Hyökkääjä kertoi varastaneensa 40 000 asiakkaan tiedot ja uhkasi julkaista ne verkossa. (Yle 2020.) Verkossa on mahdollisesti julkaistu yli 30 000 asiakkaan tiedot (Yle 2021). Näin suurella tapauksella on todella merkittävä vaikutus. Se voi heikentää ihmisten luottamusta myös Vastaamon ulkopuolisiin tahoihin, kuten terveydenhuoltoon tai valtioon koska kyseessä oli arkaluontoisia potilastietoja. Vastaamon tapauksen laajuuden, arkaluontoisuuden ja mediahuomioin tulisi toimia varoittavana esimerkkinä ja kannustaa pitämään parempaa huolta tietonsa turvallisuudesta.

### 2.3 Eheys

Eheydellä tarkoitetaan sitä, että tietoja ei voi muokata ja muuttaa muut kuin siihen oikeutetut henkilöt (Traficom 2020c). Luottamuksellisuus ja eheys sitoutuvat toisiinsa. Luottamuksellisen tiedon on pysyttävä eheänä, eikä se saa kadota. Sitä ei myöskään saa muokata turhaan.

Terveydenhuolto toimii myös eheydestä hyvänä esimerkkinä. Kuten luottamuksellisuudessa, kukaan ulkopuolinen ei saa pystyä muokkaamaan tai poistamaan asiakkaan tietoja. Samalla tämä johtaa käytettävyyden (luku 2.4) rikkoutumiseen.

### 2.4 Käytettävyys

Tietojen ja tietojärjestelmien tulee olla aina niitä tarvitsevien ja niihin oikeutettujen käytettävissä (Traficom 2020c). Tarvittavien järjestelmien, tiedostojen ja palveluiden tulisi olla aina saatavilla, kun niitä tarvitaan. Tämä tarkoittaa myös esimerkiksi

verkkosivujen ylhäällä pitoa. Kun kaikki tarvittavat systeemit ovat toiminnassa aina tarvittaessa, turvataan myös yhteiskunnan toiminta.

Olisi esimerkiksi suuri ongelma, jos ihmisten terveystiedot eivät olisi saatavilla terveydenhuollon ammattilaisille silloin, kun niitä tarvitaan. Hoito hidastuisi ja se saatettaisiin jopa toteuttaa väärin, tärkeiden tietojen puuttuessa. Hyvä tapa ylläpitää käytettävyyttä on tehdä varmuuskopioita ja suojata järjestelmät tietoturvauhilta.

## 2.5 Todentaminen

”Todentaminen tarkoittaa osapuolten luotettavaa tunnistautumista” (Helsingin yliopisto n.d.). Tämä voidaan toteuttaa monella eri tavalla. Yleisin tunnistautumisen tapa on käyttäjätunnus ja salasana. Muita tapoja ovat esimerkiksi pankkitunnukset, PIN-koodi, mobiilivarmenne, varmennekortti, sertifikaatti ja biotunniste (sormenjälki ja kasvojentunnistus). Nykyään paljon yleistynyt lisätunnistautumisen muoto on kaksivaiheinen tunnistautuminen. ”Lisätunnistautumisen avulla käyttäjä todentaa itsensä erillisellä koodilla salasanan lisäksi kirjautumisen yhteydessä” (Traficom 2020a). Yleensä kirjautumiseen vaadittava koodi saadaan mobiililaitteelta. Tämä helpottaa myös tunnistamaan tunnustenkalasteluyrityksiä. Jos toinen henkilö yrittää kirjautua käyttäjän tunnuksilla sisään ja käytössä on kaksivaiheinen tunnistautuminen, käyttäjä tunnistaa heti murtautumisyrityksen.

## 2.6 Tietosuoja

”Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.” (Tietosuojavaltuutetun toimisto n.d.) Rekisteröity on tässä tapauksessa henkilö, jota käytössä oleva henkilötieto koskee. Henkilötiedoksi lasketaan kaikki tieto, joka viittaa rekisteröidyn henkilöllisyyteen. Tieto voi olla eri muodoissa, kuten fyysisessä, sähköisessä tai tallenteena. (Tietosuojavaltuutetun toimisto n.d.) Yksityishenkilöllä on

oikeus vaatia henkilötietojen muutosta tai poistamista, jos henkilötiedon käyttö perustuu johonkin muuhun kuin lakisääteiseen velvoitteeseen (Traficom 2020b).

Henkilötietojen käsittely pitää perustua aina lakiin. Asiasta riippumaton viranomainen valvoo tietosuojaa koskevien sääntöjen noudatusta. (Tietosuojavaltuutetun toimisto n.d.) Suomessa tietosuojaa valvoo Liikenne- ja viestintävirasto Traficom. Traficomin tietosuojapolitiikka sisältää EU:n tietosuoja-asetuksen (GDPR) ja Suomen kansalliset tietosuojalain asetukset. (Traficom 2020b.)

Suomessa sekä muissa Euroopan maissa alettiin soveltaa uutta yleistä tietosuoja-asetusta (GDPR) keväällä 2018. Tietosuojalain muutoksen tavoitteet voidaan jakaa neljään isompaan kategoriaan: parantaa henkilötietojen suojaa ja tietosuojaoikeuksia, vastata uusiin digitalisaatioon ja globalisaatioon liittyviin tietosuojakysymyksiin, yhtenäistää tietosuojasääntelyä kaikissa EU-maissa, sekä edistää digitaalisten sisämarkkinoiden kehittymistä. (Tietosuojavaltuutetun toimisto 2018.)

# 3 TUTKIMUSSUUNNITELMA

## 3.1 Tutkimuksen tavoitteet

Tutkimuksen päätavoitteena on selvittää nykyisen etätyöskentelyn tietoturvallisuuden tasoa, löytää mahdollisia epäkohtia ja rakentaa näihin ratkaisuja tietoturvan parantamiseksi. Tarkastelu tehdään etupäässä työntekijän näkökulmasta. Etätyöskentelyn tietoturvallisuuden taso koostuu useasta eri osa-alueesta, joita kartoitetaan luvun 3.3 tutkimusmenetelmät mukaisilla kyselyillä ja haastatteluilla.

Tutkimuksen välitavoitteina voidaan pitää tiedon keräämistä työntekijöiden osaamisesta, koulutuksen tasosta, sekä yleisestä asennoitumisesta tietoturvaa kohtaan. Lisäksi tutkimuksella pyritään selvittämään, millä keinoin yritykset ovat tukeneet työntekijöitä tietoturvaan liittyvissä asioissa. Lisätavoitteena voidaan pitää yleisen tietoturvan tärkeyden korostamista ja tietouden levittämistä.

## 3.2 Tutkimusongelmat

Tutkimussuunnitelmaa rakentaessa huomattiin, että tietoturvakokonaisuus pitää sisällään suuren määrän erilaisia muuttujia. Tietoturvaongelma saattaa johtua lukuisista eri syistä, kuten laitteista, ympäristöstä, työnantajasta tai työntekijöistä. Nämä syyt voidaan jakaa vielä alakokonaisuuksiksi, kuten työntekijän huolimattomuus ja työntekijän tietämättömyys. Tietoturvaongelmiin liittyvien syiden laajuuden vuoksi tutkimus käsittelee useita alakategorioita sen sijaan, että keskittyisi syvällisesti yhteen tiettyyn kategoriaan ja siihen liittyviin käsitteisiin. Valinnalla pyritään tuomaan esiin ongelman moninaisuutta ja lisäävän perustietämystä useammasta eri osa-alueesta.

Tutkimus antaa hyvää pohjatietoa monesta aiheeseen liittyvästä osa-alueesta ja sen vuoksi se toimii myös hyvänä pohjana jatkokehittämiseen. Mikäli jatkokehittämisessä ja -tutkimuksessa halutaan syventyä tarkemmin johonkin etätyöskentelyn tietoturvaan liittyvään osa-alueeseen, esittelee työ hyvän pohjan tarkemmalle käsittelylle. Tutkimus voi auttaa myös erilaisten kategorioiden määrän ja

toisiinsa kytkeytymisen hahmottamisessa, mikä puolestaan auttaa rajaamaan toisiinsa liittyviä käsitteitä myös jatkotutkimuksessa.

### 3.3 Tutkimusmenetelmät

Tutkimusmenetelminä käytettiin kahta erilaista haastattelumetodia. Haastattelut jaettiin kahteen eri ryhmään: verkossa täytettävään kyselyyn ja kasvokkain toteutettaviin haastatteluihin. Tällä tiedonkeruun jaottelulla pyrittiin saamaan mahdollisimman todenmukaista dataa ja pystyttiin vertailemaan tuloksia kohderyhmien kesken. Verkkokyselyiden käyttö osana tutkimusta mahdollisti myös suuremman otannan. Haastattelun ja verkkokyselyn kysymykset pidettiin täysin samoina vertailukelpoisuuden vuoksi.

# 4 TUTKIMUKSEN TOTEUTUS

## 4.1 Haastattelu

Kasvotusten suoritetun haastattelun ja verkkokyselyn tutkimuskysymykset alkoivat työalan selvittämisellä, jota hyödynnettiin myöhemmin vastaajien jaottelemisella työaloittain. Vastaaja sai itse määritellä työalansa; haastateltava kertoi sen omin sanoin ja kyselyyn vastaaja kirjoitti sen omin sanoin. Lisäksi kysymyksissä otettiin huomioon, aloittiko henkilö työnsä etänä vai siirtyikö hän etätöihin työsuhteensa aikana. Tämä tehtiin tarkempaa tulosten vertailua varten.

Tietoturvaan liittyvän tiedon keruu aloitettiin avoimilla kysymyksillä, joiden tarkoituksena oli selvittää vastaajien tietämystä ja suhtautumista tietoturvaan. Tämän jälkeen vastaajilta kartoitettiin tietoturvakoulutuksen tasoa ja heidän jo käyttöönottamiaan toimia tietoturvansa parantamiseksi. Haastattelut pitivät sisällään 24 kysymystä ja vastaamiseen kulunut aika oli noin 10–15 minuuttia.

## 4.2 Haastattelun sisältö

Tässä kappaleessa on listattu haastatteluissa ja verkkokyselyssä käytetyt kysymykset. Molempien metodien toteutuksessa käytettiin samoja kysymyksiä.

1. Millä alalla olet töissä?
2. Mitä tietoturva tarkoittaa sinulle? (kerro omin sanoin)
3. Mitä sinulle tulee mieleen termistä ”tietoturvamurto?”
4. Aloititko työsi etänä, vai siirryitkö etätöihin koronatilanteen vuoksi?

Ensimmäiset neljä kysymystä olivat vastaajan profilointia ja ryhmittelyä varten olevia kysymyksiä. Työalalla on erityisen suuri merkitys tulosten vertailun kannalta.

5. Oletko ollut tietoturvakoulutuksessa?
6. Koetko saaneesi tarpeeksi koulutusta tietoturvaan liittyvissä asioissa?

7. Käytätkö avoimia verkkoja? (esim. hotellissa/lentokentillä)
8. Käytätkö VPN-yhteyttä?

Kysymyksillä 5–8 kartoitettiin vastaajan teknistä tietämystä ja osaamista tietoturvaan liittyen. Kysymykset 5 ja 6 ovat tarkoituksella peräkkäin, koska niiden välillä on oletettavasti selkeä yhteys. Kysymyksissä 7 ja 8 oli valittavissa myös ”en tiedä mikä on avoinverkko/VPN” -vaihtoehto, jotta saadaan parempi käsitys myös vastaajan puuttuvista tiedoista.

9. Käytätkö samaa salasanaa useassa eri paikassa?
10. Useimmiten salasanassasi on: (monivalinta)
11. Kuinka usein vaihdat salasanasi?
12. Miten työssä käyttämäsi laite on suojattu?
13. Onko sinulla työsähköposti?
14. Miten tai missä säilytät työhösi liittyvän datan?

Kysymyksillä 9–14 selvitettiin vastaajien tietoturvaan liittyviä työskentelymalleja etätöissä. Kysymyksissä 9 ja 10 oli valittavissa myös ”en halua vastata” - vaihtoehto, sillä salasanaan liittyvät kysymykset voivat olla arkaluontoisia varsinkin verkon välityksellä.

15. Tarjoaako työnantaja etätyöhön tarvittavat työvälineet?
16. Kuinka usein päivität laitteidesi ohjelmistoa?
17. Onko työnantajasi ohjeistanut sinua laitteiden päivityksestä?
18. Kumpaa työskentelytapaa pidät riskialttiimpana tietoturvan kannalta?
19. Mikäli sinulla ilmenee ongelma (laitteiden käyttö, tietoturvakysymykset jne.) mistä/keneltä etsit apua?
20. Miten mielestäsi työpaikallasi voisi parantaa tietoturvaa? (ei pakollinen)

Kysymykset 15–20 jatkoivat etätyöskentelyn toimintatapojen selvitystä tietoturvan näkökulmasta. Kysymyksissä keskityttiin työpaikkaan ja työnantajaan liittyviin asioihin. Lisäksi haluttiin selvittää, keneltä tai mistä vastaaja etsii apua ongelmatilanteissa (kysymys 19). Tällä kysymyksellä selvitettiin sitä, tietävätkö vastaajat mistä hakea apua ja onko heillä mahdollisesti ohjeita avunhakuun työnantajan puolelta.

21. Kuinka tärkeänä pidät tietoturvaa päivittäisessä työssäsi?
22. Miten riittävänä koet oman osaamisesi ja tietämyksesi tietoturvaan liittyvissä asioissa?
23. Kuinka pelottavana koet ajatuksen työpaikallesi tapahtuvasta tietoturvamurrosta?
24. Kuinka todennäköisenä pidät työpaikallesi sattuvaa tietoturvamurtoa?

Kysymykset 21–24 olivat monivalintakysymyksiä asteikolla 1–6. Nämä kysymykset kuvasivat vastaajan omaa mielipidettä kysymysten aiheisiin, eikä näillä pyritty kartoittamaan osaamisen tasoa. Asteikko valittiin yhdestä kuuteen, jotta voitiin estää vastaajilta keskimmäisen vaihtoehdon valinta. Tämä tehtiin, jotta vastaajan oli pakko kallistua hieman enemmän puoleen tai toiseen.

Kyselyssä oli kolmen kysymyksen kohdalla mahdollisuus lisäkysymyksiin riippuen monivalintavastauksesta. Mikäli kysymykseen 4. ”Aloititko työsi etänä, vai siirryitkö etätöihin koronatilanteen vuoksi?” vastasi siirtyneensä etätöihin, antoi kysely vastaajalle jatkokysymykset:

4.1 Mitä ohjeita sait siirtyessäsi etätöihin?
4.2 Koitko nämä ohjeet riittäväksi?

Mikäli kysymykseen 8. ”Käytätkö VPN-yhteyttä?” vastasi myöntävästi, seurasi tästä jatkokysymys:

8.1 Millaisissa tilanteissa käytät VPN-yhteyttä?

Mikäli kysymykseen 13. ”Onko sinulla työsähköposti?” vastasi myöntävästi, seurasi tästä jatkokysymys:

13.1. Käytätkö työsähköpostia mihinkään muuhun kuin työasioihin?

### 4.3 Haastateltavat

Haastatteluihin sopivat henkilöt, jotka tekevät tai ovat tehneet etätöitä. Etätyön ajankohtaa ei rajattu COVID-19-pandemian ajalle, vaan kaikki kokemukset etätyöskentelystä nähtiin tärkeinä. Sekä kasvotusten suoritettu haastattelu että verkkokysely toteutettiin nimettömänä. Näin haastateltavat pystyivät vastaamaan totuudenmukaisesti pelkäämättä, että heidän oma tai heidän työnantajansa nimi on näkyvillä missään tutkimuksenteon vaiheessa. Tietoturvaan ja sen puutoksiin liittyvät aiheet voivat olla henkilökohtaisia ja arkaluontoisia, ja valinnalla pyrittiin luomaan luotettavaa ja turvallista vastausilmapiiriä.

Kasvotusten toteutettaviin haastatteluihin valittiin kolme henkilöä, jotka ovat tehneet tai tekevät vieläkin etätöitä. Haastateltaviksi valittiin eri alojen työntekijöitä otannan monipuolisuuden vuoksi.

Verkkokyselyä jaettiin henkilöille, joiden tiedettiin olevan tai olleen etätöissä. Lisäksi sitä jaettiin Tampereen ammattikorkeakoulun kanavien kautta opiskelijoille. Opiskelijoita pyydettiin vastaamaan vain, jos he ovat tehneet etätöitä (etäopiskelua ei laskettu). Verkkokyselyn alussa oli saateteksti (Liite 1.).

### 4.4 Haastattelun toteutus ja analyysi

Haastattelut toteutettiin kasvotusten haastateltavan kanssa. Kysymyksinä käytettiin täysin samoja kysymyksiä kuin verkkokyselyssä (luku 4.2). Ero verkkokyselyyn oli siinä, että haastateltava pystyi vastaamaan halutessaan vapaammin tai tarkentamaan vastaustaan. Haastattelut nauhoitettiin, jotta niistä saatu raakadata on tallella. Haastatteluiden äänitallenteet litteroitiin jälkikäteen tekstimuotoon ja näistä kirjattiin analyysivaiheessa vastaukset ylös verkkohaastattelun tapaan. Mikäli vastauksen yhteydessä oli annettu tarkentava vastaus tai avoimeen kysymykseen on vastattu yksityiskohtaisesti, otettiin vastauksesta myös tarkentava osa mukaan analyysiin.

Verkkokysely toteutettiin Google Forms palvelua käyttäen. Formsilla pystyttiin luomaan tutkimukseen tarkoituksenmukainen kysely siten, että sen jakaminen

haastateltaville oli nopeaa. Kyselyn kysymykset ovat listattuna luvussa 4.2. Forms kerää kyselyn vastaukset yhteen ja luo esimerkiksi monivalintakysymyksistä yhteenvetoja suuresta vastausmäärästä. Jälkikäteen myös yksittäisiä vastauksia voi lukea tarkemmin.

Sekä haastatteluista litteroidut vastaukset että verkkokyselyn vastaukset koottiin analyysivaiheessa taulukoihin. Vastauksista poistettiin vastaajatunnisteet, jotta työhön sitaateiksi päätyvistä vastauksista ei voi muodostaa tarkempaa kuvaa yksittäisen vastaajan kyselyvastauksista.

# 5 TUTKIMUKSEN TULOKSET

## 5.1 Haastattelu

Kasvotusten suoritettaviin haastatteluihin osallistui kolme haastateltavaa. Kaikki kolme haastattelua suoritettiin erikseen. Haastattelija tiesi haastateltavan etukäteen ja heitä oli pyydetty osallistumaan tutkimukseen, sillä oli tiedossa heidän olevan eri ammattialan harjoittajia. Haasteltaville kerrottiin aluksi verkkokyselyn saatetekstin mukaiset asiat (liite 1). Haastattelut numeroitiin toteutusjärjestyksessä.

### 5.1.1 Haastattelu 1

Ensimmäinen haastateltava on erään kunnan sosiaalialan työntekijä, joka siirtyi etätöihin COVID-19-pandemian vuoksi (luku 4.2 kysymykset 1, 4). Tietoturva tarkoitti hänelle sitä, että asiakkaiden tiedot pysyvät salassa ja että on luottamuksellisuus siihen, että arkaluontoiset asiat pysyvät turvassa. Kun haastateltavalta kysyttiin mitä tulee mieleen termistä tietoturvamurto haastateltava vastasi että ”*Mulle tuli Vastaamo mieleen ensimmäisenä.”* Vastaus viittaa luvussa 2.2 esiteltyyn Vastaamo tapaukseen. Lisäksi haastateltava kertoi tietoturvamurron tarkoittavan, että joku pääsee katselemaan salassa olevia tietoja ilman lupaa. (luku 4.2 kysymykset 2, 3.)

Haastateltava kertoi etätyön siirtymästä että ”*Meillä tuli se tosi yllätyksenä, yks perjantai iltapäivä niin siinä sitten niinkun muutama tunti saatiin ohjeistusta siihen asiaan ja sitten jatkettiin seuraavalla viikolla. Se tuli yllättäen*.” Haastateltavan kohdalla etätyöhön siirtyminen tapahtui siis erittäin nopeasti ja siirtymässä ohjeistus oli hänen kokemuksensa mukaan vähäistä. Haastateltava ei kokenut ohjeistuksia siirtymävaiheessa riittäviksi, mutta lisäsi että ohjeistuksia tuli pikkuhiljaa etätyön aikana lisää. (luku 4.2 kysymykset 4.1, 4.2.) Haastateltava on kertomansa mukaan osallistunut työsuhteensa aikana tietoturvakoulutuksiin ja on yleisellä tasolla saanut omasta mielestään tarpeeksi koulutusta tietoturvaan liittyvissä asioissa. (luku 4.2 kysymykset 5, 6).

Haastateltavalta kysyttiin käyttääkö tämä avoimia verkkoja; ”*En varmaan käytä, mutta en myöskään tiedä mikä avoin verkko on. Mutta en myöskään en mä työasioita tee missään tommosissa paikoissa*.” Paikka viittaa tässä kysymyksessä annettuun esimerkkiin ”esim. hotellissa/lentokentillä.” (luku 4.2 kysymys 7.) Haastateltava kertoi käyttävänsä VPN yhteyttä työasioissa. Lisäselvennyksenä haastateltava kertoi, että työkonetta käytettäessä pitää olla VPN yhteys päällä aina verkkoon yhdistäessä. (luku 4.2 kysymykset 8, 8.1.)

Salasanaan liittyvissä kysymyksissä haastateltava ei halunnut kertoa käyttääkö samaa salasanaa useassa eri paikassa. Haastateltava kuitenkin kertoi, että työpaikka määrittelee käytettävien salasanojen sisällön (pituus merkit jne.) Vaatimuksena on 6–10 merkkiä ja sen on sisällettävä iso kirjain. Töissä salasanaa tulee vaihtaa noin muutaman kuukauden välein. (luku 4.2 kysymykset 9, 10, 11.) Etätyössä käytettävä laite on suojattu tunnistusjärjestelmällä. Haastateltava ei osannut kuvailla tunnistusjärjestelmää kovin tarkasti, mutta kertoi että laite kysyy välillä henkilökohtaisia PIN-koodeja ja järjestelmään pitää tunnistautua. (luku 4.2 kysymys 12.) Työsähköpostista haastateltava kertoi, että hänellä on työsähköposti ja käyttää sitä myös työn ulkopuolisiin asioihin (luku 4.2 kysymykset 13, 13.1).

Työssä liittyvää dataa haastateltava säilyttää osan paperisena kotona ja osan työkoneella. Kotona ei ole turvakaappia, mutta hän kertoi siirtävänsä paperit pois muiden silmistä. Työkoneella tarvitsee VPN yhteyden päästäkseen käsiksi dataan, eli arkaluontoinen data ei ole vain lokaalisti työkoneella. (luku 4.2 kysymys 14.) Haastateltavan mukaan työnantaja tarjoaa kaikki etätyöhön tarvittavat työvälineet. Välineinä toimii kannettava tietokone ja älypuhelin (luku 4.2 kysymys 15). Laitteiden päivitykseen liittyen haastateltava kertoi, että joskus IT-tuki hoiti päivitykset, mutta nykyään koneelle tulee automaattisesti muistutus päivityksestä ja se hoidetaan itse. Haastateltava ei osannut sanoa tarkasti, kuinka usein päivityksiä tulee tai kuinka nopeasti ne hoidetaan. (luku 4.2 kysymys 16.) Haastateltavalta kysyttiin päivitysten ohjeistamisesta ja siitä pitikö se opetella itse; ”*Noh, ennen vanhaan ei pitäny, mutta nykyään meidän pitää kaikki osata itse, elikkä että pitää itse opetella ja jos ei tiedä niin pitää semmoselta digihenkilöltä kysyy, neuvoo tai työkaverilta*.” (luku 4.2 kysymys 17.) Aiheeseen liittyen haastateltava

kertoi, että jos ilmenee ongelmia, johon tarvitsee apua, hänen pitää joko soittaa Tietoon (suomalainen ohjelmisto- ja palveluyhtiö) tai soittaa kunnan puolella jollekin, joka IT-asioista tietää paremmin. Kuitenkaan kunnalla ei ollut varsinaista IT-tukihenkilöä, jolle soittaa. (luku 4.2 kysymys 19.)

Haastateltavan mielestä etätyö on riskialttiimpaa tietoturvan kannalta kuin lähityö. Haastateltava ei antanut esimerkkejä, miten työpaikan tietoturvaa voisi parantaa. (luku 4.2 kysymykset 18, 20.) Lopuksi haastateltava vastasi monivalintakysymyksiin, jotka olivat asteikolla 1–6 (luku 4.2 kysymykset 21, 22, 23, 24);

21. Kuinka tärkeänä pidät tietoturvaa päivittäisessä työssäsi?
→ ”*No toi kutonen, hyvin tärkeänä*”

22. Miten riittävänä koet oman osaamisesi ja tietämyksesi tietoturvaan liittyvissä asioissa?
→ ”*No pistä toi nelonen*”

23. Kuinka pelottavana koet ajatuksen työpaikallesi tapahtuvasta tietoturvamurrosta?
→ ”*Pistä se kolmonen siihen, en mä sitä oo niin miettiny*”

24. Kuinka todennäköisenä pidät työpaikallesi sattuvaa tietoturvamurtoa?
→ ”*Pistä se kolmonen, eihän sitä koskaan tiedä*”

### 5.1.2 Haastattelu 2

Toinen haastateltava on kiinteistöalan työntekijä, joka siirtyi etätöihin COVID-19-pandemian vuoksi (luku 4.2 kysymykset 1, 4). Haastateltavaa pyydettiin kertomaan tietoturvan tarkoitus hänelle omin sanoin; ”*Se on kovasti tapetilla ollu ja meilläkin on tehty hirveesti sen eteen ja tietysti mitä työtä määkin teen, niin käsittelen aika arkaluontosia asioita ja, että se on se juttu ja se on meidän firmassa tosi iso juttu*.”

Haastateltavaa pyydettiin kertomaan mitä tulee mieleen termistä tietoturvamurto; ”*Mul tulee heti mieleen tää kuuluisa firma, kun sen potilastiedot ryöstettiin, eli tullaan firman tietojärjestelmiin ja hakkeroidutaan sielä ja ryöstetään tietoja ja levitetään tietoja ja kiristetään*.” ”Kuuluisa firma” viittaa jälleen psykoterapiakeskus Vastaamoon (luku 2.2) niin kuin haastattelussa 1 (luku 5.1.1). ”*Tietomurto tietysti voihan se olla sitäkin, että ryöstetään paperijuttuja, että ei se pelkästään tietokoneisiin liity*.” Haastateltava tunnistaa tietoturvan ajankohtaisuuden ja kertoo työssään tärkeäksi. (luku 4.2 kysymykset 2, 3.)

Etätyöhön siirtymästä haasteltava kertoi, että etätyöhön ei saatu varsinaista ohjeistusta. Hän kertoi, että ”*omaa työtähän me tehdään*”, mutta etätyöskentelyyn ei ohjeistusta annettu. Kun kysyttiin ohjeiden riittävyydestä, haasteltava nauroi. Selkeästi hänen saamansa olemattomilta tuntuvat ohjeet eivät olleet riittäviä. (luku 4.2 kysymykset 4.1, 4.2.) Haastateltava kertoi, että työpaikalla on ollut tietoturvakoulutuksia, mutta ne ovat kunnolla lisääntyneet vasta etätyön alettua. Hän lisäsi kuitenkin, että puhetta oli ollut aiemminkin EU:n uusista tietoturvamuutoksista. Tällä haastateltava viittasi EU:n tietosuoja-asetukseen (GDPR). Hän ei osannut sanoa onko työpaikalla tarjottu yleisellä tasolla tarpeeksi koulutusta tietoturvasta. Haastateltava kertoi, että hän ei koe olevansa ainakaan ekspertti asiassa. (luku 4.2 kysymykset 5, 6.)

Haastateltava kertoi, että hän ei käytä avoimia verkkoja. VPN-yhteyttä haastateltava käyttää jatkuvasti etätyössään esimerkiksi yhdistäessään työpaikan verkkoon. (luku 4.2 kysymykset 7, 8, 8.1.) Haastateltava ei halunnut kertoa käyttääkö samaa salasanaa useassa eri paikassa. Haastateltavan työpaikalla on määritelty salasanan vaatimukset; salasanan on oltava ainakin 11 merkkiä, siinä on oltava isoja ja pieniä kirjaimia ja salasanassa on oltava numeroita. Salasanan vaihtoaika tulee työpaikalta myös määrityksenä. Salasanan vaihto tulee haastateltavan mukaan useammin kuin puolen vuoden välein. (luku 4.2 kysymykset 9, 10, 11.) Haastateltavan etätyössä käyttämät laitteet (tietokone ja kaksi puhelinta) ovat kaikki suojattu salasanalla (luku 4.2 kysymys 12). Hän kertoi lisäksi, että hänellä on työsähköposti ja käyttää sitä myös muihin kuin työasioihin (luku 4.2 kysymykset 13, 13.1).

Haastateltava kertoi, että hänen työssään käyttämät fyysiset paperit hän säilyttää laatikossa, josta ei tiedä muut kuin hän itse ja mahdollisesti hänen puolisonsa. Puoliso ei kuitenkaan papereihin koske. Näitä papereita on myös poltettu, kun niitä ei ole enää tarvittu. Arkaluontoiseen dataan pääsee käsiksi tietokoneella vain VPN-yhteydellä. (luku 4.2 kysymys 14.) Työnantaja antoi käyttöön kaikki tarvittavat laiteet etätyötä varten. Laitteiden päivitys tapahtuu automaattisesti ilman, että haastateltavan tarvitsee itse tehdä mitään. (luku 4.2 kysymykset 15, 16, 17.)

Haastateltava pitää etätyötä ja lähityötä yhtä riskialttiina tietoturvan kannalta. Ongelmatilanteen sattuessa haastateltava voi ottaa yhteyttä ulkopuoliseen IT-tukiyritykseen. Lisäksi hänen osastollaan on tietotekniikkaosaajia, jotka ovat esimerkiksi etäyhteydellä auttaneet häntä ongelmissa. Haastateltava ei osannut kertoa mitään tapaa, jolla työpaikalla voisi parantaa tietoturvaa. (luku 4.2 kysymykset 18, 19, 20.) Kuten muissakin haastatteluissa, lopuksi oli monivalintakysymykset asteikolla 1–6 (4.2 kysymykset 21, 22, 23, 24);

21. Kuinka tärkeänä pidät tietoturvaa päivittäisessä työssäsi?
→ ”*Se on kyllä se kuus*”

22. Miten riittävänä koet oman osaamisesi ja tietämyksesi tietoturvaan liittyvissä asioissa?
→ ”*Meillä on kyllä sen verran hyvin hoidettu, että mun ei hirveesti tarvi osata, mutta en mä nyt koe myöskään, että mä olisin joku osaaja. Nyt mä sanoisin siihen johki kolmoseen ehkä* ”

23. Kuinka pelottavana koet ajatuksen työpaikallesi tapahtuvasta tietoturvamurrosta?
→ ”*No se on kyllä ihan kutosen luokkaa, että kyl se aika pelottavaa on* ”

24. Kuinka todennäköisenä pidät työpaikallesi sattuvaa tietoturvamurtoa?
→ Haastateltava: ”*No se on aina mahdollista, että siinä laitetaan johki siihen puoleenvälii, mistä sä et tykänny ollenkaan [Naurua]*”

Haastattelija: *”No se on kolme tai neljä*”

Haastateltava: ”*Laita sitten vaikka se neljä*”

### 5.1.3 Haastattelu 3

Kolmas haastateltava on töissä kirkolla johtavassa asemassa ja siirtyi etätöihin koronatilanteen vuoksi (luku 4.2 kysymykset 1, 4). Hän kuitenkin kertoi etätöiden olleen mahdollista jo pidempään hyvien tietoturva- ja verkkoratkaisuiden vuoksi. Omin sanoin henkilö kuvasi tietoturvaa: ”*No se tarkoittaa sitä, että koneet on vain omassa käytössä, ei luovuteta muille, ei jätetä autoihin tai muuta vastaavaa. Ehkä myös sitä, että kun poistutaan omalta työpisteeltä, niin pitäisi muistaa lukita tietokone, kun meillä käsitellään henkilökohtaisia tietoja ja kalentereissa on arkaluontoisia asioita ja paljon salassa pidettävää tietoa.*” Tietoturvamurrosta ilmenevät ajatukset haastateltava kuvasi sanoin: ”*No se on sitä, että joku on johonkin meidän laitteeseen tunkeutunut… meillä niitä on aika vähän ollut – enemmän ne on ollu tämmösiä viruksia esim. kännykässä tai jonkun sähköpostin tai sovelluksen kautta.*” (luku 4.2 kysymykset 2, 3.)

Siirtoa etätöihin haastateltava kuvasi helpoksi, sillä mahdollisuus tähän oli rakennettu jo aikaisemmin, ja jokaisella työntekijällä oli jo valmiiksi kannettava tietokone. Etätyöhön siirryttäessä saatuja ohjeita hän kuvasi: ”*Saatiin jotakin ohjeita, mutta aika vähän loppujen lopuksi – esimerkiksi kokouskäytäntöihin tuli ohjeita liittyen luottamuksellisiin asioihin*” Kysyttäessä kokiko hän ohjeet riittäväksi, hän totesi: ”*No ei ainakaan liikaa ollut ohjeita, varmaa olis voinut olla jotain pelisääntömuistutuksia tästä tänä aikana. Välillähän sieltä IT tuelta tulee joku muistutus, mutta niilläkin on aika paljon omia töitä, niin ei ne aina kerkiä.*” (luku 4.2 kysymykset 4.1, 4.2.)

Haastateltava kertoi olleensa tietoturvakoulutuksessa ja jatkoi vielä: ”*Meillä on semmoinen käytäntö, että ennen kun saadaan laitteet, niin meidän pitää allekirjoittaa tietosuojasitoumus ja siinä sitoudutaan käymään semmoinen puolikkaan päivän mittainen tietosuojakoulutus yhden kerran. Siitä kyllä on jo aika kauan aikaa, niin en tiedä olisiko paikallaan pieni kertaus*.” Haastateltava ei osannut sa-

noa oliko saanut mielestään tarpeeksi tietoturvakoulutusta, sillä hän otti huomioon muut työpaikallaan työskentelevät (varsinkin iäkkäämmät) henkilöt, jotka joutuisivat myös opettelemaan saman asian. ”*Se opetuskokonaisuus ei voi olla liian laaja ja rima tulee asettaa sopivalle korkeudelle, että kaikki voi sen hyvin omaksua*.” (luku 4.2 kysymykset 5, 6.)

Haastateltavalta kysyttäessä käyttääkö hän avoimia verkkoja, ei hän oikein osannut sanoa, sillä ei ollut täysin varma mitä avoin verkko tarkoittaa. VPN- yhteydestä kysyttäessä hän vastasi ”*Juu varmaankin… en kyllä tiedä..*”. Pienen selventämisen jälkeen selvisi, että hän käyttää VPN- yhteyttä, mutta termi ei vain ollut hänelle entuudestaan tuttu. Työpaikalla oli vain ohjeistettu ”aukaisemaan yhteys tästä”. (luku 4.2 kysymykset 7, 8)

Haastateltava käyttää samaa salasanaa useassa eri paikassa ja tämä useimmiten koostuu n. 10 merkistä, isoista sekä pienistä kirjaimista, numeroista ja merkeistä. Salasanan muodostamisen hän kertoi muistaneensa aikoinaan suorittaneesta tietoturvakoulutuksesta. Salasanan hän vaihtaa sanojensa mukaisesti ”*Talon puolesta se tulee vaihtaa 3 tai 4 kertaa vuodessa, siitä tulee aina ilmoitus… Voisinhan mä sen vaihtaa aikaisemmin, mutta tuolloin se on pakko vaihtaa*”. Haastateltavan laite on suojattu pelkällä salasanalla. (luku 4.2 kysymykset 9, 10, 11, 12.)

Haastateltavalla on työsähköposti ja hän käyttää sitä myös muihin kuin työasioihin: ”*Tulee käytettyä myös normi asioihin vaikkakin ohjeet on, että ei pitäs… mutta kun ei millään jaksa käyttää useita eri sähköposteja.*” (luku 4.2 kysymykset 13, 13.1.)

Työssä säilytettävän datan haastateltava osasi hyvin paikantaa: ”*No sitä säilytetään kolmessa eri paikassa, eli tietokoneen omassa muistissa (työpöydällä pääasiassa), meidän palvelimessa/serverillä on henkilökohtaiset kansiot ja työyksiköille omat, mutta nykyisin on menty enempi pilvipalveluun (onedrive)… ja sitten jos käytetään tämmösiä teams ja onenote -juttuja niin niistä data menee johkin sharepointtiin.*” (luku 4.2 kysymys 14.)

Haastateltavan työnantaja tarjoaa kaikki etätyössä tarvittavat työvälineet. Päivityksistä kysyttäessä hän kertoi: ”*Nooo… harvoin sitä itse tarvii näitä päivittää, kun ne tekee etäohjattavasti kaikki päivitykset IT puolelta… ne ajaa ne jotenkin kun kirjautuu siihen meidän paikallisverkkoon. Itse ei tarvitse päivittää kun kännykkää.*” (luku 4.2 kysymykset 15, 16, 17.)

Haastateltava koki, että etätyö on huomattavasti riskialttiimpi tietoturvan kannalta, sillä: ”*tiedän olevani aina oikeassa verkossa, kun olen fyysisesti paikanpäällä*”. Teknisen ongelman ilmaantuessa haastateltava kertoi voivansa olla yhteydessä päivystysnumeroon tai online-helpdesk -palveluun. Haastateltavan mielestä hänen työpaikallaan voisi parantaa tietoturvaa pitämällä parempaa huolta laitteiden fyysisestä turvallisuudesta esimerkiksi kaupungilla liikuttaessa, että näitä ei jätettäisi ikinä lojumaan mihinkään, vaan se olisi aina siinä vierellä. (luku 4.2 kysymykset 18, 19, 20.)

21. Kuinka tärkeänä pidät tietoturvaa päivittäisessä työssäsi?
→ ”*No viitonen*”

22. Miten riittävänä koet oman osaamisesi ja tietämyksesi tietoturvaan liittyvissä asioissa?
→ ”*Kakkonen… Eikun laita kolmonen, koska on niitä paljon vähemmän tietäviä*”

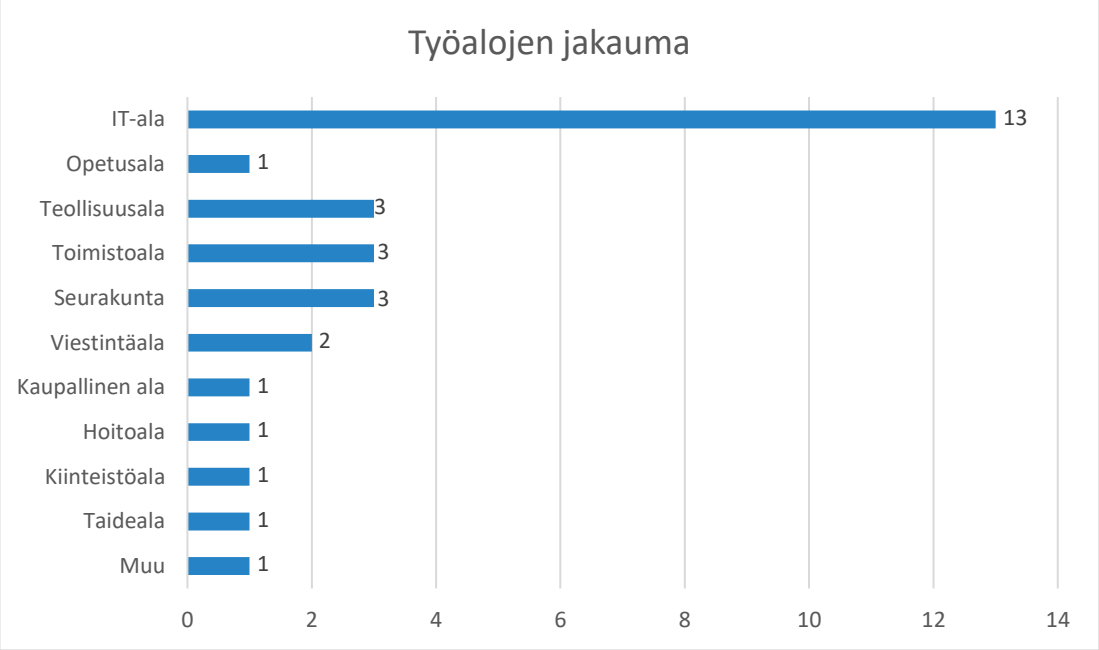
23. Kuinka pelottavana koet ajatuksen työpaikallesi tapahtuvasta tietoturvamurrosta?
→ ”*No se on kyllä tosi pelottava ajatus… Kuitenkin käsitellään niin arkaluontoisia tietoja ihmisistä… viitonen*”

24. Kuinka todennäköisenä pidät työpaikallesi sattuvaa tietoturvamurtoa?
→ ”*Kolmonen tai kakkonen… siltä väliltä*”

## 5.2 Verkkokysely

Verkkokyselyyn vastasi 31 henkilöä. Vastauksista piti analyysivaiheessa poistaa yhden vastaajan vastaukset, sillä kysymyksiin ei ollut vastattu ohjeiden mukaisesti. Tutkimukseen käytettäviä vastauksia saatiin siis 30:lta vastaajalta. Vastaajien työaloissa oli vaihtelua, eli otantaan saatiin hyvää varianssia.

Vastanneiden työalat on kuvattu kuviossa 1. Yksittäisen alan vastaajia oli eniten IT-alalla. IT-alan vastaajia oli 13 kappaletta, joka on 43,3 % kaikista vastaajista. Kuviossa 1 kuvattu kohta ”Muu” viittaa erääseen vastaukseen, missä vastaaja ei kertonut työalaansa, mutta kertoi olevansa eräällä kaupungilla/kunnalla töissä. (luku 4.2 kysymys 1.)




KUVIO 1. Kyselyyn vastanneiden työalat

Useat vastaajat kertoivat tietoturvan tarkoittavan sitä, että tiedot pysyvät turvassa eivätkä leviä ulkopuolisille. Jotkut kertoivat myös ominaisuuksista tai teknisistä vaatimuksista. Eräs vastaaja mainitsi jopa OWASP:in (Open Web Application Security Project), joka on voittoa tavoittelematon yhdistys, jonka tarkoituksena on parantaa ohjelmistojen turvallisuutta. (luku 4.2 kysymys 2.) Tietoturvaa kuvailtiin esimerkiksi seuraavasti:

*”Tietoturva tarkoittaa minulle kontrollia siitä mikä tieto leviää minnekin. Tietoturva on myös luottoa tekniikkaan”*

*”F-Securea, ohjeistusta, sääntöjä, harkintaa”*

*”Sitä, että ihmisten yksityisyyttä suojellaan ja henkilökohtaisia tietoja ei pääse ulkopuolisten käyttöön ja nähtäväksi.”*

*”Suojaa minua viruksilta, ulkopuolisilta verkkohyökkäyksiltä yms.”*

Tietoturvamurrosta vastaajille tuli mieleen tilanteet, joissa ulkopuolinen henkilö tai taho pääsee käsiksi salattuihin tietoihin. Jotkut vastaajat kuvasivat tietoturvamurtoon johtavia asioita, kuten osaamattomat työntekijät tai huono tietoturvataso. Moni vastaaja mainitsi Vastaamon tietoturvamurron (luku 2.2), kuten haastatteluissakin. Eräs kuvasi tietoturvamurron tarkoittavan tietoturvan vastakohtaa. (luku 4.2 kysymys 3.) Tietoturvamurtoon liittyviä vastauksia:

*”Ulkopuolisen- ei toivotun tahon luvaton tietojen tai järjestelmien käyttö. Tietovarkaudet tulevat mieleen, esim. case Vastaamo.”*

*”Tiedon suojaus on epäonnistunut ja jokin taho on päässyt käsiksi tietoon, joka ei kuulu sille.”*

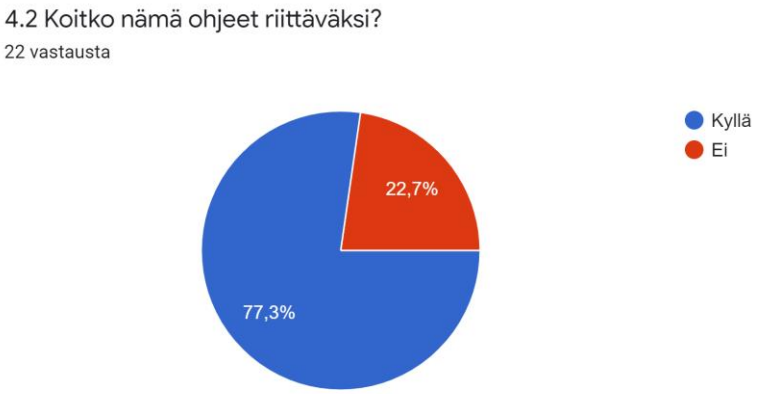
*”Työtä. Tietoturvamurtoja on monen tasosia, ja valitettavasti osa arkea. Tietysti termiin tulee kauhun fiiliksiä, siitä mahdollisuudesta, että murto voi olla pahempi ja suurempi kuin nämä 'arkiset' tapaukset.”*

COVID-19-pandemian vuoksi moni kyselyyn vastanneista on joutunut siirtymään etätöihin. Kuviosta 2 nähdään, että vain 23,3 prosenttia eli seitsemän (7) vastaajaa aloitti työnsä etänä. Muut 23 vastaajaa ovat siirtyneet etätöihin. (luku 4.2 kysymys 4.)


KUVIO 2. Etätöihin siirtymisen määrä

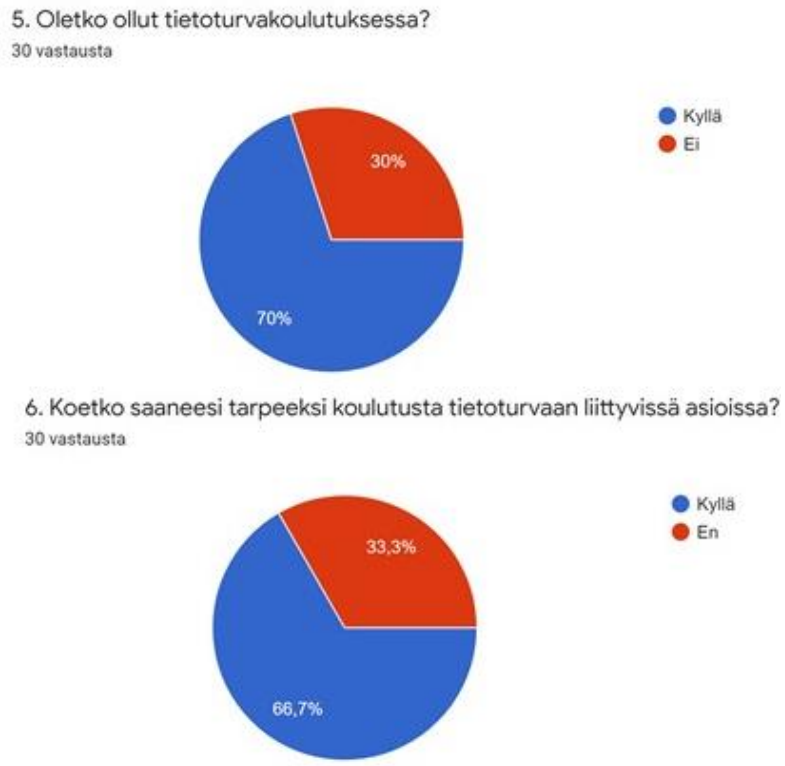
Henkilöt, jotka vastasivat siirtyneensä etätöihin, saivat kaksi lisäkysymystä etätyösiirtymästä: ” 4.1. Mitä ohjeita sait siirtyessäsi etätöihin?” sekä ”4.2. Koitko nämä ohjeet riittäviksi?”. Vastaajien mukaan he eivät ole saaneet laajoja ohjeistuksia etätyöhön. Vastaajat mainitsivat esimerkiksi yleiset lyhyet ohjeet VPN:n käytöstä ja yleiset ohjeet laitteiden etäkäytöstä. Joissakin yrityksissä etätyö oli jo valmiiksi mahdollista, ja tällöin myös ohjeistus oli saatu aikaisemmin esimerkiksi työhön perehdytyksen aikana. Kuviosta 3 nähdään, että vaikka ohjeistukset eivät olleet kovin laajoja, suurin osa (77,3 %) koki ne kuitenkin riittäviksi. (luku 4.2 kysymykset 4.1, 4.2.) Etätyön ohjeistuksesta (Kysymys 4.1.) kerrottiin seuraavaa:

> ”*VPN:n käyttö, ei tullut mitään erityisiä ohjeita.”*
>
> *”En mitään erityisiä ohjeita. Toimintamallit tuli kehittää itse.”*
>
> *”Potilaspaperit piilossa, tietokoneen käyttö rauhallisessa tilassa kotona.”*
>
> *”Kirjautumisohjeet ja laitteiden käyttämiseen ja lukitsemiseen liittyvät ohjeet.”*



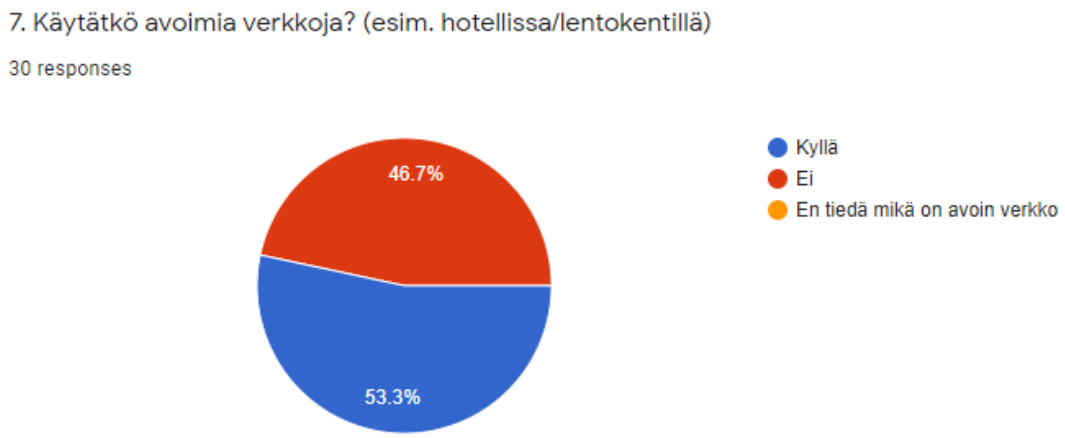

KUVIO 3. Etätyö siirtymän ohjeiden riittävyys

Tämän jälkeen kyselyssä siirryttiin selvittämään tietoturvaosaamisen tasoa selvittämällä osallistumista tietoturvakoulutukseen ja kokemusta koulutuksen riittävyydestä. Kuviosta 4 voidaan havaita korrelaatiota tietoturvakoulutukseen osallistumisen ja koulutuksen riittävyyden välillä. (luku 4.2 kysymykset 5, 6.) Näyttäisi siltä, että koulutukseen osallistuvat kokevat saaneensa tarpeeksi koulutusta, kun taas samalla koulutuksiin osallistumattomat vastaajat kokevat, että he eivät ole saaneet koulutusta riittävästi.




KUVIO 4. Tietoturvaosaamisen taso

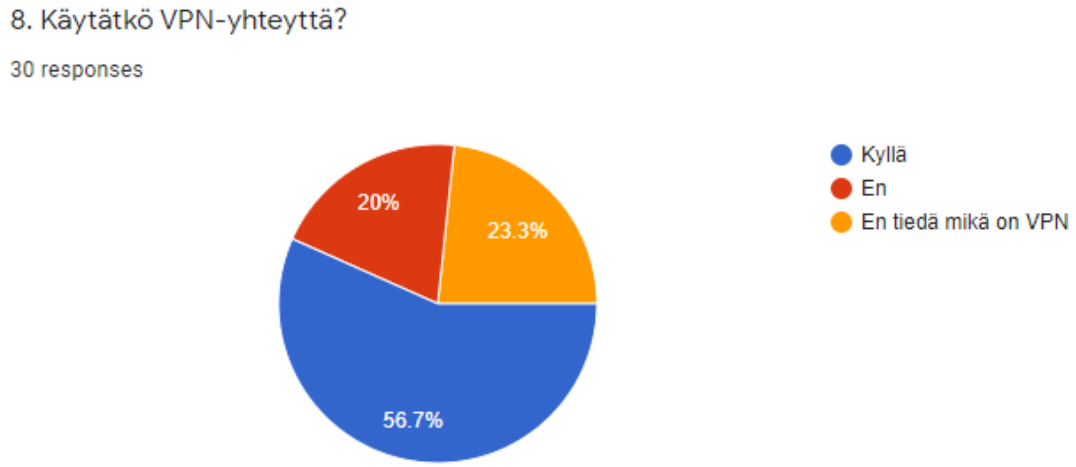
Seuraavaksi kyselyssä kartoitettiin avoimien verkkojen, sekä VPN-yhteyden käyttöä. Tällä saatiin tarkennettua kuvaa vastanneiden teknisestä tietämyksestä. Kuviosta 5 nähdään, että avoimet verkot olivat kaikille entuudestaan tuttu käsite. Vastaajista vähän yli puolet (53,3 %) käyttää avoimia verkkoja. Kysely ei selvittänyt käyttötarkoitusta. (luku 4.2, kysymys 7.)




KUVIO 5. Avoimien verkkojen käyttö

Kuviosta 6 nähdään, että VPN-yhteys -käsite oli usealle vastaajalle tuntematon (23,3 %). On mahdollista, että osa vastaajista käyttää VPN-yhteyttä tietämättään. Myös haastattelussa (haastateltava3, luku 5.1.3.) tuli tarkentavan keskustelun jälkeen ilmi, että haastateltava käyttikin VPN:n yhteyttä, muttei osannut yhdistää sen käyttöä ohjeistukseen ”yhteyden avaamisesta”.

On kuitenkin todennäköistä, että ”en”-vastauksen valinneet vastaajat eivät käytä VPN:ää, sillä vaihtoehtona oli vastata myös, että ei tiedä, mikä VPN on. Mikäli siis vastaajat käyttävätkin VPN:ää tietämättään, sisältyvät nämä vastaajat todennäköisesti ”En tiedä mikä on VPN” -vastaajiin. Kyselyn mukaan yli puolet vastaajista (56,7 %) kuitenkin käyttävät VPN-yhteyttä johonkin tarkoitukseen, joka selvitettiin seuraavaksi. (luku 4.2 kysymys 8.)




KUVIO 6. VPN-yhteyden käyttö

Mikäli henkilö vastasi käyttäneensä VPN- yhteyttä, sai hän lisäkysymyksen liittyen kyseisen yhteyden käyttöön (luku 4.2, kysymys 8.1). Pääasiassa VPN-yhteyttä käytettiin työasioiden hoitamiseen sekä laitteen yhdistämiseen työpaikalla käytettävään sisäverkkoon. Tilanteita kuvattiin seuraavin sanoin:

*”Avoimissa verkoissa.”*

*”Työpaikan sisäverkkoon kirjautumisessa ja verkkolevyasemien käytössä.”*

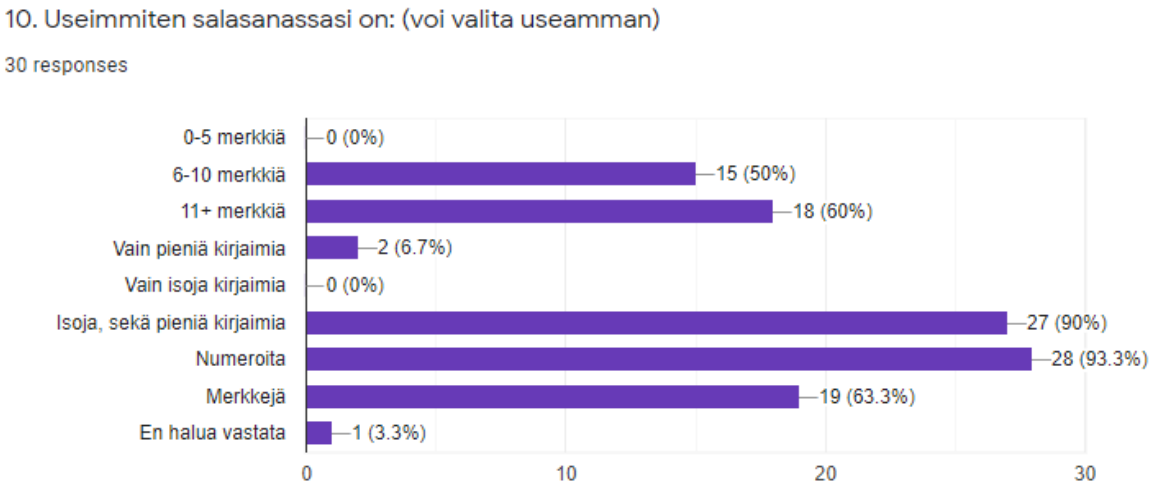
*”Kaikissa tilanteissa, jossa työskentelen edustamani yrityksen järjestelmissä.”*

*”Kun haluan suojata identiteettini tai en ainakaan halua että se on helposti selvitettävissä.”*

Seuraavaksi kysely siirtyi käsittelemään salasanaa. Tämä osio alkaa selvittämällä käyttääkö henkilö samaa salasanaa useassa eri paikassa. Salasanaan liittyviin kysymyksiin voi olla arveluttavaa vastata Internetin välityksellä, joten näihin kysymyksiin lisättiin vaihtoehto: ”En halua vastata.” Osa vastaajista (10 %) valitsikin olla vastaamatta. Kuviosta 7 nähdään, että 53,3 % vastanneista käyttää samaa salasanaa useassa eri paikassa. (luku 4.2, kysymys 9.)


KUVIO 7. Salasanan toistuvuus

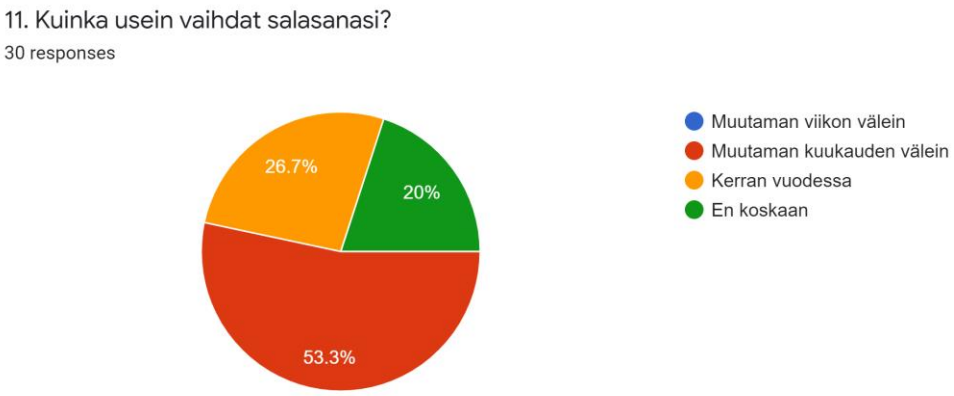
Seuraavaksi selvitettiin salasanan rakennetta ja pituutta. Vastaajan tuli rakentaa useimmiten käyttämänsä tapainen salasana useasta eri vaihtoehdosta. Jälleen kyselyssä mahdollistettiin ”en halua vastata” -vaihtoehto, jonka käytti yksi vastaaja. Kuvio 8 kuvaa vastaajien valitsemia salasanan rakenteita ja niiden yhdistelmiä. Yhdelläkään vastaajista ei ollut alle 6 merkkiä pitkiä salasanoja. Kukaan ei käyttänyt vain isoja kirjaimia ja vain kaksi käytti salasanassaan pelkkiä pieniä kirjaimia.  Suurin osa vastanneista käytti pitkiä salasanoja, eri kokoisia kirjaimia, numeroita ja erikoismerkkejä. (luku 4.2 kysymys 10.)




KUVIO 8. Salasanan rakenne

Seuraavaksi selvitettiin vastaajien aktiivisuus salasanan vaihtamisessa. Kysymykseen annettiin valmiit vaihtoehdot, jotta rajaus analyysivaiheen ryhmittelyyn

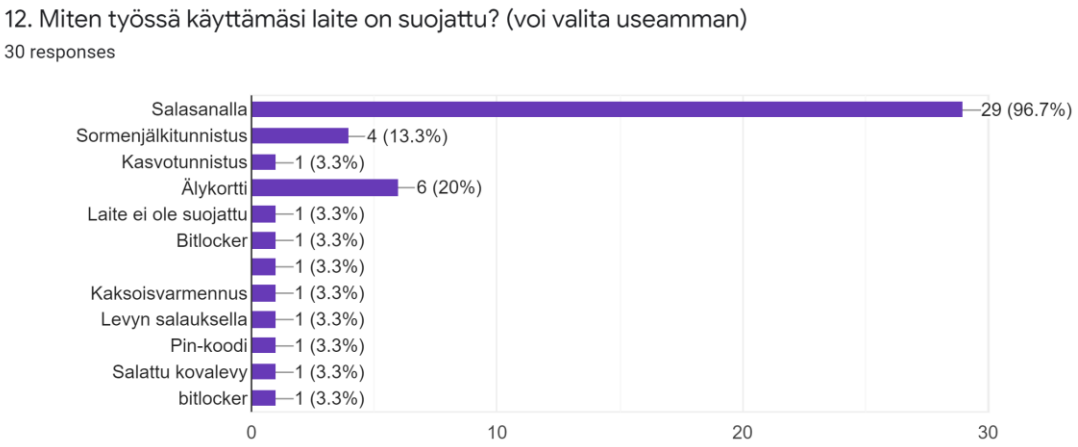
tapahtui automaattisesti. Kuviosta 9 nähdään, ettei kukaan vastanneista vaihda salasanaansa muutaman viikon välein, mutta osa (20 %) ei vaihda salasanojaan koskaan. Yleisin vastaus (53,3 %) oli ”muutaman kuukauden välein”. Osassa yrityksistä on säädökset sille, kuinka usein salasana pitää vaihtaa, mikä vaikuttaa myös salasanan vaihtamisen aktiivisuuteen. (luku 4.2 kysymys 11.)




KUVIO 9. Salasanan vaihtaminen

Seuraavaksi selvitettiin vastaajien työssä käytettävien laitteiden suojausmetodeja. Vastaajat pystyivät valitsemaan valmiiksi annetuista vaihtoehdoista yhden tai useamman, sekä lisäämään omia vastauksiaan. Kuvio 10 kuvaa näitä valintoja. Kuvion keskellä näkyvä tyhjä rivi on ”Suljettu verkkoyhteys tiettyihin ohjelmiin ja verkkoasemiin.” Vastaus oli niin pitkä, että se ei mahtunut kuvaajaan automaattisesti.

Yleisimmät vastaukset laitteen suojaamiselle olivat salasana (96,7 %), älykortti (20 %) ja sormenjälkitunnistus (13,3 %). Osa vapaasti kirjoitettavista vastauksista (Bitlocker ja suojattu kovalevy) valittiin enemmän kuin yhden kerran, mutta ne näkyvät kuviossa erillisinä kirjoitusasun eroavuuden vuoksi. (luku 4.2 kysymys 12.)




KUVIO 10. Laitteiden suojaus

Tämän jälkeen kyselyllä selvitettiin, onko haastateltavalla työsähköpostia (luku 4.2 kysymys 13). Kaikki vastanneet (30) vastasivat ”Kyllä”, jonka seurauksena he saivat jatkokysymyksen siitä, käyttävätkö he työsähköpostia muuhun kuin työasioiden hoitamiseen. Kuviosta 11 nähdään että yli puolet (60 %) vastaajista käyttää työsähköpostiaan myös muuhun kuin työasioihin. (luku 4.2, kysymys 13.1)


KUVIO 11. Työsähköpostin käyttö

Seuraavaksi selvitettiin, kuinka haastateltava säilyttää työhönsä liittyvän datan. Suurin osa vastaajista säilyttivät datan sähköisessä muodossa tietokoneella tai pilvipalvelussa. (Luku 4.2 kysymys 14.) Säilytystapojaan henkilöt kuvasivat seuraavin sanoin:

*”Pääosin työnantajan järjestelmissä. Joitakin muistiinpanoja on tallessa omalla työkoneella, salatulla levyllä.”*

*”Verkkoasemilla, mutta säilytän hyvin vähän. Arkistosäännöissä mainittavat dokumentit säilytetään toki myös paperisena ensin virastolla ja sitten päätearkistossa.”*

*”OneDrivessa, primessä, verkkoasemalla ja teamssissa”*

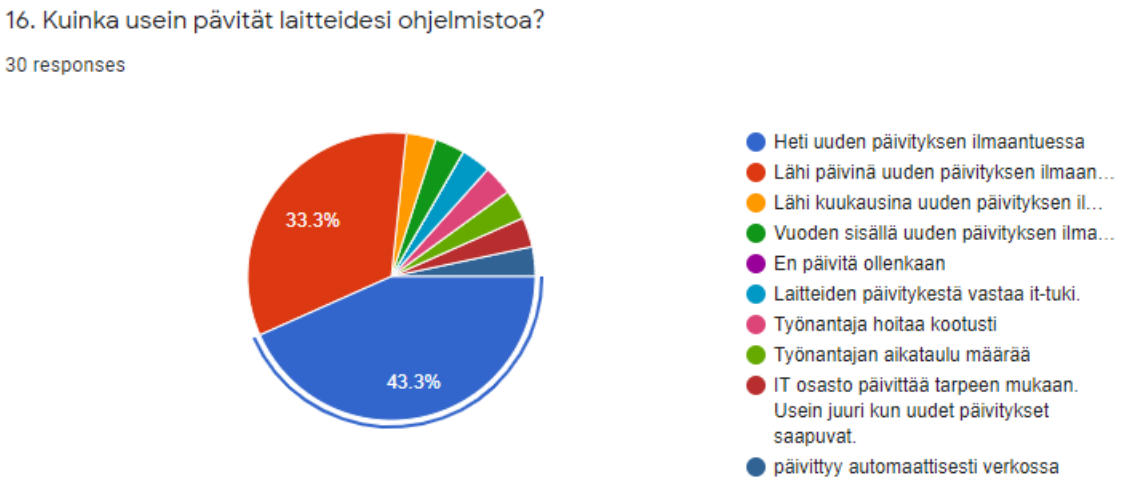
*”Työkoneella tai työpaikan tarjoamassa pilvitallennustilassa.”*

Sen jälkeen selvitettiin, tarjoaako työnantaja vastaajalle tarvittavat työvälineet etätöiden tekemiseksi. Kuvio 12 havainnollistaa, että suurin osa (76,7 %) sai kaikki tarvitsemansa työvälineet työnantajalta. Pieni osa (16,7 %) sai osan työvälineistä ja muutama (6,7 %) ei saanut tarvittavia työvälineitä. Todennäköisesti henkilöt, jotka eivät saaneet työvälineitä, joutuivat käyttämään omia henkilökohtaisia laitteitaan etätyön mahdollistamiseksi. (luku 4.2 kysymys 15.)


KUVIO 12. Työvälineet etätyössä

Seuraavaksi kyselyssä selvitettiin, kuinka usein henkilö päivittää laitteidensa ohjelmistoa, ja onko hänen työnantajansa ohjeistanut päivityksiin. Kysymykseen

(16) annettiin vaihtoehto luoda oma vastaus siltä varalta, ettei itse päivitä laitteitaan. Kuten kuviosta 13 nähdään, moni antoikin kysymykseen oman kirjallisen vastauksensa. Kaikki nämä vastaukset liittyvät joko siihen, että laite päivittyy automaattisesti tai joku muu hoitaa sen vastaajan puolesta. Näin oli noin 16,5 prosentilla. Noin 76,6 prosenttia vastanneista päivittää laitteet joko heti tai lähipäivinä uuden päivityksen ilmaantumisesta. (luku 4.2 kysymys 16.)




KUVIO 13. Laitteiden päivitys

Kuviosta 14 nähdään, että yli puolta (56,7 %) vastaajista oli ohjeistettu laitteiden päivityksestä työnantajan toimesta. Kysymys ei selvittänyt tarkemmin, miten vastaajia on tai miksi heitä ei ole ohjeistettu.

Kuten edellisessä kysymyksessä (kuvio 13) huomattiin, noin 16,5 prosentilla joku muu henkilö tai taho hoitaa laitteiden päivityksen. Tämä vaikuttaa myös työntekijöiden ohjeistuksiin. Mikäli päivitykset tapahtuvat automaattisesti tai muun tahon kautta, voi riittävä oheistus tarkoittaa selvitystä siitä, miten päivitys tapahtuu työntekijästä riippumatta.

Kuviosta 14 huomataan, että osa (43,3 %) ei ole saanut ohjeistusta lainkaan laitteiden päivittämisestä, mutta samalla iso osa laitteista päivitetään tai päivittyy oletettavasti ajallaan (kuvio 13). Kysymykset eivät siis tuo vastausta siihen, onko työnantajan ohjeistuksella vaikutusta laitteiden päivittämiseen. (luku 4.2 kysymys 17.)


KUVIO 14. Päivityksen ohjeistus

Tämän jälkeen selvitettiin, pitävätkö vastaajat etätyötä tai lähityötä riskialttiimpana tietoturvan kannalta. Vaihtoehdoiksi annettiin myös ”yhtä riskialttiita” ja ”en osaa sanoa” -vaihtoehdot. Kuviosta 15 nähdään, että kukaan vastanneista ei pidä lähityötä riskialttiimpana ja vain pieni osa (30 %) pitää etätyötä riskialttiimpana. Suurin osa (63,3 %) piti molempia työskentelytapoja yhtä riskialttiina. (luku 4.2 kysymys 18.)


KUVIO 15. Työskentelytapojen riskit

Seuraavaksi selvitettiin, osaavatko haastateltavat hakea apua laitteiden käyttöön tai tietoturvaan liittyvissä kysymyksissä ongelmien ilmaantuessa. Selvitettiin myös, mistä apua etsitään tai saadaan. Suurin osa vastaajista kertoi hakevansa apua IT- tuelta/ tekniseltä tuelta sekä työkavereiltaan. (luku 4.2 kysymys 19.) Avun hakemista vastaajat kuvasivat:

*”Työkavereilta, IT-osastolta, tietoturvavaltuutetulta”*

*”Ensisijaisesti pyrin itse ratkaisemaan ongelmat Googlen avulla, mutta tarvittaessa voin kysyä IT-osaajaltamme apua.”*

*”Kaupungin Servicedeskiltä”*

*”Laiteongelmille meillä on tarjolla tekninen tuki ja tietoturva-asioille on omat yhteyshenkilöt.”*

Viimeisenä avoimena kysymyksenä selvitettiin, olisiko vastaajilla ideaa tai ajatusta siitä, kuinka heidän työpaikoillaan voisi parantaa tietoturvaa. Myös tämä kysymys tehtiin vapaaehtoiseksi, sillä kysymys voi olla vaikea tai siihen ei välttämättä haluta vastata työnantajaan kohdistumisen vuoksi. Vastauksia tuli yhteensä 11 ja suurin osa näistä koostui työntekijöiden (varsinkin iäkkäämpien) kouluttamisesta. (luku 4.2 kysymys 20.) Seuraavassa esimerkkejä vastauksista:

*”Parempi etätyö-/tietoturvallisuuskoulutus. Monivaiheisen tunnistautumisen käyttöönotto”*

*”Kouluttaa vanhempaa henkilökuntaa”*

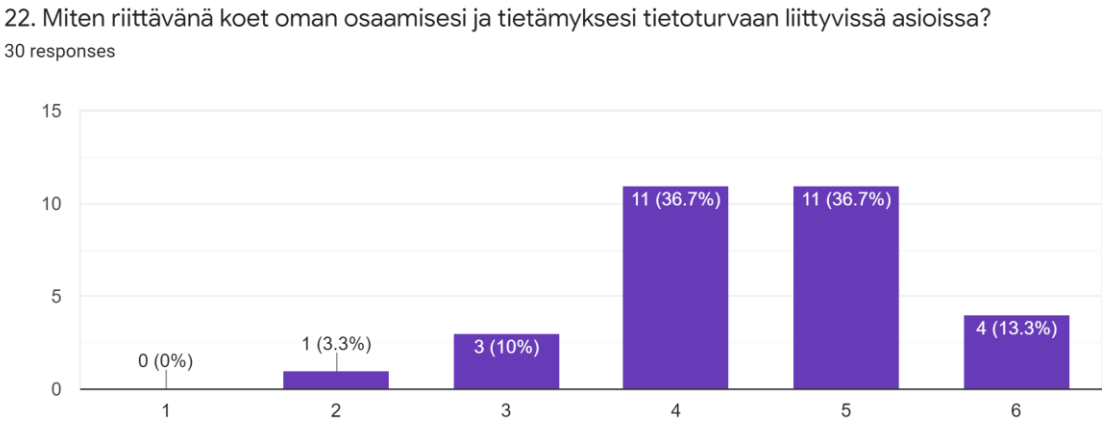
*”Tietoiskuja, että tietoturvaasiat olisivat kaikkien mielessä ja kaikki muistavat omalta osaltaan huolehtia siitä.”*

*”Tarjoamalla koulutusta riittävän usein.”*

Seuraavaksi kysely siirtyi monivalintaosioon. Osion kysymyksissä vastaajilla oli valittavanaan numeerinen arvo väliltä 1–6. Aluksi kysyttiin kuinka tärkeänä henkilö pitää tietoturvaa päivittäisessä työssään. Vastaukset annettiin asteikolla 1: ei tärkeä välille 6: hyvin tärkeä. Kuviosta 16 nähdään, että vastaajat pitävät tietoturvaa tärkeänä asiana. Vastaajista 96,7 prosenttia valitsivat vaihtoehdot 4–6 ja vain 3,3 prosenttia (yksi vastaaja) valitsi vaihtoehdon 3. (luku 4.2 kysymys 21.)


KUVIO 16. Tietoturvan tärkeys päivittäisessä työssä

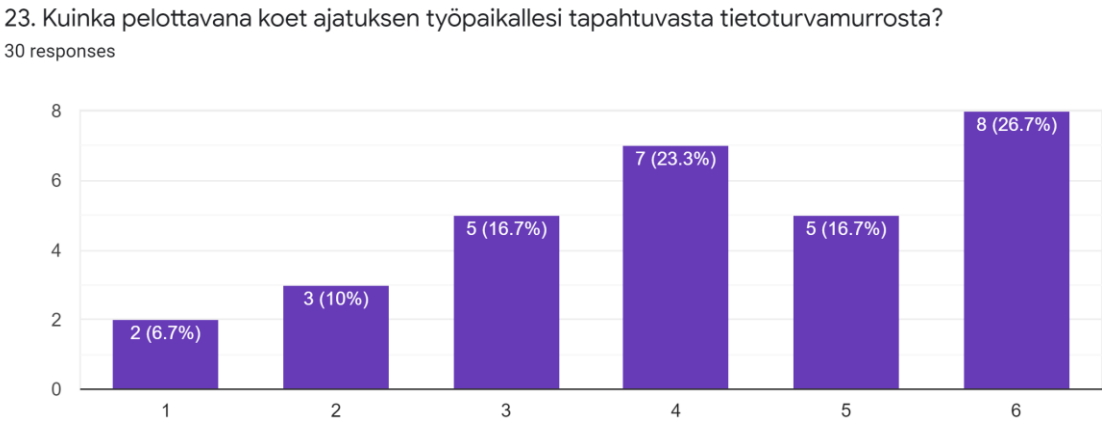
Tämän jälkeen selvitettiin, kuinka riittävänä henkilö kokee oman osaamisensa ja tietämyksensä tietoturvaan liittyvissä asioissa. Tässä kysymyksessä vaihtoehdot valittiin väliltä 1: täysin riittämätön ja 6: erittäin riittävä. Kuvio 17 kertoo, että tietoturvaosaaminen koettiin suurilta osin riittäväksi. 86,7 prosenttia vastaajista valitsi vaihtoehdot 4–6. (luku 4.2 kysymys 22.)




KUVIO 17. Osaamisen ja tietämyksen riittävyys

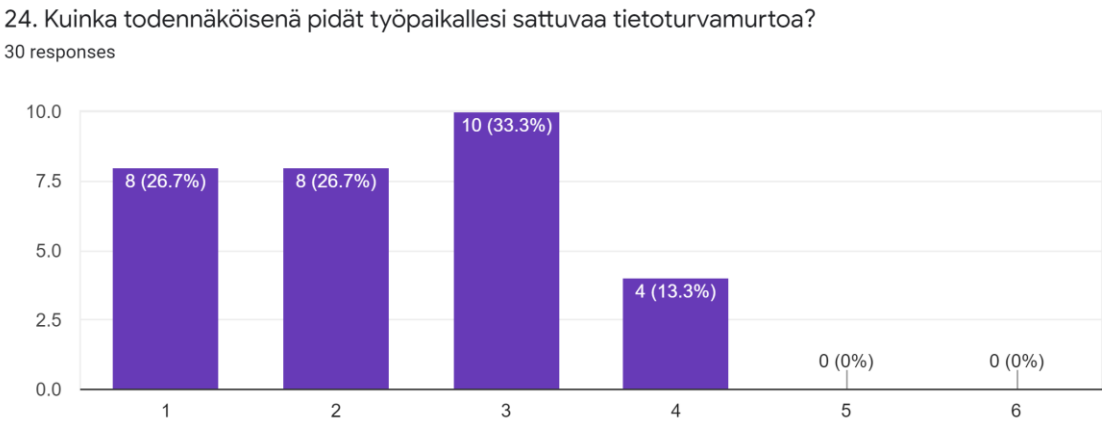
Viimeiset kaksi kysymystä käsittelivät haastateltavan työpaikalle tapahtuvaa kuvitteellista tietomurtoa. Aluksi selvitettiin, kuinka pelottavana koetaan ajatus kyseisestä tietomurrosta. Tässä kysymyksessä valittiin väliltä 1: vähiten pelottava ja 6: eniten pelottava. Kuvioista 18 nähdään, että yli puolet (66,7 %) vastasivat

vaihtoehdot 4–6 ja eniten yksittäisiä vastauksia oli vaihtoehdossa 6, eli tietoturvamurtoa pidettiin pelottavana ajatuksen tasolla. (luku 4.2 kysymys 23.)




KUVIO 18. Tietoturvamurron pelottavuus

Viimeisenä selvitettiin, kuinka todennäköisenä haastateltava pitää työpaikalleen tapahtuvaa tietoturvamurtoa. Kysymyksessä vaihtoedot valittiin väliltä 1: on hyvin epätodennäköistä ja 6: on hyvin todennäköistä. Kuviosta 19 nähdään, että tietoturvamurtoa ei pidetä kovin todennäköisenä. 83,7 prosenttia valitsi vaihtoehdon 1–3 ja kukaan ei valinnut vaihtoehtoja 5–6. (luku 2.4 kysymys 24.)




KUVIO 19. Tietoturvamurron todennäköisyys

# 6 TULOSTEN YHTEENVETO

## 6.1 Haastattelu ja verkkokysely

Haastateltavia saatiin tutkimukseen kolme henkilöä. Haastattelujen määrää pidettiin riittävänä niiden toimiessa lähinnä tueksi verkkokyselylle, jossa otanta oli suurempi. Haastattelujen teko ja niissä käyty keskustelu auttoivat tunnistamaan analyysivaiheessa verkkokyselyssä ilmeneviä mahdollisia ongelmakohtia, kun kysymykset olivat samat sekä haastattelussa että verkkokyselyssä. Koska tutkimuksessa ei käytetty pilottikyselyä, oli haastateltavien tarkentavat kysymykset ja lisäykset tärkeää tietoa kysymysten tulkitsemiseen liittyvissä ongelmissa.

Verkkokyselystä saatiin 30 käytettävää vastausta. Kyselyn validiteetin ja jatkokehityksen kannalta olisi ollut hyvä saada vielä enemmän vastaajia. Kuitenkin kyselyn avoimet kysymykset tarkensivat vastauksia ja vastaajien omin sanoin kirjoitetuista 30 vastauksesta oli nähtävillä yleistettäviä piirteitä.

Koska haastatteluissa ja verkkokyselyssä käytettiin samoja kysymyksiä, käsitellään näitä vastauksia samalla tavalla. Haastatteluista saatu datamäärä oli suurempi, koska vastaaja sai vapaasti vastata kaikkiin kysymyksiin sanallisesti. Kuitenkin vastauksia voidaan yleisesti käsitellä samanarvoisina. Tässä luvussa (luku 6) esitellään vastauksista löytyviä mahdollisia tietoturvaongelmia ja annetaan parannusehdotuksia niihin liittyen.

Kolmen kasvotusten suoritetun haastattelun vastauksissa oli paljon samoja teemoja erilaisilla yksityiskohdilla. Päällimmäinen samankaltaisuus tuli etätöihin siirtymisestä; ohjeistus oli erittäin vähäistä. Kaikilla haastateltavilla oli ollut jonkinlaisia yleisiä tietoturvakoulutuksia ja työnantajan puolelta tuli säännöt salasanoille sekä päivityksille. Kaikilla haastateltavilla oli huomattavissa hieman epävarmuutta tietoturva-asioissa, mutta kaikki tiesivät mistä saavat apua tarvittaessa.

Haastatteluista ja verkkokyselystä nousi samankaltaisia aihealueita esille. Suurin yhtenäisyys on etätyö siirtymän ohjeistuksen vähäisyydessä. Ohjeistus on ollut

yleisesti pintapuolista tai olematonta. Tästä huolimatta suurin osa (77,3 %) verkkokyselyn vastaajista koki nämä vähäiset ohjeet silti riittäviksi. Vastavuoroisesti haastateltavista kukaan ei kokenut ohjeiden olevan riittäviä. Ylipäätään haastateltavat kokivat olevansa hieman arempia tietoturvaosaamisestaan kuin verkkokyselyn vastaajat. Muita yhtä suuria eroavaisuuksia ei haastattelujen ja kyselyn vastausten väliltä löydetty.

## 6.2 Tuloksista löytyviä tietoturvaongelmia

Tutkimuksen yhteydessä löytyi useita tietoturvaongelmia. Nämä olivat pääasiallisesti työntekijälähtöisiä, osa tahallisia ja osa tahattomia. Tietoturvaan pätee hyvin sanonta ”tietoturva on yhtä vahva kuin sen heikoin lenkki” (Väisänen 2019).

Osa vastaajista toimi tietoisesti vastoin saamiaan ohjeita, sillä tämä oli helpompaa työntekijän näkökulmasta. Hyvänä esimerkkinä tästä on työsähköpostin käyttäminen vapaa-ajan asioihin ja liian kevyet suojaukset työssä käytettävissä laitteissa. Tämä varmasti osakseen johtuu hieman harhaanjohtavasta turvallisuuden tunteesta, sillä tietomurtoa pidetään jopa liiankin epätodennäköisenä kuten kuvio 19 osoittaa.

Lisäksi tietoturvakoulutuksen taso vaikutti olevan liian alhainen varsinkin etätöihin siirryttäessä. Tästä saattaa seurata se, että useat työntekijät käyttävät liian helppoja ja samoja salasanoja useissa eri paikoissa, eivätkä vaihda näitä tarpeeksi usein. Verkkokyselyyn vastanneista 20 % ei vaihda salasanaansa koskaan (luku 5.2). Myös laitteiden fyysisen turvallisuuden puutteet tulivat ilmi: mikäli laite sisältää arkaluontoista dataa, tulisi se suojata muullakin kuin yksinkertaisella salasanalla.

Suurin osa vastaajista piti tietoturvamurtoa hyvin pelottavana ajatuksen tasolla. Tätä tukee myös Traficomin suorittama tutkimus vuodelta 2020, missä todettiin tietoturvaan liittyvien uhkakuvien yleistyneen voimakkaasti vuodesta 2019 (Traficom 2020d). Kuviossa 20 nähdään kyseisen tutkimuksen tuloksia.

Vaikka vastaajat kokivat kuvitteellisen tietoturvamurron pelottavana, eivät he pitäneet tietoturvamurtoa todellisuudessa kuitenkaan kovin todennäköisenä omalla kohdallaan. Yllättävää oli myös se, että suurin osa vastanneista ei kokenut etätyön olevan riskialttiimpaa kuin lähityö tietoturvan kannalta. Tulokset viittaavat siihen, että vaikka tietoturvaan liittyvät uhat ovat pelottavia ja ne ovat paljon esillä, ei tietämys niistä ole tarpeeksi korkealla tasolla. Tästä seuraa se, että tietoturvaan liittyviä uhkia ei osata ottaa aidosti vakavasti ja uskota sen mahdollisuudesta omalle kohdalle.


KUVIO 20. ”Kaikki kartoitetut tietoturvaan liittyvät uhkakuvat ovat yleistyneet voimakkaasti vuoden 2019 keväästä” (Traficom 2020d)

Useat vastaajat toivat esiin omaa epävarmuuttaan tietoturvaan liittyvissä asioissa, mutta toisaalta toivat esille löytyvän myös heitä vähemmän osaavia, vanhemman sukupolven työntekijöitä. Myös kouluttamisen kohdalla pohdittiin sitä, että vanhempien työntekijöiden omaksumiskyvyn vuoksi on koulutuksen taso pidettävä matalalla. Vastaajat toivat siis selvästi esiin vastauksissaan iän vaikutuksen tietoturva-asioihin. Iän selvittäminen vastaajilta osana kyselyä olisi voinut tuoda yhden hyvän näkökulman lisää tutkimukseen.

Tietoturvaan ja tietotekniikkaan liittyvissä asioissa saattoi havaita myös osaamattomuuteen liittyvää häpeää. Osa vastaajista ei esimerkiksi halunnut vastata kaikkiin salasanaa koskeviin kysymyksiin, mikä voi johtua myös häpeästä salasanoihin liittyen. Vastaajilla tuntui olevan kuva siitä, miten tulisi toimia, mutta käytännön toimet saattoivat kuitenkin erota näistä tavoitteista, mikä osaltaan voi lisätä häpeää vastata omien tapojen olevan vastoin säännöksiä ja ohjeita.

Osaamiseen ja tietoturvaan liittyen olisikin tärkeää, että työntekijöillä on saatavilla apua, joista he uskaltavat kysyä apua kaikissa heitä askarruttavissa asioissa. Avun pyytäminen voi vähentyä ”tyhmien kysymysten” pelossa tai häpeässä kysyä samaa asiaa uudelleen, kun se on jo neuvottu aikaisemmin. Ilmapiiri ja rohkeudenpuute voi tällöin osaltaan lisätä tietoturvaongelmia.

Useassa yrityksessä on järjestetty jonkinlaisia tietoturvakoulutuksia, ja tuloksien mukaan tietoturvakoulutukseen osallistuneet kokivat saaneensa tarpeeksi koulutusta (kuvio 4). Nämä koulutukset eivät kuitenkaan välttämättä ota huomioon työntekijöiden tieto- ja taitotasoa, vaan käyvät samat asiat läpi jokaiselle. Osalle tietotekniset asiat eivät ole yhtä helppoja kuin toisille ja joillekin tietoturva-asioiden omaksuminen vaatii huomattavasti enemmän aikaa. Työntekijöiden lähtötaidot ja -tiedot tulisi huomioida myös kouluttamisessa ja sitä voisi hyödyntää esimerkiksi kollegoiden välisen neuvomisen muodossa (esimerkiksi digituutorit). Moni työntekijöistä onkin varmasti hyötynyt koulutuksista, mutta osalle nämä ovat saattaneet olla työajan tuhlausta sekä yritykselle siten turha rahallinen ja ajallinen menoerä.

### 6.3 Parannusehdotuksia ongelmille

Yksinkertaisin ratkaisu tietoturvaongelmiin on lisätä tietoturvakoulutuksia sekä kiinnittää huomiota niiden suunnitteluun (kohdeyleisö) ja laatuun. Koulutuksia tulisi pyrkiä räätälöimään sopiviksi eri aloille ja eri työntekijöille siten, että kaikki oppisivat tarpeelliset asiat. Tietoturvapuolen asioihin voisi myös tulevaisuudessa liittää jonkin sortin meriitin. Esimerkiksi Ruokaviraston vuonna 2006 tuoma hygieniapassi tuli elintarvikelain muutoksen seurauksena, takaamaan ruuan turvallista

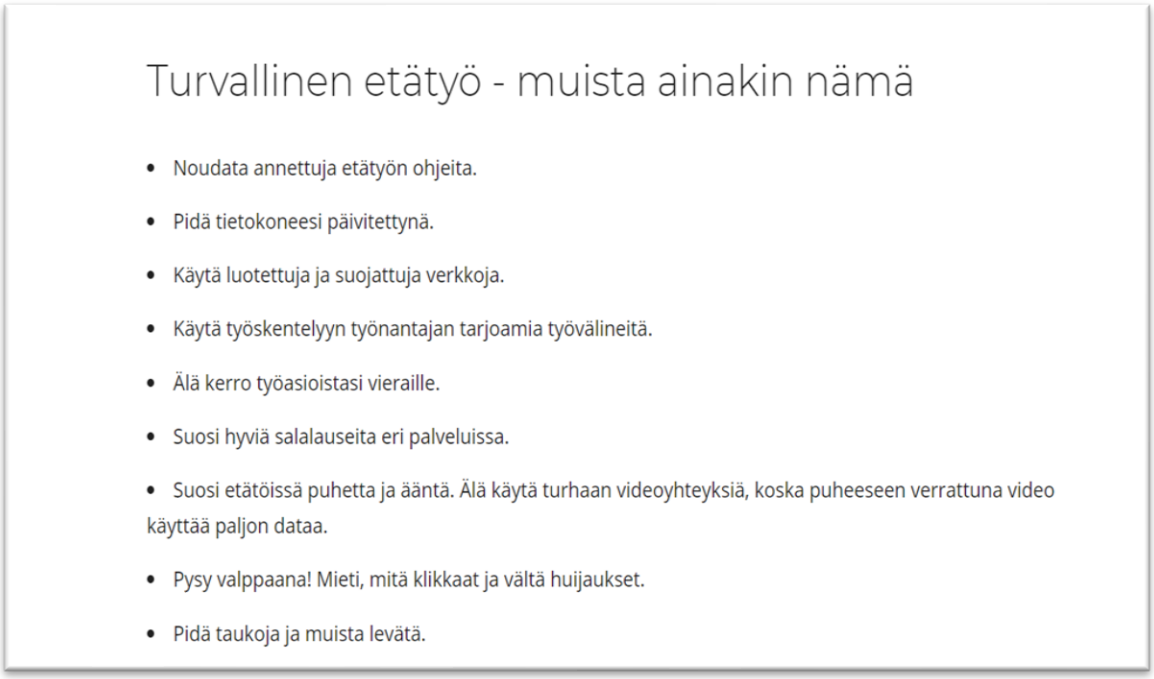
käsittelyä. Samalla idealla voitaisiin rakentaa vastaavanlainen tietoturvapassi takaamaan tietoteknisten asioiden (varsinkin arkaluontoisten) turvallisen käsittelyn. Passissa voisi olla eri tason arvoja, jotka kuvastaisivat oman koulutuksen tasoa tietoturvaan liittyvissä asioissa siten, että esimerkiksi arkaluontoisen tiedon käsittelyyn vaadittaisiin myös korkeamman arvon tasoista ja voimassa olevaa tietoturvapassia.

Toisena hyvänä vaihtoehtona olisi lisätä ulkoisten tahojen testausta yritysten tietoturvasta (penetraatiotestaus) ja tarpeen tullen tuoda löydetyt ongelmat ilmi, sekä kouluttaa ongelmien paikkaamisessa. Suosittelisimme testaukseen ulkopuolista, tähän erikoistunutta ja kouluttunutta tahoa kahdesta syystä. Ensimmäiseksi, tällainen koulutetun tahon käyttäminen takaisi sen, että testaus olisi tarpeeksi monipuolista ja osaavaa. Toiseksi jo yksityishenkilöiden vastauksista käy ilmi, miten he toimivat tietoisesti ohjeistuksia rikkoen. Ulkopuolisen tahon käyttäminen voisi osaltaan olla varmistamassa sitä, etteivät työnantajatahot pääsisi lipsumaan vähemmän tärkeinä pitämissään tietoturvaseikoissa, vaikka tietäisivät, kuinka tulisi toimia.

Lisäksi yritykset voisivat estää liian lyhyiden ja helppojen salasanojen käytön. Salasanat voitaisiin myös ajastaa vanhentumaan tietyin väliajoin (esimerkiksi kahden kuukauden välein), jotta salasana tulisi vaihdettua tarpeeksi usein. Tämä onkin monessa yrityksessä jo arkipäivää, mutta kyselyn perusteella on myös työntekijöitä, jotka eivät vaihda salasanojaan koskaan. Salasanojen hallintaohjelmat voivat olla hyvä tapa helpottaa työntekijöiden salasanojen muistamisongelmia ja mahdollistaa monimutkaisemmat sekä useammin vaihtuvat salasanat. Tällaisten ohjelmien käyttö vähentäisi myös IT-apuun kohdistuvia salasanaunohduksista johtuvia yhteydenottoja. Mikäli työssä käsitellään arkaluontoista materiaalia, olisi myös tarpeen lisätä monitasoinen autentikointi esimerkiksi puhelinsovelluksella, erillisellä autentikointikortilla tai biometrisillä tunnistautumisilla.

Lisäksi Liikenne- ja viestintävirasto Traficom (2021) on antanut selkeän ja helppoymmärteisen tietoturvaohjeistuksen kaikille etätyötä tekeville (kuva 1). Tämä ohjeistus on tarkoitettu työntekijöille selkeyttämään etätyön arkea. Nämä ohjeet

voivat olla tuttuja monelle teoriassa, mutta käytännössä niitä ei välttämättä seurata. Montaa ohjeistuksen seikkaa voi hyvin soveltaa myös työn ulkopuolelle, päivittäiseen tietoturvaosaamiseen.




KUVA 1. Ohjeita turvalliseen etätyöhön (Traficom, 2021)

### 6.4 Jatkokehittäminen

Tutkimuksemme käsittelee useaa tietoturvaan liittyvää osa-aluetta, mutta pintapuolisesti. Työ mahdollistaa jatkokehittämisen syvemmälle valitusta aiheesta. Jatkokehittäjän tulee kuitenkin ottaa huomioon otannan pienuus ja tämän mahdollinen vaikutus jatkotutkimukseen. Lisäksi mikäli tulevaisuudessa parannusehdotuksia otettaisiin käyttöön, voitaisiin niiden vaikutusta tietoturvan tasoon tutkia. Erityisen hyödyllinen tutkimus olisi kokeilla tietoturvapassin toteutusta ja sen pitkäaikaista vaikutusta tietoturvan tasoon.

Tutkimuksen tuloksista ja teemoista voi löytyä monta muutakin aihetta mitä voisi tarkemmalla tutkimuksella selvittää. Tämän työn puitteissa lähempi tarkastelu ei ollut mahdollista. Voisi olla esimerkiksi hyödyllistä selvittää eroavatko tietoturvakoulutuksien sisältö tai laatu aloittain merkittävästi tai vaikuttaako tähän kenties arkaluontoisen datan käsittely ja miten.

# 7 POHDINTA

Pohjasimme tutkimuksemme hypoteesiin siitä, että työntekijät ovat itse omalla toiminnallaan suurin tietoturvariski etätyöskentelyssä. Saamamme tutkimustulokset tukevat hypoteesimme olevan oikea.

Opinnäytetyön aiheemme oli hyvin laaja ja aiheen rajaaminen tuotti useita ongelmia, sillä tietoturva on käsitteenä monitahoinen. Monia tietoturvan osa-alueita olisi ollut mielenkiintoista tutkia laajemmin, mutta aihe tuli rajata opinnäytetyöhön sopivaksi. Osaltaan tämä helpotti aiheen rajaamista, mutta samalla esti meitä tutkimasta asioita liian syvällisesti.

Toisena haasteena oli riittävän otannan hankkiminen. Kyselylomakkeen jakaminen oli aluksi haastavaa, sillä halusimme mahdollisimman ison otannan, mutta samalla halusimme rajata kyselyyn vastaajat etätyöntekijöiksi, mikä poisti etäopiskelijat kohdejoukosta. Halusimme myös otantaamme useiden eri alojen työntekijöitä, mikä haastoi osaltaan sopivien vastaajien löytymistä.

Työmme onnistuu kuvaamaan etätyöhön liittyviä osa-alueita ja nostamaan esiin etätyöhön liittyviä ongelmakohtia. Työntekijöiden omaan toimintaa liittyvät ongelmat ovat osaltaan heistä riippuvia ja osaltaan heistä riippumattomia. Selkein työntekijöistä riippuva ongelmakohta on se, etteivät työntekijät toimi saamiensa ohjeiden mukaan. Työntekijät tuntuivat luistavan tietoturvaan liittyvistä ohjeistuksista, vaikka tiesivät toimivansa ohjeistusten vastaisesti.

Työntekijöistä itsestään riippumattomat tietoturvaa heikentävät asiat liittyvät puolestaan työnantajaan. Työnantajasta riippuviin ongelmiin nostaisimme kouluttamisen ja perehdyttämisen. Pandemia aiheutti poikkeuksellisen nopean ja suunnittelemattoman siirtymän etätyöhön, minkä vuoksi myös ohjeistuksissa ja koulutuksissa on puutteita etätyömäärään nähden. Vastaajat, jotka eivät olleet saaneet koulutusta tunsivat myös, etteivät ole saaneet tarpeeksi ohjeistusta työskentelyyn. Näemmekin tärkeäksi, että nopean aikataulun siirtymästä johtuvia koulutuspuutteita paikattaisiin myös nyt jälkikäteen. Kun työntekijät ovat varmasti vuoden aikana oppineet tekemään työtään myös etänä, tulisi työn sujuessa kiinnittää

huomioita myös tietoturvallisuuteen kertaavien ja täydentävien koulutusten ja ohjeistusten avulla.

Pyrimme työmme avulla korostamaan myös tietoturvan tärkeyttä. Kyselyidemme perusteella tietoturvamurrot tuntuivat vastaajista pelottavilta, mutta he eivät nähneet niiden tapahtumista todennäköisenä omalle kohdalleen. Vastaajat nostivat vastauksissaan esiin esimerkiksi Vastaamo -tapauksen, joten myös vastaajat tuntuivat ymmärtävän tietomurtojen vakavuuden. Toivommekin, että työmme saa kyselyyn vastaajia sekä työhön tutustuvia etätyöntekijöitä pohtimaan myös omaa etätyökäyttäytymistään tietoturvan näkökulmasta ja ehkä jopa muuttamaan joitakin käytäntöjään tietoturvallisempaan suuntaan.

Aloitimme opinnäytetyön tekemisen joulukuussa 2020 aiheen tutkimisella ja rajaamisella. Aiheeseen syvemmin tutustuessamme saimme myös rajattua osa-alueita selkeäksi kokonaisuudeksi. Pysyimme asettamassamme aikataulussa ja saimme palautettua opinnäytetyön ajoissa. Koemme saavuttaneemme opinnäytetyölle asetetut tavoitteet.

**LÄHTEET**

Helsingin yliopisto. N.d. Opiskelijan digitaidot. Tietoturvan periaatteet. Luettu 25.2.2021
https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset/

Järvinen, P. 2012. Arjen tietoturva. Jyväskylä: Saarjärven Offset Oy.

Laakso, M. N.d. Tietoturvan osa-alueet. Luettu 8.3.2021
https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvan-osa-alueet

Liikenne- ja viestintävirasto Traficom. 2021. Etätyön tietoturva- ohjeita työntekijöille. Luettu 10.4.2021
https://www.kyberturvallisuuskeskus.fi/fi/etatyon-tietoturva-ohjeita-tyontekijoille

Liikenne- ja viestintävirasto Traficom. 2020a. Office 365 -tietomurrot kasvussa – suojaudu, havaitse, tiedota! Luettu 15.3.2021
https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/office-365-tietomurrot-kasvussa-suojaudu-havaitse-tiedota

Liikenne- ja viestintävirasto Traficom. 2020b. Tietosuoja Traficomissa. Luettu 25.3.2021.
https://www.traficom.fi/fi/traficom/tietosuoja-traficomissa

Liikenne- ja viestintävirasto Traficom. 2020c. Tietoturva. Luettu 22.2.2021
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Liikenne- ja viestintävirasto Traficom. 2020d. Yhä useampi on huolissaan lähipiiriinsä kohdistuvista tietoturvauhkista. Luettu 20.3.2021
https://www.traficom.fi/fi/ajankohtaista/yha-useampi-huolissaan-lahipiiriinsa-kohdistuvista-tietoturvauhkista

Tietosuojavaltuutetun toimisto. 2018. GDPR. Luettu 18.4.2021
https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. N.d Tietosuoja. Luettu 20.3.2021
https://tietosuoja.fi/tietosuoja

Yle. 2021. Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: "Emme tiedä, monenko käsissä tietokanta on". Luettu 17.4.2021
https://yle.fi/uutiset/3-11757676

Yle. 2020. Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Tor-verkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa. Luettu 17.4.2021
https://yle.fi/uutiset/3-11612399

Väisänen, M 2019. Tietoturva, kumiseva käsite vai hallinnassa oleva suoja-portti? Luettu 10.4.2021
https://www.neuvonenpalvelut.fi/tietoturva_kumiseva_kasite_vai_suojaportti/

**LIITTEET**

Liite 1. Verkkokyselyn saateteksti

Tällä kyselyllä kerätään taustatietoa TAMKissa toteutettavaan “Etätyöskentelyn tietoturva” opinnäytetyötä varten. Vastaamiseen kuluu alle vartti. Tähän kyselyyn vastaaminen ei sido mihinkään ja se toteutetaan täysin nimettömänä. Kaikki vastaukset käytetään vain tämän opinnäytetyön toteuttamiseen.

Opinnäytetyön ideana on tutkia työntekijöiden käyttäytymistä ja mieltymystä etätyöhön liittyen. Näiden vastausten (ja meidän omien etäopiskelukokemusten) perusteella, etsitään mahdollisia puutteita, uhkia ja kehityskohtia etätyön tietoturvaan liittyen.  Tarkoituksena olisi lopulta esittää suosituksia ja ehdotuksia näiden kohtien paikkaamiseen.

Koska kysely toteutetaan nimettömänä olisi toivottavaa, että vastaisit mahdollisimman rehellisesti kysymyksiin. Näin kyselystä saadaan todellista dataa ja pystytään tekemään oikeita johtopäätöksiä.

Kyselyssä on 24 kysymystä.

Kiitos vastauksista jo etukäteen!

Taavi Pelkonen & Kristian Rintala