jamk

Tietoturvallinen etätyö

Case: Qvantel Finland Oy

Ville Veijanen

Opinnäytetyö, AMK
Toukokuu 2022
Tietojenkäsittely ja tietoliikenne
Insinööri (AMK), Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Veijanen Ville

Tietoturvallinen etätyö

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2022**,** 51 sivua.

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: Suomi

Verkkojulkaisulupa myönnetty: Kyllä

Tiivistelmä

Etätyöt yleistyivät nopeasti keväällä 2020 maailmalla alkaneen koronapandemian seurauksena. Nopean etätöihin siirtymisen takia työntekijöiden kouluttaminen etätyöhön oli jäänyt vähäiseksi. Opinnäytetyössä kartoitettiin etätöitä tekevien työntekijöiden tietoturvaosaamisen tasoa, etätyöstä aiheutuvia tietoturvariskejä sekä luomaan ratkaisuja niiden korjaamiseksi.

Tietoperustassa käsiteltiin CIA-mallia, valtiohallinnon tietoturvaratkaisuja sekä yleisiä työympäristöön liittyviä tietoturvariskejä. Haastattelukysymykset luotiin Qvantelin etätyöohjeistuksen ja yleisen tietosuoja-asetuksen määräysten perusteella.

Tutkimusaineiston keruumenetelminä on käytetty verkkokyselyä sekä haastatteluita. Tutkimustulosten perusteella tietoturvaosaamisen taso on ollut heikkoa osalla työntekijöistä, sillä työnantajat eivät ole tarjonneet tarpeeksi koulutusta tai ohjeistusta tietoturvalliseen etätyöskentelyyn. Useat etätöitä tekevät työntekijät olivat luoneet tietoturvariskejä huolimattomuudestaan tai jopa piittaamattomuudestaan.

Valtaosa tutkimuksessa löydetyistä tietoturvaongelmista on työntekijälähtöisiä, mutta ne pystyttäisiin ratkaisemaan työnantajan toimesta lisäämällä tietoturva- ja tietosuojakoulutusta työntekijöille. Tietosuojaosaamisen tasoa tulisi myös testata ja varmentaa niiltä työntekijöiltä, jotka käsittelevät työssään henkilötietoja tai muita arkaluonteisia tietoja.

Avainsanat (asiasanat)

Tietoturva, etätyö, GDPR

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Veijanen Ville

Secure teleworking

Jyväskylä: JAMK University of Applied Sciences, March 2022, 51 pages.

Engineering and technology. Degree Programme in Information and Communications Technology. Bachelor´s thesis.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

As a result of the global pandemic that began in the spring of 2020, many people switched to telecommuting on a very fast schedule. There was little time to plan for the transition and some employees had little or no experience of working remotely. Thesis mapped the level of information security competence of teleworkers, the information security risks arising from teleworking and to create solutions to fix them.

The knowledge base covered the CIA-model, government security solutions, and a general work-related security risks. Interview and online survey questions were based on Qvantel's telework instructions and general data protection regulation.

An online survey and interviews have been used as methods for collecting research material. The level of information security skills has been poor for some employees, as employers have not provided enough training or guidance on safe teleworking. Several employees had also created security risks while working remotely due to their carelessness and negligence.

Most of the information security problems found in the study are employee-driven, but the employer could reduce them with security trainings. The level of data protection expertise should also be tested and verified from those employees who process personal data or other sensitive information in the course of their work.

Keywords/tags (subjects)

Information security, remote work, GDPR

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

Etätyöskentely on yleistynyt koronapandemian vuoksi maailmanlaajuisesti. Vaikka pandemiarajoitukset ovat vähentyneet, on etätyöskentely koettu tehokkaaksi työskentelymalliksi sekä työntekijän että työnantajan näkökulmasta. Vauhdikas siirtyminen lähityöstä etätyöhön loi uusia tietoturvahaasteita sekä työntekijöille että organisaatioille. Tämä opinnäytetyö pyrkii nostamaan esiin tietoturvan tärkeyttä selvittämällä etätyöskentelyn aiheuttamia tietoturvaongelmia ja luomaan niihin ratkaisuja.

Työ toteutetaan yritykselle Qvantel Finland Oy, jossa työskentelen tuki-insinöörinä. Qvantel on pilvipohjaisiin liiketoiminnan tukijärjestelmiin erikoistunut ohjelmistotalo, jolla on toimipisteitä kahdeksassa maassa ja noin 700 työntekijää. Jokainen Qvantel Finlandin työntekijä on työskennellyt etänä koronapandemian alettua, mutta useat myös ennen sitä. Tavoitteena on luoda tietoturvallisia ratkaisuja etätyöhön, jota kohdeyritys voi hyödyntää.

Työn empiirinen osa on toteutettu kvalitatiivisena, eli laadullisena tutkimuksena. Työssäni pyritään vastaamaan seuraaviin kysymyksiin:

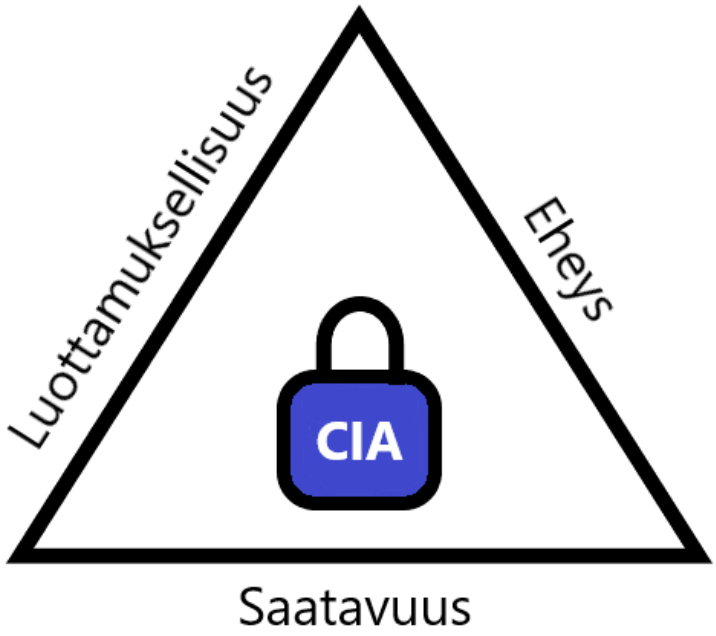
1. Kuinka hyvin tietoturva- ja tietosuojavaatimukset ovat hallussa etätöitä tekevillä työntekijöillä?
2. Millaisia tietoturvauhkia etätyöt aiheuttavat?
3. Miten näitä uhkia voidaan ehkäistä?

Tutkimusaineiston keruumenetelminä on käytetty havainnointia, verkkokyselyä sekä puolistrukturoitua haastattelua. Verkkokyselyn mukana toimitettiin saateteksti (ks. Liite 1.), jossa korostettiin kyselyn tärkeyttä ja vastausten luottamuksellisuutta.

2 Tietoturva

2.1 CIA-kolmikko

CIA-kolmikko (engl. *CIA-triad*) kuvaa tietoturvan kolmea peruspilaria. Nämä ovat tiedon luottamuksellisuutta (engl. *confidentality*), eheyttä (engl. *integrity*) ja saatavuutta (engl. *availability*). Näillä osa-alueilla on ratkaiseva rooli kyberturvallisuudessa, sillä niiden avulla voidaan jäljittää kyberhyökkäyksiä aivan alusta alkaen ja siten löytää käytetyt hyökkäysvektorit. Tämä taas antaa mahdollisuuden kehittää turvatoimia, jotta mitään vastaavaa ei pääsisi tapahtumaan. (Allen 2021.)



Kuvio 1. CIA-kolmikko (mukaillen Allen 2021.)

2.1.1 Luottamuksellisuus

Luottamuksellisuus on sitä, kun tiedot ovat vain niiden käyttöön oikeutettujen saatavilla. (Kyberturvallisuuskeskus 2020a). Luottamuksellisista tiedoista ilmenee esimerkiksi henkilön:

- Ammattiliiton jäsenyys
- Poliittiset mielipiteet
- Terveystiedot
- Seksuaalinen suuntautuminen tai käyttäytyminen
- Geneettisiä ja biometrisia tietoja henkilön tunnistamista varten
- Etninen alkuperä tai rotu
- Uskonnollinen tai filosofinen vakaumus
- Palkka
- Henkilötunnus

(Tietosuoja n.d.)

2.1.2 Eheys

Eheys tarkoittaa sitä, että vain tietojen muuttamiseen oikeutetut voivat niitä muuttaa tai poistaa. (Kyberturvallisuuskeskus 2020a). Eheyden kriteerit täyttyvät, kun suojattavat tiedot ovat aitoja, vääristymättömiä ja luotettavia säilytettäväksi. (Allen 2021).

2.1.3 Saatavuus

Saatavuus tai käytettävyys on sitä, että tiedot ja tietojärjestelmät ovat helposti niiden käyttöön oikeutettujen hyödynnettävissä. (Kyberturvakeskus 2020). Tämä edellyttää laitteiston, teknisen infrastruktuurin ja järjestelmien asianmukaista ylläpitoa, jotka säilyttävät ja näyttävät tietoja valtuutetuille henkilöille. (Allen 2021).

Saatavuus on haavoittuvin CIA-kolmikon osa-alueista, jos sitä ei ylläpidetä huolellisesti. Hyökkäysvektoreita voi syntyä esimerkiksi päivittämättömien järjestelmien käyttämisestä, käyttäjähakemiston ongelmista tai yksityisen verkon väärinkäytöstä. (Allen 2021.)

2.1.4 AAA-malli

Jotta käyttäjän rooli saataisiin otettua paremmin huomioon tietoturvassa, voidaan CIA-mallia täydentää myös AAA-mallilla. Tämä malli pitää sisällään todennuksen (engl. *authentication*), valtuutuksen (engl. *authorization*) ja tilastoinnin (engl. *accounting*). Todennuksella tarkoitetaan keinoa tunnistaa käyttöoikeuden omaava käyttäjä esimerkiksi käyttäjätunnuksen ja salasanan avulla. Valtuuttaminen on oikeiden käyttöoikeuksien antaminen oikeille käyttäjille. Tilastointi pitää sisällään käyttäjien tapahtumien ja resurssienkäytön valvomista ja kirjaamista. CIA-mallia täydennetään AAA-mallilla erityisesti verkkopalveluiden pääsynhallinnassa. (Päivärinta 2020.)

2.2 Tietoturva ja tietosuoja etätyössä

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) jakaa tietoturvaratkaisut seuraaviin osa-alueisiin:

OSA-ALUE	**SELITYS**
Hallinnollinen turvallisuus	Tietoturvan suunnittelu ja toteutus, tietojärjestelmien etäkäytön valvominen, etäkäyttäjän ohjeistaminen
Henkilöstöturvallisuus	Sijaisjärjestelyn varmentaminen
Fyysinen turvallisuus	Laitteiden ja toimitilojen fyysinen suojaaminen
Tietoliikenneturvallisuus	Etäyhteyden valvonta ja hallinta
Laitteistoturvallisuus	Laitteiden rekisteröinti, toiminta ja huolto
Ohjelmistoturvallisuus	Etäkäyttäjän ja etäylläpidon ohjelmistojen suojaaminen
Tietoaineistoturvallisuus	Sähköisen ja fyysisen aineiston suojaaminen ja käsittely
Käyttöturvallisuus	Etäkäyttäjän tunnistaminen, rajoitus ja seuranta

Taulukko 1. Tietoturvaratkaisut (VAHTI 2002, luku 3.)

Tietoturva ja tietosuoja ovat haasteena varsinkin, kun työskennellään julkisissa tiloissa tai kulkuneuvoissa. Läheisyydessä voi olla ihmisiä, jotka voivat nähdä käyttäjän laitteen ruudulle tai olla kuuloetäisyydellä puheluihin. Työntekijöiden, asiakkaiden ja yhteistyökumppaneiden henkilötiedot sekä yrityksen liiketoimintaan liittyvät tiedot voivat helposti vuotaa ulkopuoliseen tietoon huolimattoman toiminnan kautta. Laitteet saattavat myös jäädä valvomatta esimerkiksi vessassa käydessä tai käyttäjän nukahtaessa. (Lindberg 2022.)

Teknisestä tietoturvallisuudesta on aina huolehdittava, kun laitteita käytetään työssä. Laitteille tulee olla asennettuna ja päivitettynä aktiivinen virustorjuntaohjelma. On myös syytä kirjautua laitteelta ulos, kun laitetta ei käytetä. Laitteelle kirjautuessa tulisi myös käyttää monivaiheista todentamista. Yhteyksien osalta on huomioitava, että käytettäisiin salattua liikennettä niin kotona kun matkalla. (Lindberg 2022.)

3 Etätyö

Etätyöksi katsotaan vapaaehtoisuuteen ja sovittuihin sääntöihin perustuvaa joustavaa ansiotyötä, joka voi tapahtua myös fyysisen työpaikan ulkopuolella. Ajasta ja paikasta riippumattomat työjärjestelyt ovat olennaista etätyössä. Etätyö voi olla joko kokoaikaista tai osittaista, eli hybridityötä. (Työsuojelu 2020.)

3.1 Etätyö Suomessa

Koronapandemian alettua keväällä 2020 lähes 60 prosenttia suomalaisista päätyi tekemään etätöitä. (Eurofound 2020, 5). Duunitorin kävijädatan perusteella myös selviää, että etätöitä etsittiin noin 360 000 kertaa vuonna 2019. Vuonna 2020 etätöitä etsittiin n. 670 000 kertaa ja vuonna 2021 etätöitä etsittiin 1 240 000 kertaa. (Salonen 2022.)

Vaikka valtakunnallinen etätyösuositus on päättynyt, jää työnantajan päätettäväksi sallia tai velvoittaa työntekijöitä palaamaan työpaikalle. (Sosiaali- ja terveysministeriö 2022). Etätyöskentelyn määrä voi siis vähentyä Suomessa, mutta hybridityö on saapunut jäädäkseen. (Multisilta 2021.)

3.2 Etätyön hyödyt ja haitat

Etätyöskentely tarjoaa työntekijälle ja työnantajalle monia erilaisia mahdollisuuksia, mutta myös haasteista. Etätyön hyödyt ja haitat riippuvat pitkälti millaisesta organisaatiosta, työstä, liiketoiminnasta ja tehtävistä on kyse. Onnistuneen etätyön edellytys on, että johtaminen ja työkulttuuri perustuvat luottamukseen kontrolloinnin sijasta. (Työterveyslaitos n.d.)

Etätyökokemuksiin vaikuttaa henkilöiden yksilölliset erot. Näitä ovat muun muassa persoonallisuus, työkokemus, työolot ja perhetilanne. Monet uskovat, että etätyö lisää heidän hyvinvointiaan, mutta jotkut saattavat tuntea olonsa eristäytyneeksi ja tylsistyneeksi. Siksi on tärkeää tiedostaa etätyön riskit ja oppia välttämään niitä. (Työterveyslaitos n.d.)

Työterveyslaitoksen ammattilaisten näkemys etätöiden hyödyistä ja haitoista niin työntekijälle kuin työnantajalle. (ks. Taulukko 2)

	Työntekijä	Työnantaja
Hyödyt	- Työajan joustavuus ja rytmittäminen oman arjen ympärille - Lisääntynyt keskittyminen ja työrauha - Työtehon ja työtyytyväisyyden paraneminen - Ajan ja rahan säästöt työmatkoissa - Perhe-elämän ja työn joustavampi yhteen sovittaminen - Mahdollisuus asua eri paikkakunnalla - Osatyökykyisten Mahdollisuus osallistua työelämään - työn tekeminen poikkeustilanteissa	- Työn tuottavuudeen ja työtehon paraneminen - Työuran piteneminen paremman jaksamisen takia - Pienemmät kustannukset toimitiloille - Rekrytointivaltti - Parantaa työnantajan ympäristövastuullisuutta
Haitat	- Työajan venyminen - Työ ja vapaa-ajan sekoittuminen - Vaikeudet irroittua työstä ja liiallinen kuormittuminen - Sopimattomat tilat ja kalusteet etätyöhön - Yksinäisyyden ja eristyneisyyden tunne - Riittämätön esihenkilön tai työkaverin tuki - Huoli urakehityksestä	- Etäjohtaminen ja työn hallitseminen - Työntekijöiden tietoturvariskit

Taulukko 2. Etätyön hyödyt ja haitat. (Työterveyslaitos n.d.)

4 Tutkimussuunnitelma

4.1 Tutkimuksen tavoitteet

Tutkimuksen tavoitteena on kartoittaa etätyötä tekevien henkilöiden tietoturvaosaamisen tasoa, löytää niistä mahdollisia puutteita ja luoda ratkaisuja niiden korjaamiseksi. Tarkastelu toteutetaan pääasiallisesti työntekijän näkökulmasta.

Tutkimuksessa pyritään myös selvittämään työnantajan antamaa tietoturvaperehdytystä etätöihin liittyen sekä työntekijöiden näkemystä siitä, onko se ollut riittävää. Lisätavoitteena pyritään nostamaan esiin tietoturvan tärkeyttä etätyössä.

4.2 Tutkimusongelmat

Etätyöskentelyn tietoturvaongelmat voivat johtua esimerkiksi työntekijästä, työnantajasta, laitteistosta, työympäristöstä tai koulutuksesta. Syitä tietoturvariskeille voi olla henkilön välinpitämättömyys, osaamattomuus tai huolimattomuus tietoturvassa. Kaikkia edellä mainittuja osa-alueita käsitellään tutkimuksessa.

Tutkimus toimii hyvänä jatkotutkimuksen tai -kehityksen kohteena antaessaan hyvää pohjatietoa etätyön tietoturvariskeistä. Opinnäytetyön jatkokehittämistä on kuvailtu tarkemmin luvussa 8.2 Jatkokehittäminen.

4.3 Tutkimusmenetelmät

Tutkimuksen aineistonkeruussa hyödynnettiin sekä verkkokyselyä että puolistrukturoitua, eli teemahaastattelua. Haastattelun kysymykset perustuivat verkkokyselyn kysymyksiin (luku 5.2), mutta kysymysten sanamuodot ja järjestykset muuttuivat haastatteluissa. Verkkokyselyn käyttö osana aineistonkeruuta mahdollisti laajemman otannan, sillä haastatteluja oli vain kolme.

5 Tutkimuksen toteuttaminen

5.1 Haastattelu

Haastattelun ja verkkokyselyn ensimmäisessä kysymyksessä selvitettiin henkilön työalaa, sillä se on tärkeässä osassa tutkimusta. Haastateltaville ja verkkokyselyyn vastaajille annettiin mahdollisuus kertoa työalansa, mutta tämä ei ollut pakollista. Verkkokyselyn täyttämiseen kului aikaa noin 10 minuuttia ja haastattelut ilmoitettiin kestävän noin 30 minuuttia. Haastatteluiden pituus oli kuitenkin vain suuntaa antava ja tämän vuoksi haastatteluihin kului aikaa 20–90 minuutin välillä.

5.2 Haastattelun sisältö

Henkilöhaastattelut sekä verkkokysely koostuvat pääosin samoista kysymyksistä. Osa kysymyksistä on luotu kohdeyrityksen etätyöohjeistuksen perusteella. Vastausten perusteella kysymyksiä oli 32–36 kappaletta. Verkkokyselyssä oli pakollista vastata kaikkiin kysymyksiin tai muuten kyselyä ei voinut palauttaa.

5.2.1 Osio 1 – Etätyöskentely

Ensimmäinen osio on tärkeänä osana kyselyä ja se koostuu kolmesta kysymyksestä. Tämä osio on vastaajien profilointia varten. Ensimmäiseen kysymykseen pystyi vastaamaan valmiiksi annetuilla työaloilla tai kirjoittamalla oman alan vapaasti. Kysymyksessä 2 haastateltavalta varmistettiin, onko hän työskennellyt etänä. Mikäli vastaus oli kielteinen, sulkeutui kysely hänen osaltaan. Kysymyksellä 3 haettiin sitä, kuinka suuri osa verkkokyselyn vastaajista oli työskennellyt etänä ennen koronapandemiaa vai vasta sen alettua.

1. Työalani on:
2. Työskenteletkö, tai oletko työskennellyt etänä?
3. Työskentelitkö etänä ennen koronapandemiaa vai vasta sen alettua?

5.2.2 Osio 2 - Työskentely julkisilla paikoilla (1/2)

Toisessa osiossa tiedustellaan työskentelystä julkisilla paikoilla. Mikäli henkilö vastasi kysymykseen, että hän ei ole työskennellyt julkisilla paikoilla, siirtyi kysely seuraavan osion yli.

1. Työskenteletkö ikinä julkisilla paikoilla?

5.2.3 Osio 3 - Työskentely julkisilla paikoilla (2/2)

Tämä osio koostuu julkisilla paikoilla työskentelyn kannalta tärkeistä kysymyksistä, joilla koitettiin selvittää vastaajan tietoturvaosaamista ja sen mahdollisia puutteita.

1. Käytätkö näyttöön kiinnitettävää tietosuojafiltteriä työskennellessäsi julkisilla paikoilla?
2. Käytkö työhösi liittyviä puhekeskusteluja julkisilla paikoilla?
3. Käytätkö julkisia verkkoja tehdessäsi töitä etänä?
4. Käytätkö yleisessä käytössä olevia tulostimia tulostamaan töihisi liittyviä tiedostoja?

5.2.4 Osio 4 - Tietoturva (1/5)

Kysymyksillä 1 ja 2 selvitettiin vastaajan yleisymmärrystä tietosuojasta ja sen yhdestä toteuttamisen keinosta, tietoturvasta. Nämä kysymykset olivat verkkokyselyssä ainoita kysymyksiä, joissa vastaajaa pyydettiin antamaan lyhyt kuvaus kirjoittaen.

Vastaajalta kysyttiin kysymyksessä 3, käsitteleekö hän työssään henkilötietoja. Yrityksen vastuulla on kouluttaa työntekijät tietoturvalliseen henkilötietojen käsittelyyn. EU:n yleinen tietosuoja-asetus (engl. *General Data Protection Regulation – GDPR*) ja sen kanssa sovellettava tietosuojalaki koskee kaikkia tahoja, jotka ovat tekemisissä henkilötietojen kanssa niin kuluttaja-, kuin yrityssektorilla. (Ronkainen n.d.)

Kysymykset 3–6 olivat osana vastaajan syvemmän tietosuojaymmärryksen kartoittamista. Kysymyksissä 3, 5 ja 6 oli mahdollisuutena vastata, että ei ymmärrä termiä tai kysymystä. Näin saataisiin selkeämpi käsitys vastaajan tietoturvataitojen puutteista.

1. Mitä tarkoittaa tietoturva?
2. Mitä tarkoittaa tietosuoja?
3. Käsitteletkö työssäsi henkilötietoja?
4. Voiko joku ulkopuolinen nähdä työkoneesi näyttöön työskennellessäsi etänä?
5. Oletko käynyt GDPR koulutuksessa?
6. Kuinka usein käytät VPN-yhteyttä työskennellessäsi etänä?

5.2.5 Osio 5 - Tietoturva (2/5)

Tämän osion aiheena oli keskittyä sekä työlaitteiden fyysiseen- että ohjelmistolliseen suojaamiseen. Osion kolmella ensimmäisellä kysymyksellä kartoitettiin vastaajien työlaitteiden suojaustasoa. Kysymyksiin 2 ja 3 pystyi vastaamaan ”En tiedä”-vaihtoehdolla, jotta saataisiin parempi käsitys henkilön puuttuvista tiedoista. Kysymyksillä 3–6 pyrittiin selvittämään vastaajan tietämystä ohjelmistoturvallisuuden tärkeydestä ja siitä, onko heitä ohjeistettu työnantajan toimesta siinä.

Kysymyksellä 7 keskityttiin etätyöskentelyn verkkoturvallisuuteen. Nopea siirtyminen etätyöhön ilmeni Suomen verkkoihin liitettyjen suojaamattomien laitteiden kasvuna. Vuonna 2020 maaliskuussa julkiseen verkkoon liitettyjen laitteiden määrä oli noin neljänneksen isompi verrattuna tammi-helmikuuhun. (Kyberturvallisuuskeskus 2020b, 7.) Reitittimen oletussalasanan muuttaminen on tärkeässä osassa etätyöskentelyä, sillä ne ovat hyökkääjillä tiedossa. Oletussalasanan omaavan reitittimen kautta voi hyökkääjä saada pääsyn kaikkiin siihen yhdistettyihin laitteisiin. (F-Secure n.d.)

Osion viimeisessä kysymyksessä kysyttiin työhön liittyvien tiedostojen tallennuksesta salaamattomiin tallennuslaitteisiin, esim. USB-muistitikulle tai ulkoiselle kovalevylle. Ulkoiset lisälaitteet on syytä hyväksyttää työnantajalla, sillä niistä voi tarttua haittaohjelmia työlaitteille, joista ne taas voivat levitä työantajan järjestelmiin. Ulkoiset laitteet voivat myös joutua varastetuksi tai hukatuksi helpommin pienen kokonsa ansiosta.

1. Lukitsetko laitteesi aina, kun se jätetään valvomatta?
2. Miten työlaitteesi on suojattu?
3. Onko työkoneesi tallennuslaite salattu?
4. Kuinka usein päivität laitteesi käyttöjärjestelmän?
5. Ohjeistaako työnantajasi sinua laitteesi päivityksessä?
6. Käytätkö virustorjuntaohjelmaa työkoneellasi?
7. Huolehditko virustorjuntaohjelman päivittämisestä?
8. Onko etätöihin käyttämäsi reitittimen oletussalasana muutettu?
9. Tallennatko töihisi liittyviä tiedostoja salaamattomiin tallennuslaitteisiin?

5.2.6 Osio 6 - Tietoturva (3/5)

Tässä osiossa kartoitettiin vastaajan salasanaturvallisuutta ja sen ymmärrystä. Ensimmäisessä kysymyksessä tiedusteltiin salasanan hallintasovelluksen käyttöä vastaajalta ja sitä, onko työnantaja ohjeistanut siinä.

Hallintasovelluksella voidaan säilyttää ja käyttää salasanoja esimerkiksi eri nettipalveluissa. Sen avulla voidaan luoda nopeasti ja helposti vahvoja salasanoja, jotka auttavat suojautumaan niihin kohdistuvilta hyökkäyksiltä. (Kyberturvallisuuskeskus 2020c.)

Toisessa kysymyksessä kysyttiin, käyttääkö vastaaja samaa salasanaa useaan eri paikkaan. Kysymykseen pystyi vastaamaan ”En halua vastata”-vaihtoehdolla. Vahvakin salasana voi vuotaa tietomurron yhteydessä ja silloin hyökkääjillä on pääsy kaikille tileille, joissa samaa salasanaa on käytetty. Tämän vuoksi samaa salasanaa ei tulisi käyttää kahdessa palvelussa. (Rantalainen 2018.)

Kysymyksellä 3 selvitettiin, vastaavatko henkilön salasanat yrityksen standardeja ja siihen pystyi vastaamaan ”En ole varma”-vaihtoehdolla. Kysymyksellä 4 tiedusteltiin kuinka usein haastateltava vaihtaa salasanojaan. Karhulan (2020) mielestä salasana on syytä vaihtaa noin kolmen kuukauden välein, mutta sitä voidaan vaatia työnantajan toimesta useamminkin. Osion viimeisellä kysymyksellä selvitettiin, tallentaako henkilö salasanojaan työlaitteensa selaimeen. Haittaohjelma työlaitteella voi saada pääsyn selaimeen tallennettuihin salasanoihin, mutta myös työkoneen menettäminen vääriin käsiin tuo tämän riskin.

1. Käytätkö salasanojen hallintasovellusta?
2. Käytätkö samaa salasanaa useaan eri paikkaan?
3. Vastaako käyttämäsi salasanat yrityksesi määrittelemiä salasanastandardeja?
4. Kuinka usein vaihdat salasanasi?
5. Tallennatko salasanojasi työlaitteesi selaimeen?

5.2.7 Osio 7 - Tietoturva (4/5)

Osiossa 7 käsiteltiin työsähköpostia ja sen käyttämistä tietoturvallisesti. Työsähköpostin käyttäminen julkisilla alueilla on toteutettava varoen, varsinkin henkilötietoja käsitellessä. Kysymykset 3 ja

4 tiedustelivat vastaajalta, milloin sähköpostiviestejä kuuluisi salata ja onko vastaaja saanut siihen koulutusta työnantajaltaan.

Jokaisen suomalaisen yrityksen henkilötietojen käsittelyn on oltava EU:n tietosuoja-asetuksen mukaista. Esimerkiksi terveydenhoitoalalla mitään henkilötietoja, ei edes nimeä, saa lähettää suojaamattomassa sähköpostissa. (Turvaposti n.d.)

1. Käytätkö työsähköpostia julkisilla alueilla?
2. Käytätkö työsähköpostiasi johonkin muuhun kuin työasioihin?
3. Onko sinulle selvää, milloin lähetettäviä sähköpostiviestejä kuuluu salata?
4. Onko työnantajasi ohjeistanut sinua sähköpostiviestien salauksessa?

5.2.8 Osio 8 - Tietoturva (5/5)

Kyselyn viimeisen osion kahdessa ensimmäisessä kysymyksessä vastaaja laitettiin arvioimaan etätöiden riskejä lähityöhön ja tietoturvan tärkeyttä omassa työssä.

Yrityksen tiloissa on hyvässä tapauksessa huolehdittu kulunvalvonnasta, paloilmaisimista, kameravalvonnasta, tietoverkon turvaamisesta, turvalukituksesta ja vartioinnista. Lähes kaikki edellä kuvatut fyysisen tietoturvan elementit ovat poissa etätyössä. (Anttila 2020.)

Osion neljäs kysymys antoi vastaajalle mahdollisuuden ilmoittaa, ettei ole saanut tarpeeksi ohjeistusta tietoturvan osalta etätöiden tekemiseen.

1. Koetko etätyöskentelyn olevan lähityötä riskialttiimpaa tietoturvan näkökulmasta?
2. Kuinka tärkeänä pidät tietoturvaa nykyisessä työssäsi?
3. Kuinka vahvana koet osaamistasi ja tietämystäsi tietoturvaan liittyvissä asioissa?
4. Koetko tarvitsevasi ohjeistusta työnantajaltasi tietoturvaan liittyen?

5.3 Haastateltavat

Haastatteluihin valittiin henkilöt samalla periaatteella kuin verkkokyselyyn. Haastateltavan oli siis pitänyt tehdä etätöitä jossain vaiheessa työsuhteensa aikana, eikä sitä oltu rajattu esimerkiksi pelkälle pandemia-ajalle. Haastateltavat valittiin tutkimuksen monipuolisuuden vuoksi eri työaloilta.

Sekä haastattelut että verkkokysely toteutettiin täysin nimettömänä, koska tietoturvataidot tai niiden puutos ovat monelle arkaluonteista tietoa. Täyden nimettömyyden takia vastaukset voitiin antaa täysin luottamuksellisesti ja totuudenmukaisesti.

Verkkokyselyä jaettiin pääasiassa niille henkilöille, jotka olivat työskennelleet etänä. Jakokanavina käytettiin työsähköpostia ja henkilökohtaista sähköpostia. Vastaajille annettiin lupa jakaa verkkokyselyä etätöitä tekeville henkilöille. Verkkokysely toimitettiin saatetekstin kanssa. (ks. Liite 1).

5.4 Haastattelun toteutus ja analyysi

Haastattelut toteutettiin tietokoneen välityksellä, Microsoft Teams viestinä- ja yhteistyöalustaa käyttäen. Haastattelukysymykset olivat pääasiassa samoja kuin verkkokyselyssä, mutta avoimempia. Kysymyksiin ei vaadittu ”Kyllä” ja ”Ei”-vastauksia, vaan aiheesta keskusteltiin avoimesti. Näin ollen kysymyksiin pystyttiin vastaamaan vapaammin ja haastateltava pystyi tarvittaessa tarkentamaan vastaustaan. Haastattelut äänitettiin litteroinnin vuoksi.

Verkkokysely tehtiin Google Forms palvelulla sen ilmaisen ja yksinkertaisen käyttöliittymän takia. Kysely voitiin jakaa luvussa 5.2 esitettyihin osioihin, jotta se olisi vastaajalle helposti lähestyttävä ja vastattava.

6 Tutkimustulokset

6.1 Haastattelut

Puolistrukturoituun, eli teemahaastatteluun osallistui kolme henkilöä. Haastattelut toteutettiin ja tallennettiin erikseen Microsoft Teams viestinä- ja yhteistyöalustalla. Haastateltavat valittiin tarkoituksellisesti eri työaloilta monipuolisuuden vuoksi. Haastattelukysymykset olivat pääosin samoja kuin verkkokyselyssä (luku 5.2), mutta haastattelussa keskusteltiin myös välillä jostain alueista laajemmin.

Haastatteluja ennen haastateltaville ilmoitettiin haastattelun olevan täysin nimetön ja että se tallennetaan. Kysymyksillä ei ollut tarkkaa järjestystä, vaan tietoturvasta ja etätyöstä keskusteltiin aluksi avoimesti. Haastattelussa ei ollut pakko vastata kysymyksiin tai ottaa kantaa oman yrityksen toimintaan. Haastateltaville ilmoitettiin myös äänitallenteen poistosta jälkikäteen.

6.1.1 Haastattelu 1

Ensimmäinen haastateltava työskentelee puolustusvoimilla johtamisjärjestelmäalalla. Haastateltava tekee etätöitä ja on aloittanut etätyöt jo ennen koronapandemiaa. (luku 5.2.1). Puolustusvoimilla on haastateltavan mukaan kaikille pakolliset vuosittaiset tietoturvakoulutukset. (luku 5.2.4, kysymys 5). Koska kaikki ovat käyneet samat koulutukset, voi etätöitä tekemätön henkilö siirtyä etätöihin ilman erillistä koulutusta.

Tietoturvaa haastateltava kuvaili tietojen tai tietojärjestelmien turvaamisella eri järjestelmillä tai menettelytapamalleilla, jotta arkaluontoiset asiat eivät pääsisi niille kuulumattomien henkilöiden tietoon. Tietosuojaa taas kuvattiin tiedon suojaamiseen käytettävinä menetelminä ja suojaustason määrittämisellä esim. tietojen omilla tietoturvaluokilla. Haastateltava ei käsittele työssään henkilötietoja, eikä työskentele julkisilla alueilla. (luku 5.2.2, 5.2.4.)

Haastateltava tekee etätyöt niin, että rakennuksen ulkopuolelta ei voi olla mahdollisuutta nähdä työkoneen näyttöön. Hän kuitenkin piti mahdollisena perheenjäsenen nähdä työlaitteen näytölle tai kuulla työhön käytäviä keskusteluja. (luku 5.2.4, kysymys 4). Taukoja pidettäessä haastateltava

sanoi poistavansa toimikortin työkoneen lukitsemiseksi, mikäli asunnossa on muita ihmisiä. Työlaitteelle kirjautuessa vaaditaan toimikortin lisäksi salasana. Työlaitteen fyysiseen suojaukseen kuuluu myös kryptattu tallennuslaite ja näytön tietosuojakalvo. (luku 5.2.5, kysymykset 1–3.) Töihin käytettävät ulkoiset tallennuslaitteet ovat suojattu, ja kuten haastateltava totesi: ”*ulkoisia tallennuslaitteita käytetään vain tietojen siirtämiseen, ei säilyttämiseen*”. (luku 5.2.5, kysymys 9).

Laitteen ohjelmistot on suojattu virustorjuntaohjelmalla ja käyttöjärjestelmien päivittäminen tapahtuu etänä, eli työntekijältä vaaditaan vain työkoneen uudelleenkäynnistys. (luku 5.2.5) Päivitykset voidaan myös pakottaa johtamisjärjestelmäkeskukselta, mikäli niitä ei ole asennettu tai jos niissä on huomattu ongelmia. Myös eri ohjelmia, sovelluksia tai verkkosivuja laitetaan kieltoon, mikäli niistä on löytynyt tietoturvahaavoittuvuuksia. Salattu yhteys puolustusvoimien käyttämään yksityisverkkoon on aina töitä tehdessä päällä ja ilman tätä ei voi yhdistää julkiseen verkkoon. (luku 5.2.4, kysymys 6). Verkkoyhteyden luomiseen saa käyttää vain WLAN-yhteyttä, joko omalta puhelimelta tai kotiverkossa. Haastateltava on vaihtanut kotiverkon oletussalasanan ja salannut puhelimella jaetun yhteyden.

Haastateltavan mukaan työnantaja ei ole ohjeistanut salasanaohjelmiston käytössä, mutta salasanat ovat haastateltavalla salasanalla suojattuna tallella. (luku 5.2.6, kysymys 1). Salasanoja ei tallenneta työlaitteen selaimeen, eikä suojaamattomalle laitteelle. (5.2.6, kysymys 5). Salasanat vaihdetaan hallitusti järjestelmistä riippuen. Joissain järjestelmissä salasanat vaihdetaan noin kolmen kuukauden välein ja toisissa harvemminkin. (luku 5.2.6, kysymys 4). Salasanavaatimukset vaihtelevat järjestelmien iästä ja suojaustasosta, mutta mitään salasanastandardeja ei ole yrityksen puolesta kaikille järjestelmille annettu. (luku 5.2.6, kysymys 3). Haastateltava ei käytä samaa salasanaa useassa järjestelmässä, eikä vanhoja salasanoja voi uudelleen käyttää vaan ne on aina luotava uusi turvallinen salasana. (luku 5.2.6, kysymys 2).

Sähköpostin käyttöön liittyvissä kysymyksissä vastattiin esimerkiksi, että työsähköpostia käytetään vain työkoneella, sillä työpuhelimessa ei ole nettiyhteyttä. (luku 5.2.7, kysymys 1). Työhön liittyvät sähköpostit lähetetään tarkoin suojatussa ja valvotussa hallinnon turvallisuusverkossa (TUVE), mutta on myös olemassa ns. punaisen puolen sähköpostiverkko, jossa lähetetään kaikki tietoturva-

luokan sähköpostit. (luku 5.2.7, kysymykset 3,4). Haastateltava mainitsi lähettäneensä omasta sähköpostista työsähköpostiin viestejä, mutta työsähköpostilla lähetetään vain töihin liittyviä asioita. (luku 5.2.7, kysymys 2).

TUVE-toimintaan liittyvään tarkentavaan kysymykseen vastattiin seuraavasti:

> *En voi vastata tähän. En ole tarkoituksella edes yrittänyt selvittää tarkemmin TUVE-toimintaa, koska se ei suoranaisesti liity omaan työnkuvaani. Se on myös osa tietoturvaa, ettei etsi tietoja mitä ei tarvitse työssään. Silloin sitä ei voi vahingossakaan viedä ihmisille, kenelle se ei kuulu*.

Haastateltava kokee etätöiden olevan huomattavasti lähityötä riskialttiimpaa tietoturvan näkökulmasta. Etätyön uhkana haastateltava kokee, ettei osata huomioida sivullisten katseita tai kuuntelemista ja näin ollen pitää etätyössä käytäviä puheluita suurimpana etätöiden riskinä. (luku 5.2.8, kysymys 1.) Haastateltava koki tietoturvan erittäin tärkeänä työssään, koska hän käsittelee maanpuolustukseen liittyviä kriittisiä tietoja. (luku 5.2.8, kysymys 2). Omaa tietoturvaosaamistaan haastateltava arvioi vahvaksi pitkän työkokemuksen takia. (luku 5.2.8, kysymys 3). Työnantajalta hän ei kokenut tarvitsevansa koulutusta oman työnsä tekemiseen tietoturvallisesti, mutta aina välillä voi yksittäistapauksia ilmetä. (luku 5.2.8, kysymys 4).

6.1.2 Haastattelu 2

Toinen haastateltava työskentelee kaupan alalla asiantuntijan roolissa ja pandemiasta johtuen aloittanut etätyöt. Työt hän tekee kotoansa, eikä hän työskentele julkisilla alueilla. (luku 5.2.1, 5.2.2.) Tietoturvaa haastateltava kuvaili arkaluontoisen tiedon suojaamisella tai salaamisella. Tietosuoja taas seuraavasti: ”*en ole ikinä ymmärtänyt näiden käsitteiden eroa, mutta tietosuoja kuulostaa siltä, että se on joku ohjelma, jolla saa koneelleen virussuojan*”.

Työssään hän käsittelee henkilötietoja päivittäin, mutta yksin asuessaan ei koe kenelläkään olevan mahdollisuutta kuunnella työpuheluita tai nähdä työkoneen näytölle. (luku 5.2.4, kysymykset 1–4.) Haastateltava ei ole ikinä käynyt missään GDPR-, tai tietosuojakoulutuksessa, eikä niitä ole tarjottu työnantajankaan puolesta. VPN-yhteyttä ei käytetä työnteossa, eikä reitittimen oletussalasanaa ole vaihdettu. (luku 5.2.4, kysymykset 5–6.)

Työlaitteiden fyysisestä suojaamisesta ei ole ohjeistettu haastateltavaa ollenkaan. Haastateltava työskentelee työpaikalla työpaikan tietokoneilla ja kotona henkilökohtaisella tietokoneellaan. Työpaikalla käytetään ns. ”hotspot”-työpisteitä, jotka ovat henkilökunnalle varattuja tietokoneellisia paikkoja. Hän ei lukitse laitetta työpaikalla, eikä kotona. (luku 5.2.5, kysymys 1). Työkoneelle ja henkilökohtaiselle koneelle hän kirjautuu joko salasanalla tai PIN-koodilla. (5.2.5, kysymys 2.) Tallennuslaitteita ei ole omalla, eikä työpaikan koneella haastateltavan ymmärryksen mukaan salattu. (5.2.5, kysymys 3).

Työpaikan tietokoneilla on osalla käyttäjistä henkilökohtaiset käyttäjätunnukset, muutamalla nimetyillä henkilöillä järjestelmävalvojan tunnukset ja muut käyttävät tietokoneen yleistä käyttäjää. Haastateltavan mielestä tämä järjestely on erittäin huonosti toteutettu, mutta ei arvioinut muita työntekijöitä tämän kiinnostavan. Syyksi haastateltava arvioi startup-yrityksen nopean kasvun, eikä tietoturva ole kerennyt tulla yrityksen muun kasvun mukana.

Työnantaja ei ole ohjeistanut ohjelmistoturvallisuudessa haastateltavaa. Virustorjunnasta eikä käyttöjärjestelmän päivityksestä ollut ohjeistusta. Käyttöjärjestelmän hän mainitsi kotikoneella päivittänsä silloin tällöin, mutta työpaikan koneet eivät ole aina aivan ajan tasalla. (luku 5.2.5, kysymykset 4–7). Hänen henkilökohtaista konettaan ei millään tavalla tarkistettu esimerkiksi tietoturvaosaston puolesta, vaan hän sai suoraan aloittaa työn tekemisen sillä.

Salasanoihin liittyvissä kysymyksissä haastateltava mainitsi esimerkiksi käyttävänsä samaa salasanaa useimpiin kirjautumisiin, eikä niitä ole tallennettu selaimeen eikä muihin sovelluksiinkaan. (luku 5.2.6, kysymykset 1,2,5). Jotkut järjestelmät voivat hänen mukaansa vaatia tietyn vahvuuden salasanoja ja työnantajan toimesta on yhden kerran vuoden sisällä määrätty kaikki työntekijät vaihtamaan salasanansa. Henkilökohtaisella tietokoneellaan hän vaihtaa salasanojaan satunnaisesti. Joskus voi mennä vuosi ja jossain voi olla usean vuodenkin vanha salasana. (luku 5.2.6, kysymys 4.)

Työsähköpostia haastateltava käyttää pelkästään työasioihin ja pelkästään työlaitteilla. (luku 5.2.7, kysymykset 1–2). Hänelle ei ollut selvää, milloin sähköpostiviestit kuuluvat salata, eikä työnantaja ollut ohjeistanut tässä. (luku 5.2.7, kysymykset 3–4).

Haastateltava koki etätyöt riskialttiimpana kuin lähityön ja perusteli sen seuraavasti: *”työnantajan on paljon vaikeampi kontrolloida sitä mitä työntekijät tekevät, varsinkin jos käyttää omaa tietokonetta”.* (luku 5.2.8, kysymys 1). Tietoturvaa hän pitää melko tärkeänä nykyisen työnsä kohdalla ja koki sen olevan vielä tärkeämpi kuin se mihin hänen yrityksensä on varautunut. (luku 5.2.8, kysymys 2). Oman tietoturvaosaamisen hän arvioi heikoksi ja mainitsi tarvitsevansa suuresti apua tässä työnantajaltaan. (luku 5.2.8, kysymys 3). Haastateltava myös lisäsi, että hän kokee sen olevan työnantajan vastuulla opettaa työntekijöitään, eikä hänen henkilökohtainen vastuunsa. (luku 5.2.8, kysymys 4).

6.1.3 Haastattelu 3

Kolmas haastateltava työskentelee ohjelmistoalalla IT-asiantuntijana ja hän tekee työnsä vaihtelevasti etänä. Etätöitä hän on tehnyt jo ennen koronapandemiaa, mutta pandemiasta johtuen ne ovat lisääntyneet. (luku 5.2.1.) Työt hän tekee joko yksin kotona tai sitten toimistolla. Julkisilla paikoilla ei hänen tule työskenneltyä. (luku 5.2.2).

Tietoturva tarkoittaa haastateltavan mukaan fyysisiä käytänteitä ja ohjeistuksia siihen, miten toimitaan fyysisen maailman puolella. Hän myös mainitsi esimerkeiksi seuraavat asiat: ”oven sulkeminen lähtiessäsi työtilasta” ja ”muista lukita tietokoneesi poistuessasi työpaikalta”. Tietosuoja kuvattiin tavaksi käsitellä sinulle oikeutettua dataa turvallisesti. (luku 5.2.4, kysymykset 1,2.) Haastateltava käsittelee henkilötietoja harvoin työssään, mutta tätä varten on pitänyt käydä työnantajan järjestämä GDPR-koulutus. Hänen työnsä tekeminen on mahdollista vain VPN-yhteyttä käyttämällä, joten se on aina töitä tehdessä päällä. (5.2.4, kysymykset 3,5,6.)

Haastateltava sanoi työnantajan ohjeistaneen laitteen fyysisessä suojauksessa. Toimistolla työskennellessä laite lukitaan aina työpisteeltä poistuessa, mutta kotona työajalla pidettyjen taukojen aikana ei laitetta lukita. Tätä haastateltava perusteli seuraavasti: ”*en koe yksin asuessani tarpeelliseksi lukita laitettani taukojen aikana, koska ainoa tapa päästä laitteeseeni käsiksi on murtautua fyysisesti ovesta läpi ja näin ollen tunkeutuu asuntooni*”. (luku 5.2.5, kysymys 1.) Työlaitteelle kirjautuminen on suojattu käyttäjätunnuksella ja salasanalla. Näiden lisäksi laite on suojattu kovalevyn salauksella. (luku 5.2.5, kysymys 2,3.) Ulkoisia tallennuslaitteita hän ei työssään käytä, vaan mainitsi kaikkien työasioiden olevan pelkästään yhdellä tallennuslaitteella. (luku 5.2.5, kysymys 9).

Ohjelmistoturvallisuudesta hänen mukaansa oli ohjeistettu työnantajan toimesta. Työnantaja oli esimerkiksi ohjeistanut käyttöjärjestelmän päivittämisessä, kun siitä oli havaittu tietoturvahaavoittuvuus. (luku 5.2.5, kysymys 5.) Muussa tapauksessa haastateltava huolehtii itse laitteen käyttöjärjestelmän ja virustorjuntaohjelman päivittämisestä. (luku 5.2.5, kysymykset 4–7.) Etätöitä tehdessä hän käyttää langatonta-, ja langallista internetyhteyttä. Molemmat näistä yhteyksistä on salasanasuojattu. (luku 5.2.5, kysymys 8.) Työlaitteelle asennettavien ohjelmien rajoituksista hän ei ollut saanut ohjeistusta työnantajaltaan ja mainitsi selvittävänsä asiaa.

Haasteltavan salasanat ovat yrityksen salasanastandardien mukaisia ja niitä säilytetään työnantajan kehotuksesta salasanojen hallintaohjelmassa, mutta osa salasanoista on tallennettu työlaitteen selaimeen. (luku 5.2.6, kysymykset 1,3,5). Samaa salasanaa hän ei käytä useassa eri ympäristössä, koska se on määritelty yrityksen yleisissä tietoturvaohjeissa. (luku 5.2.6, kysymys 2). Haastateltava mainitsi vaihtavansa salasanansa helposti niiden hallintaohjelman avustuksella 3–6 kuukauden välein. (luku 5.2.6, kysymys 4).

Työsähköpostia haastateltava käyttää pelkästään työasioihin, mutta tästä ei ole hänen mukaansa ohjeistettu työnantajan toimesta ollenkaan. (luku 5.2.7, kysymys 2). Sähköpostia haastateltava käyttää ainoastaan työtietokoneella ja vain työskentelyn ohella. (luku 5.2.7, kysymys 1). Sähköpostiviestejä ei haastateltava ole salannut, eikä tarve niiden salauksesta ollut tuttu. (luku 5.2.7, kysymykset 3–4).

Etätyöskentelyn hän kokee olevan tietoturvan näkökulmasta riskialttiimpaa, koska työntekijällä on osittain itsellä vastuu toimia tietoturvallisesti ja koska etätyössä ei usein ole kulunvalvontaa. (luku 5.2.8, kysymys 1). Tietoturvaa haastateltava pitää erittäin tärkeänä työssään ja kokee oman tietoturvaosaamisen hyvänä. (luku 5.2.8, kysymys 2–3). Tietoturvallisen etätyön tekemisestä hän ei koe tarvitsevansa koulutusta työnantajaltaan, mutta hän haluaisi tutustua tarkemmin työnantajan tietosuoja-, ja etätyömääräyksiin. (luku 5.2.8, kysymys 4).

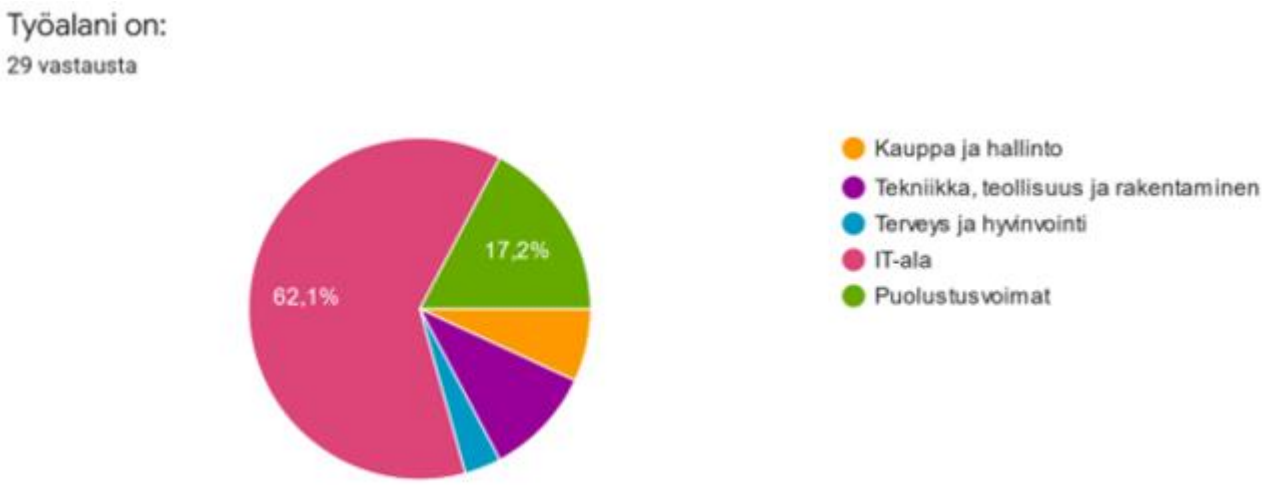
Haastateltava mainitsi hänen mielestään kolme tärkeintä asiaa, jotka tulisi muistaa etätyössä:

1. Työlaitteen fyysinen suojaus ja turvallisuus
2. Tietojen turvallinen säilytys, käyttö ja niiden oikeudet
3. Ohjelmistoturvallisuus ja salasanakäytänteet

6.2 Verkkokysely

Verkkokyselyä jaettiin kohdeyrityksessä, sekä sen ulkopuolella n. 40 henkilölle ja siihen vastasi 29 henkilöä. Yksi kyselyyn vastanneista vastasi, ettei ollut tehnyt etätöitä, vaikka verkkokyselyn saatetekstissä (Liite 1.) oli mainittu kyselyn kohdistuvan vain etätöitä tekeville, tai etätöitä tehneille henkilöille. Näin ollen tutkimukseen käytettäviä vastauksia saatiin verkkokyselyllä 28 henkilöltä. Teemahaastatteluista saatuja vastauksia ei lisätty verkkokyselyn tuloksiin, vaan ne on käsitelty luvussa 7 Tulosten yhteenveto.

Työalojen jakauma on kuvattu kuviossa 2. Kyselyyn vastanneiden työaloissa oli vaihtelua, mutta suurin (62,1 %) osa vastaajista vastasi työskentelevänsä IT-alalla. (luku 5.2.1, kysymys 1.) Kyselyn vastauksia tuli IT-alalta 18 kappaletta, puolustusvoimilta 5 kappaletta ja loput 5 kappaletta muilta työaloilta.

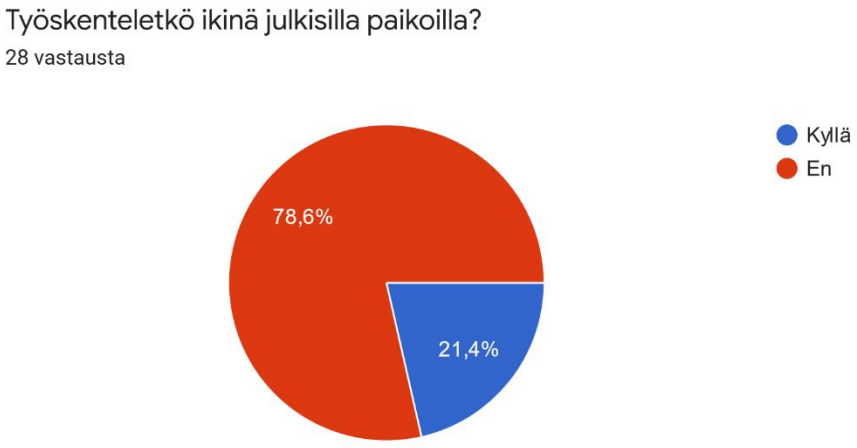


Kuvio 2. Kyselyn työalojen jakauma

Kuvio 3 osoittaa koronapandemian lisänneen etätyöskentelyä, sillä vain seitsemän vastaajaa vastasi työskennelleensä etänä jo ennen pandemia-aikaa. Loput vastanneet aloittivat etätyöskentelyn vasta koronapandemian alettua. (luku 5.2.1, kysymys 3.)

Kuvio 3. Etätyöskentelyn kasvu pandemian seurauksena

Seuraavaksi kyselyssä selvitettiin julkisilla paikoilla työskentelevien määrää. (luku 5.2.2, kysymys 1.) Vastanneista vain 6 henkilöä vastasi työskennelleensä julkisilla paikoilla (ks. Kuvio 4). Julkisilla paikoilla työskennelleet saivat neljä lisäkysymystä: ”Käytätkö näyttöön kiinnitettävää tietosuojafiltteriä työskennellessäsi julkisilla paikoilla?”, ”Käytkö työhösi liittyviä puhekeskusteluja julkisilla paikoilla?”, ”Käytätkö julkisia verkkoja tehdessäsi töitä etänä?” sekä ”Käytätkö yleisessä käytössä olevia tulostimia tulostamaan töihisi liittyviä tiedostoja?” (luku 5.2.3.)



Kuvio 4. Julkisilla paikoilla työskennelleiden määrä

Kuviosta 5 nähdään, että kolmasosa julkisilla paikoilla työskentelevistä käyttää näyttöön kiinnitettävää tietosuojafiltteriä. Yksi kuudesta vastasi käyttävänsä julkisia verkkoja töiden tekemiseen. Jokainen julkisilla paikoilla työskentelevä vastasi käyvänsä työhön liittyviä puhekeskusteluja, eikä yksikään vastannut käyttävänsä julkisessa käytössä olevia tulostimia tulostamaan töihin liittyviä tiedostoja.

Kuvio 5. Tietoturva julkisilla alueilla

Kyselyssä avoimilla kysymyksillä selvitettiin vastaajan ymmärrystä tietoturvasta ja -suojasta. (luku 5.2.4, kysymykset 1 ja 2.) Moni vastasi tietoturvan olevan tapa turvata luottamuksellista tietoa, joka on vain sille oikeutettujen saatavilla. Useissa vastauksissa myös mainittiin CIA-tietoturvamalli. Vastanneet kuvailivat tietoturvaa seuraavasti:

> *”Se tarkoittaa nimensä mukaan tiedon käsittelemistä turvallisesti. Tiedostetaan tiedon sensitiivisyys ja salaisuus ja käsitellään sitä sen mukaisesti. Tietoturvaa tulee soveltaa riippumatta missä muodossa se on.”*

> *”Turvallista datan luomista, siirtämistä tai säilyttämistä niin, että siihen ei päästä tai se ei pääse vuotamaan kolmannelle osapuolelle.”*

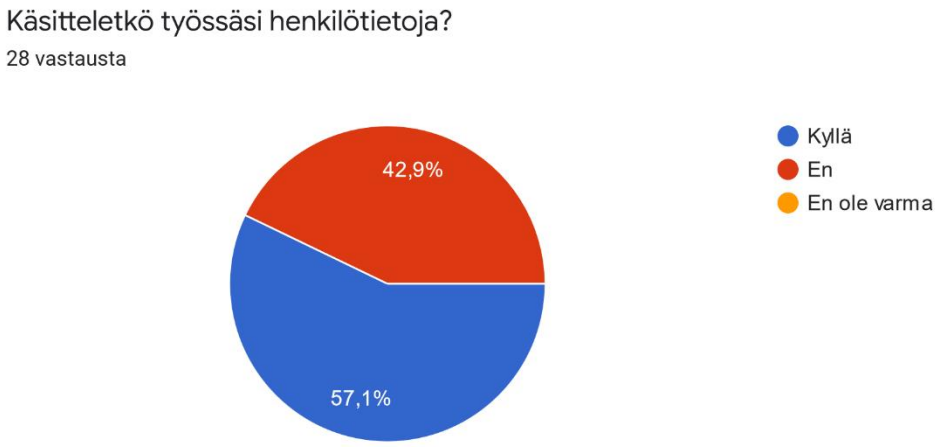
> *”Tietoturva mielestäni keskittyy enemmän tiedon kontrollointiin ja fyysiseen kerrokseen sen toteutuksessa.”*

”CIA. Tiedon saatavuus, luottamuksellisuus ja eheys”

Tietosuojaa kuvattiin suurimmaksi osaksi perustuslain takaamana yksityisyyden suojana sekä arkaluonteisten tietojen käsittelemistä vain silloin kun siihen on tarve. Kolme vastaajaa jätti vastaamatta kysymykseen. Tietosuojaa kuvattiin seuraavasti:

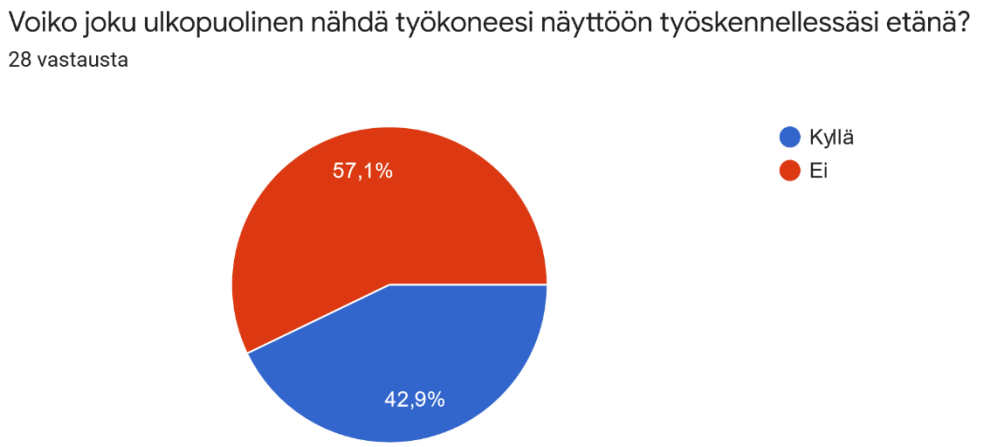
> *”Yksityisyyden suojan takaaminen, joka on mm. määritelty perustuslaissa”*
>
> *”Tiedon käsittelyyn määritellyt käyttäjäoikeudet. Kuka, miten ja missä voi mitäkin tietoa käsitellä.”*
>
> *”Henkilötietojen suojausta. Yritykset tai muut tahot saavat käyttää henkilötietoja vain, jos sille on perusteet”*
>
> *”Henkilöt voivat luottaa siihen, että annettuja tietoja käsitellään asiallisesti”*

Seuraavaksi selvitettiin henkilötietoja käsittelevien vastaajien määrää. (luku 5.2.4, kysymys 3.) Kuviosta 6 nähdään, että enemmistö (57,1 %) kyselyyn vastanneista käsittelee työssään henkilötietoja.



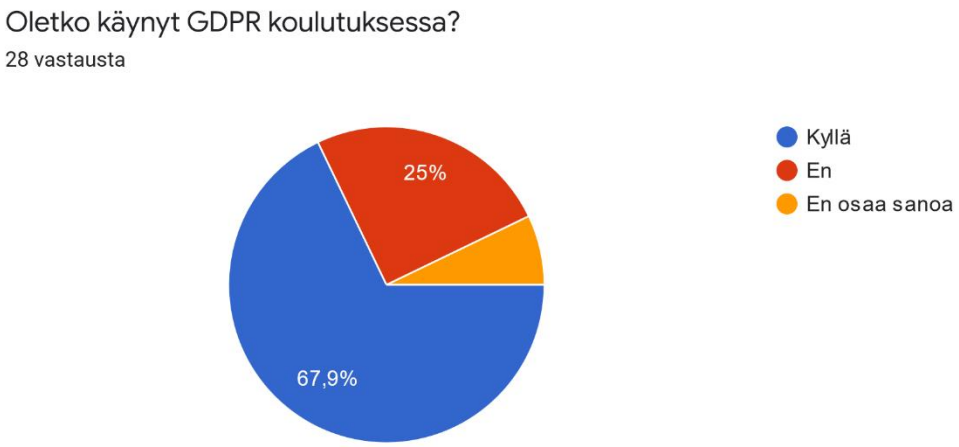
Kuvio 6. Henkilötietoja käsittelevien vastanneiden määrä

Tämän jälkeen selvitettiin, että onko etänä ulkopuolisilla mahdollisuutta nähdä etänä työskentelevien näyttöön. Kuviosta 7 ilmenee enemmistön (57,1 %) vastanneen, ettei ulkopuolisilla ole mahdollisuutta nähdä työkoneen näyttöön heidän työskennellessä etänä.



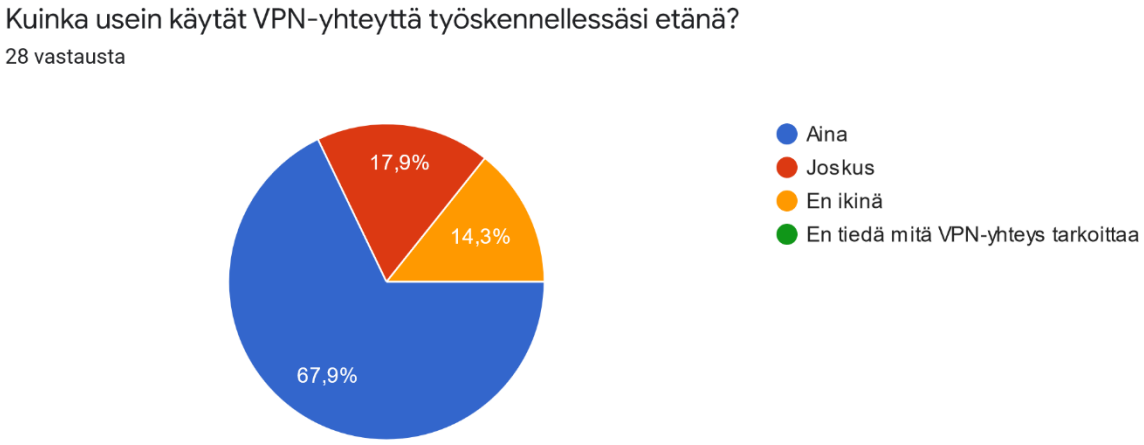
Kuvio 7. Näytönjako ulkopuoliselle

Seuraavaksi selvitettiin GDPR koulutukseen osallistuneiden vastaajien määrää. (luku 5.2.4, kysymys 5.) Kuviossa 8 nähdään, että enemmistö (67,9 %) vastasi käyneensä GDPR koulutuksessa ja neljännes vastasi, ettei ollut käynyt GDPR koulutusta. Vastauksissa oli myös vaihtoehtona ”En osaa sanoa” ja sen valitsi 2 vastaajaa.



Kuvio 8. GDPR koulutuksessa käyneiden määrä

Seuraavalla kysymyksellä selvitettiin VPN-yhteyttä käyttävien vastaajien määrää. (luku 5.2.4, kysymys 6.) Kuviossa 9 ilmenee, että 4 vastaajaa (14,3 %) ei käytä VPN-yhteyttä etätöiden tekemiseen sekä valtaosa (67,9 %) käyttää aina ja loput vastaajista käyttää joskus.



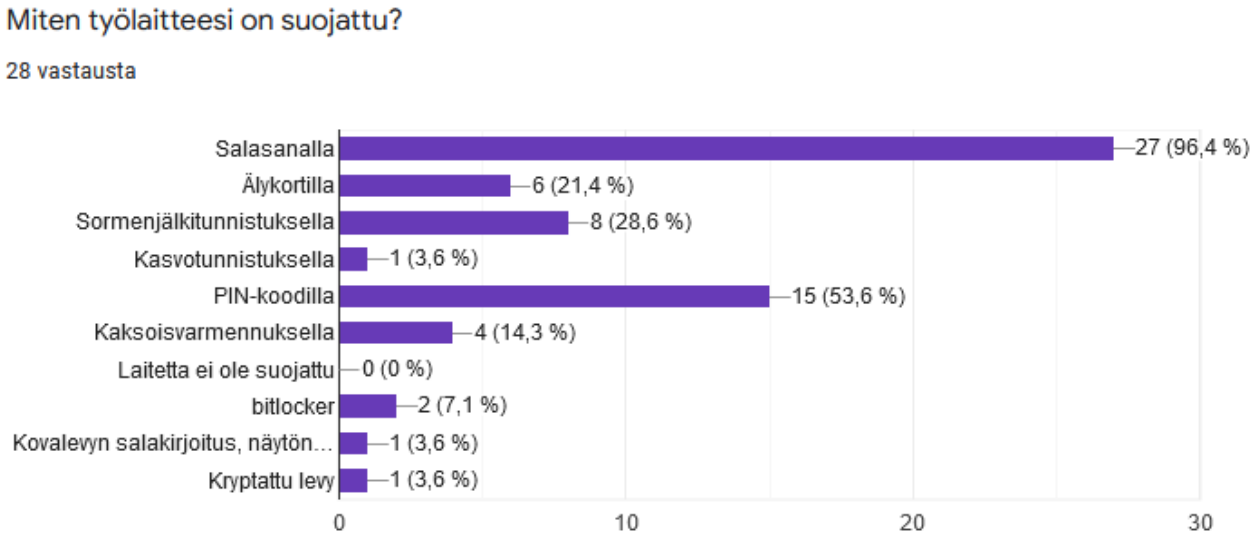
Kuvio 9. VPN-yhteyden käyttö

Seuraavaksi kyselyssä siirryttiin käsittelemään työlaitteiden suojausta. Osion ensimmäisessä vaiheessa selvitettiin, että jättääkö vastannut henkilö työlaitteensa lukitsematta, kun se jätetään valvomatta. (luku 5.2.5, kysymys 1). Kuvion 10 perusteella 67,9 % vastanneista lukitsee työlaitteen aina, kun se jätetään valvomatta.

Kuvio 10. Työlaitteen lukitseminen

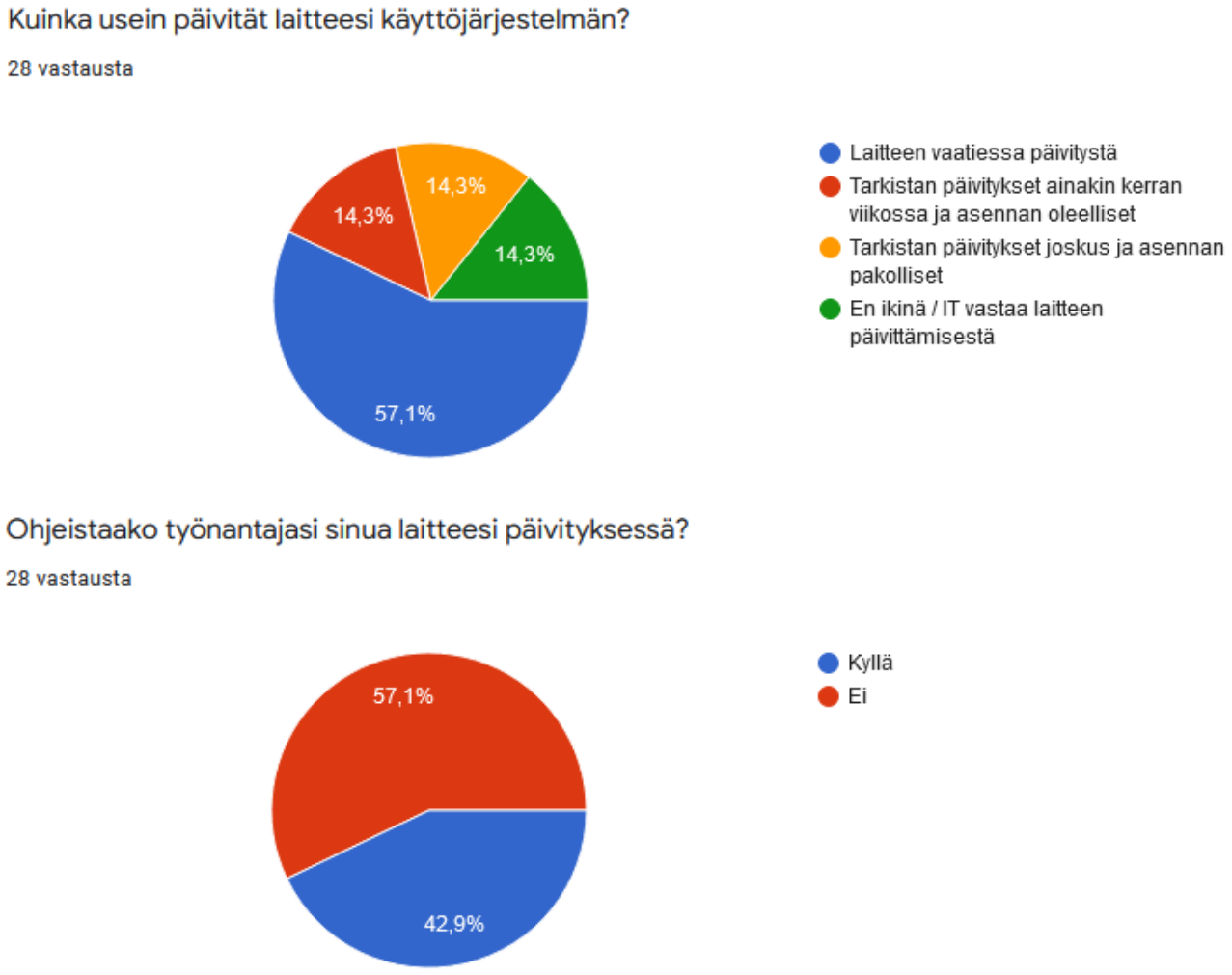
Tämän jälkeen pyrittiin selvittämään tapoja, joilla vastanneiden työlaitteet ovat suojattu. (luku 5.2.5, kysymys 2). Vastauksia pystyi valita useita, sekä kirjoittamaan oman vastauksen, mikäli valmiiksi annetuissa vastausvaihtoehdoissa ei tarvittavaa vastausta ollut.

Yleisin vastaus työlaitteen suojaukseen oli salasana (96,4 %), PIN-koodi (53,6 %) ja sormenjälkitunnistus (28,6 %). Vastaukset ”*bitlocker*”, ”*Kovalevyn salakirjoitus, näytön tietosuojakalvo*” ja ”*Kryptattu levy*” eivät olleet osana kyselyä, vaan nämä vastattiin omalla vastauksella. (Kuvio 11.)



Kuvio 11. Työlaitteen suojaus

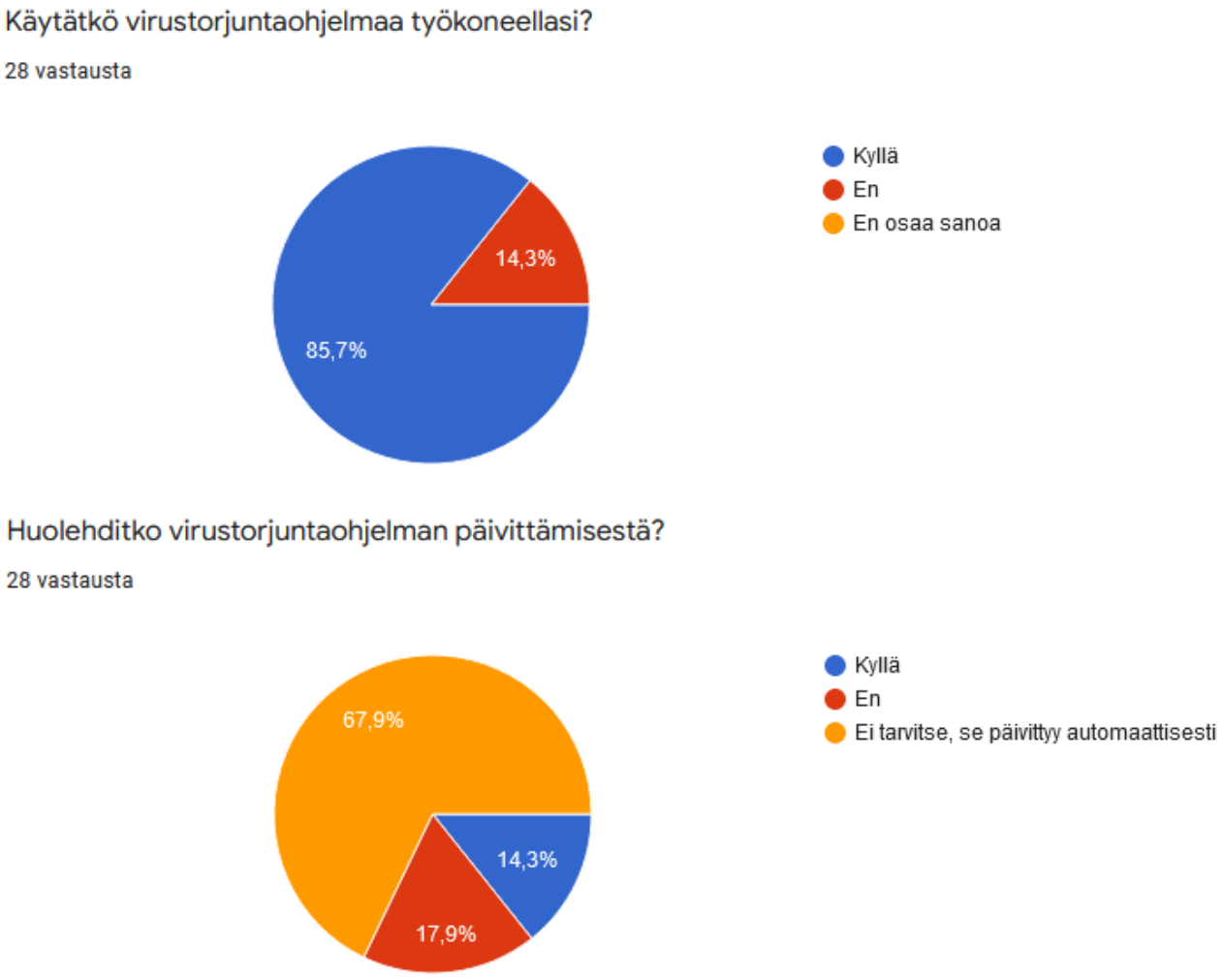
Seuraavaksi selvitettiin työlaitteen ohjelmistotason turvallisuutta. Ensiksi kysyttiin työlaitteen käyttöjärjestelmän päivittämisestä (luku 5.2.5, kysymys 3.) ja ohjeistetaanko siinä työnantajan toimesta. (luku 5.2.5, kysymys 4.) Kuviossa 12 ilmenee, että enemmistö (57,1 %) vastaajista päivittää työlaitteensa käyttöjärjestelmän silloin, kun laite sitä vaatii. Osa vastaajista huolehtii käyttöjärjestelmän päivittämisestä aktiivisesti, toiset vähemmän aktiivisesti ja jotkut ei ollenkaan. Valtaosa (57,1 %) myös vastasi, ettei työnantaja ohjeista heitä käyttöjärjestelmän päivittämisessä.



Kuvio 12. Käyttöjärjestelmän päivittäminen

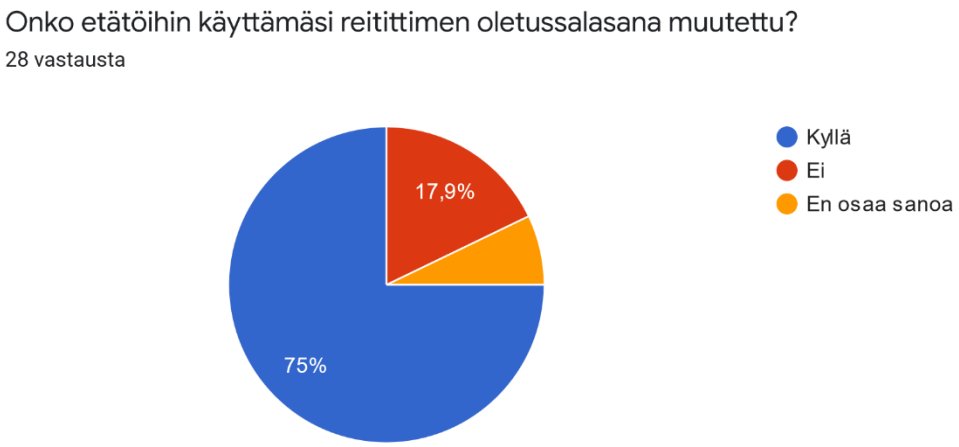
Toisena asiana ohjelmistoturvallisuudessa selvitettiin, että käyttääkö vastaaja virustorjuntaohjelmaa työkoneella ja huolehtiiko hän sen päivittämisestä. (luku 5.2.5, kysymys 5 ja 6.) Kuviosta 13 selviää, että osa (14,3 %) vastaajista ei käytä ollenkaan virustorjuntaohjelmaa työkoneellaan. Virustorjuntaohjelmaa päivittää manuaalisesti vastaajista 14,3 % ja 17,9 % vastaajista ei päivitä sitä ollenkaan. Loput vastaajista luottaa, että se päivittyy automaattisesti.

Neljä vastaajaa vastasi, ettei käytä virustorjuntaohjelmaa ollenkaan. Samoille vastaajille esitettiin kuitenkin seuraavakin kysymys virustorjuntaohjelman päivittämisestä, joten on todennäköistä heidän vastanneen, ettei he päivitäkään sitä. Tämä kuitenkin jättää yhden pätevän vastauksen kohtaan ”En (päivitä virustorjuntaohjelmaa)”.



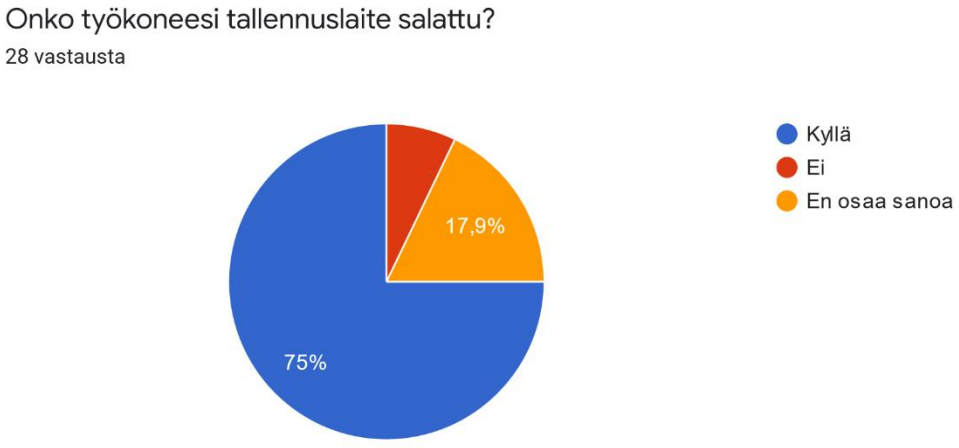
Kuvio 13. Virustorjuntaohjelman käyttö

Seuraavaksi vastaajalta kysyttiin, että onko hänen etätyöhönsä käytettävän reitittimen oletussalasana muutettu. (luku 5.2.5, kysymys 7.) Kuviosta 14 ilmenee osan (17,9 %) käyttävän reitittimen oletussalasanaa, kaksi vastannutta ei osannut sanoa ja loput (75 %) vastasi sen olevan muutettu.



Kuvio 14. Reitittimen oletussalasana

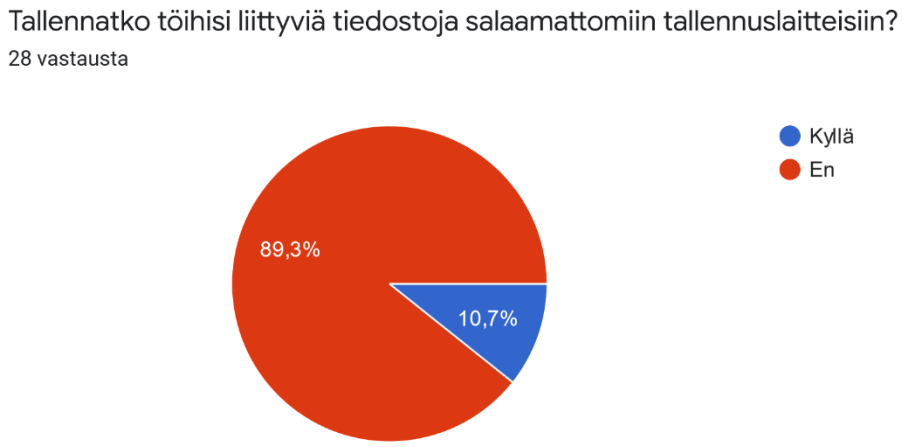
Tämän jälkeen kysyttiin, että onko vastaajan työkoneen tallennuslaite salattu. (luku 5.2.5, kysymys 8.) Vastanneista 17,9 % ei osannut sanoa, onko tallennuslaite salattu, kaksi vastannutta tiesi sen olevan salaamaton ja loput (75 %) tiesi sen olevan salattu. (Kuvio 15.)



Kuvio 15. Tallennuslaitteen salaus

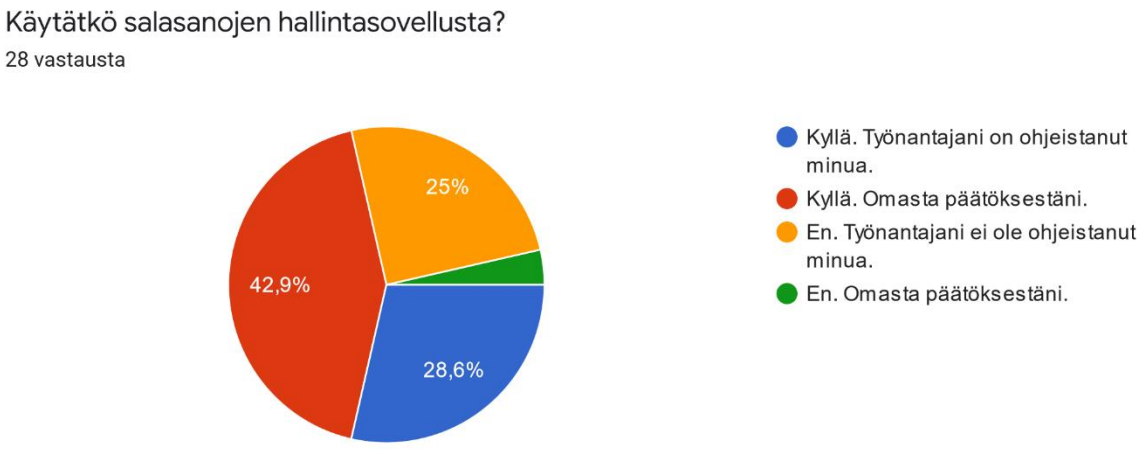
Seuraavaksi kyselyllä selvitettiin, tallentaako vastaaja töihin liittyviä tiedostoja salaamattomiin tallennuslaitteisiin, kuten USB-muistitikkuun, tai ulkoiselle kovalevylle. (luku 5.2.5, kysymys 9.) Vain 3

vastannutta sanoi tallentavansa salaamattomille laitteille työhön liittyviä dokumentteja ja loput (89,3 %) vastasi ettei tallenna. (Kuvio 16.)



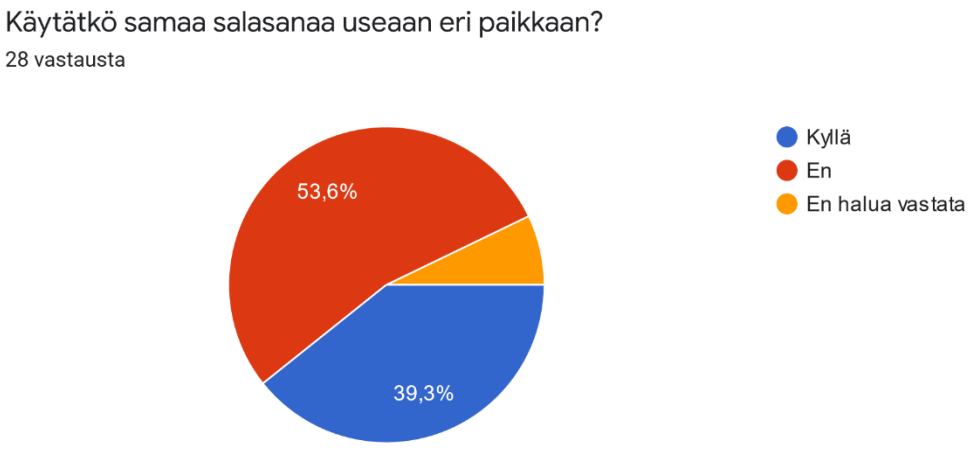
Kuvio 16. Salaamattomien tallennuslaitteiden käyttö

Kyselyn seuraavassa osiossa käsiteltiin salasanoja, niiden hallitsemista ja käyttöä. Ensiksi selvitettiin, että käyttääkö vastaaja salasanojen hallintaan tarkoitettua sovellusta. (luku 5.2.6, kysymys 1.) Kuviosta 17 nähdään, että enemmistö vastanneista käyttää salasanojen hallintasovellusta. 12 vastaajaa (42,9 %) käyttää sitä omasta päätöksestään ja 8 vastaajaa (28,6 %) työnantajan ohjeistuksesta. Neljännes vastasi, että ei käytä salasanojen hallintasovellusta ja että työnantaja ei ole ohjeistanut siinä. Yksi henkilö vastasi, ettei hän omasta päätöksestään käytä.



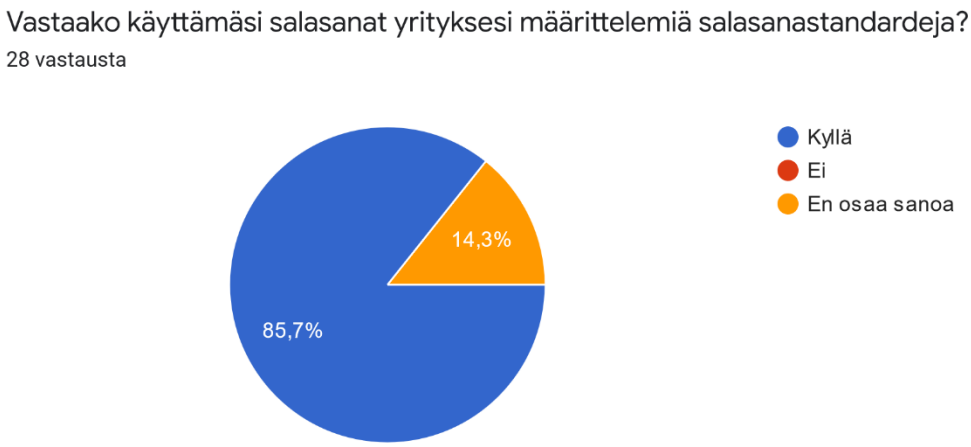
Kuvio 17. Salasanojen hallintasovelluksen käyttö

Tämän jälkeen kysyttiin, että käyttääkö vastaaja samaa salasanaa useaan eri paikkaan. (luku 5.2.6, kysymys 2.) Vastaukseen pystyi myös vastata vaihtoehdolla: ”En halua vastata”, sillä omaan salasanaan liittyviin kysymyksiin vastaaminen voi olla tietoturvariski. Kuviossa 18 ilmenee, että osa (7,1 %) vastaajista halusikin olla vastaamatta kyseiseen kysymykseen. Osa (39,3 %) vastasi käyttävänsä salasanoja toistuvasti, mutta valtaosa (53,6 %) sanoi, ettei käytä samaa salasanaa useaan eri paikkaan.



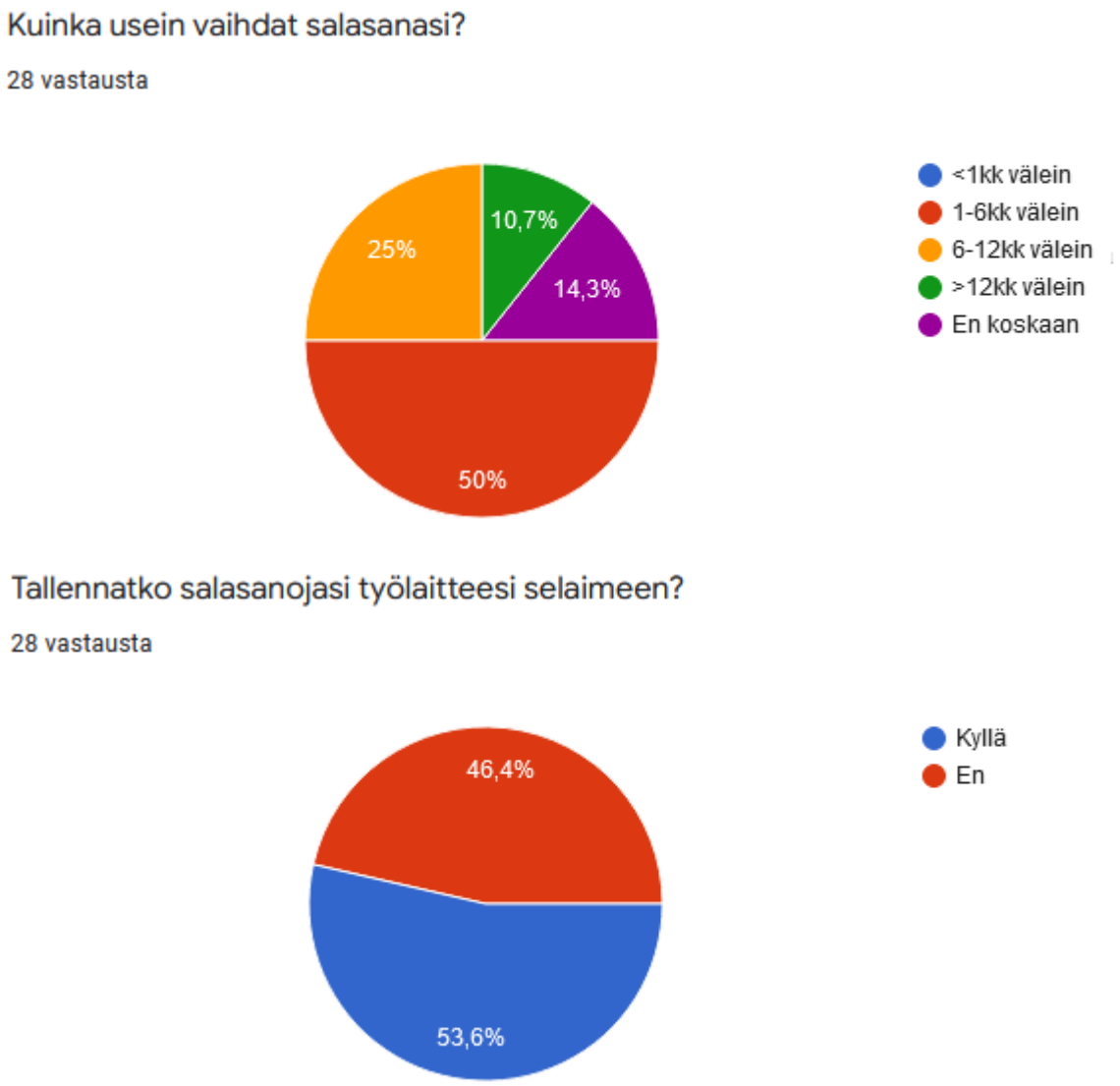
Kuvio 18. Salasanojen toistuvuus

Seuraavaksi selvitettiin, vastaako vastaajan käyttämät salasanat yrityksen määrittelemiä salasana-standardeja. (luku 5.2.6, kysymys 3.) Suurin osa vastanneista sanoi salasanojen olevan salasana-standardien mukaisia ja osa (14,3 %) vastanneista ei osannut sanoa.



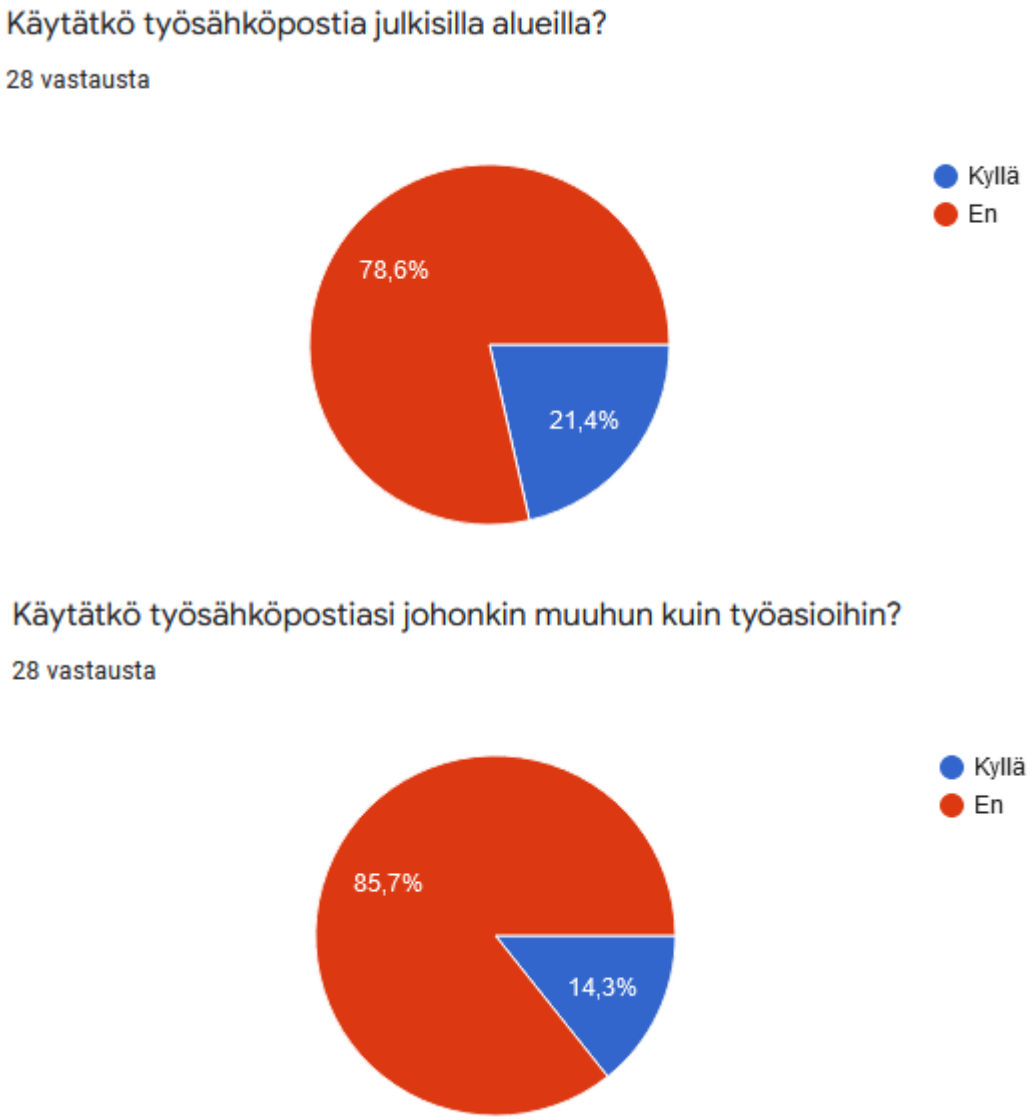
Kuvio 19. Salasanastandardit

Kuviosta 20 ilmenee, kuinka usein kyselyyn vastanneet vaihtaa salasanojaan. (luku 5.2.6, kysymys 4.) Vastanneista puolet vaihtaa salasanaansa 1—6 kuukauden välein, neljäsosa 6–12 kuukauden välein, 14,3 % ei vaihda koskaan ja 10,7 % useimmillaan kerran vuodessa. Vastanneista yli puolet (53,6 %) myös vastasivat tallentavansa salasanoja työkoneensa selaimeen.



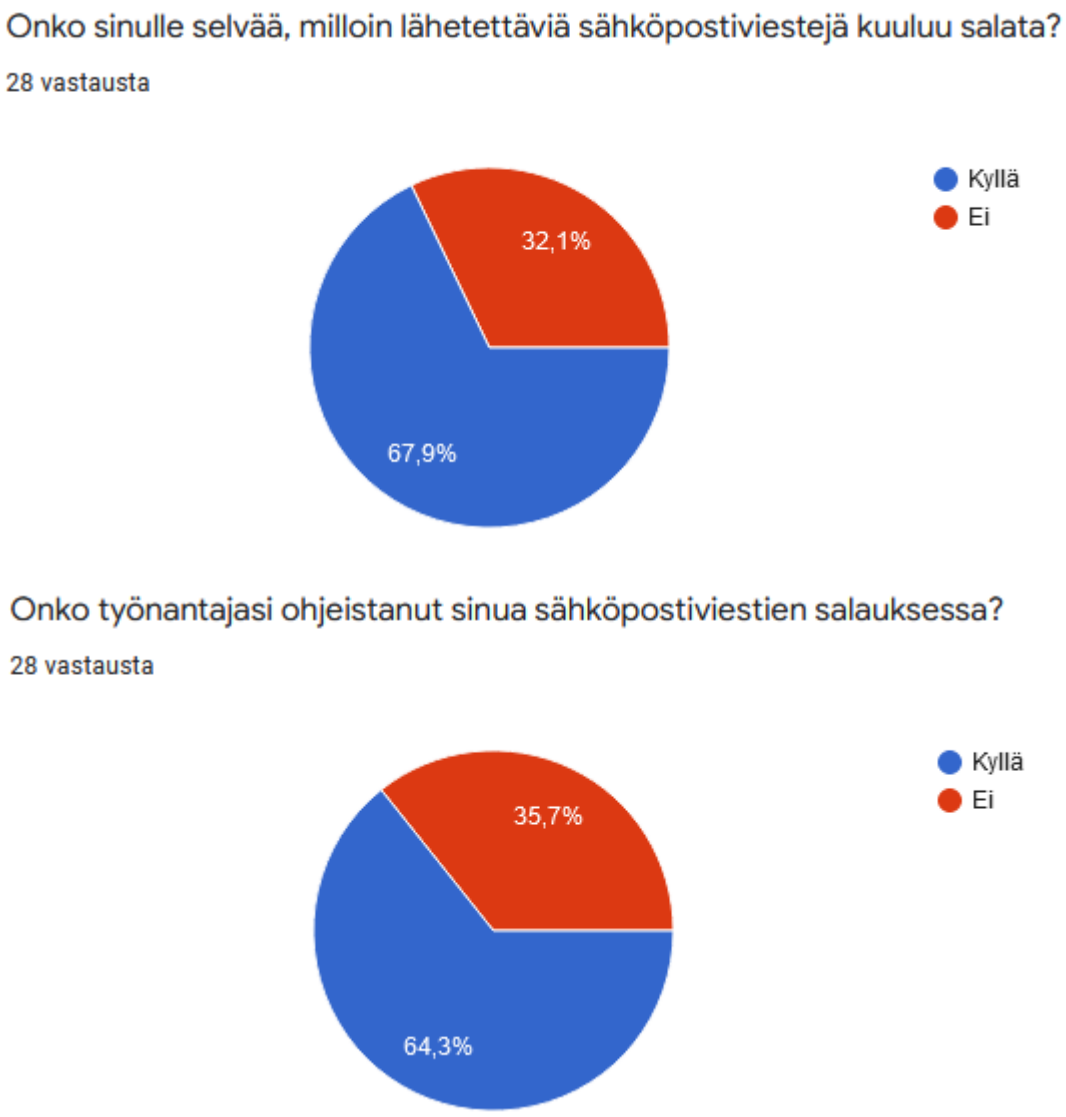
Kuvio 20. Salasanojen vaihto ja tallennus

Seuraavassa kohdassa kysyttiin, käyttääkö vastaaja työsähköpostia julkisilla alueilla ja johonkin muuhun, kuin työasioihin. (luku 5.2.7, kysymykset 1 ja 2.) Kuviosta 21 nähdään, että valtaosa (78,6 %) vastaajista ei käytä työsähköpostia julkisilla alueilla. Pieni osa (14,3 %) vastaajista käyttää työ-sähköpostia myös työasioiden ulkopuolella.



Kuvio 21. Työsähköpostin käyttäminen

Tieto siitä, että milloin lähetettäviä sähköpostiviestejä kuuluu salata, oli selvää suurelle osalle (67,9 %) vastanneista. Työnantajan vastattiin suurimmaksi osaksi (64,3 %) ohjeistaneen sähköpostiviestien salauksessa, kuten kuviosta 22 ilmenee. (luku 5.2.7, kysymykset 3 ja 4.)

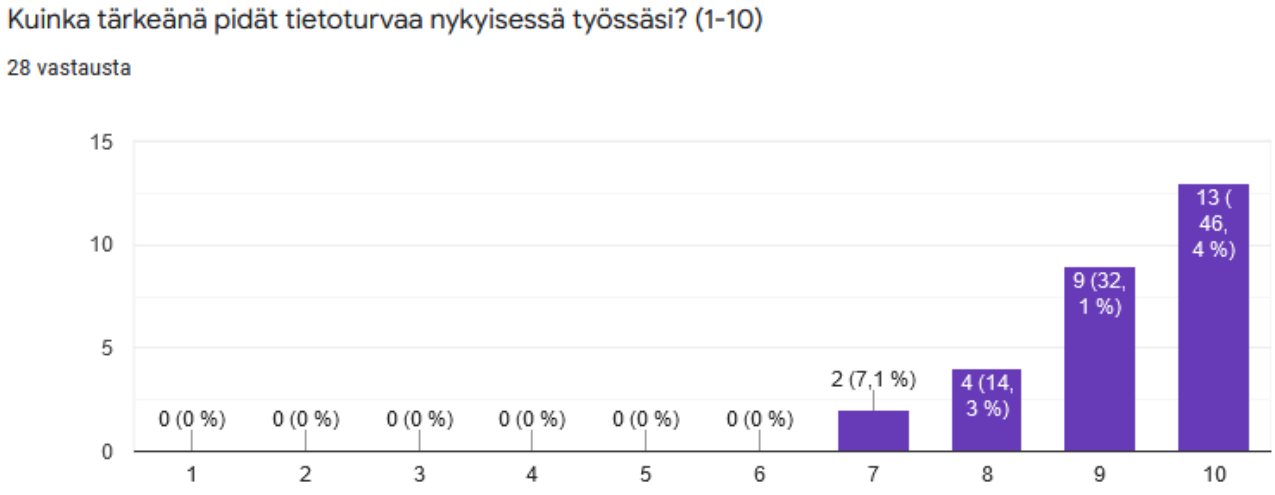


Kuvio 22. Sähköpostiviestien salaaminen

Seuraavaksi selvitettiin, kokeeko vastaaja etä- vai lähityön riskialttiimpana. (luku 5.2.8, kysymys 1.) Kuviosta 23 nähdään, että jako oli kohtuullisen tasainen. Suurin osa (42,9 %) vastasi, ettei etätyöt ole yhtään lähityötä riskialttiimpaa. Vastanneista 32,1 % kuitenkin kokee etätyöskentelyn olevan tietoturvan näkökulmasta riskialttiimpaa, 21,4 % kokee molemmat työskentelytavat yhtä riskialttiina ja 3,6 % ei osannut sanoa.

Kuvio 23. Työskentelymetodien riskit

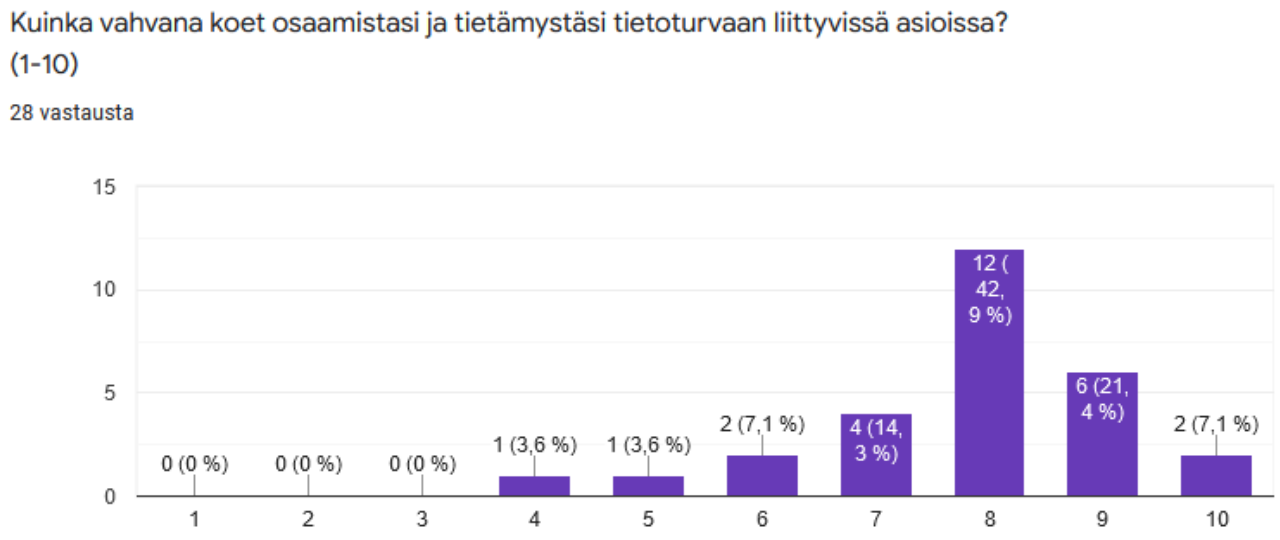
Seuraavassa osiossa vastaajan kuului arvioida tietoturvan tärkeyttä nykyisessä työssään. (luku 5.2.8, kysymys 2.) Kysymykset olivat väliltä 1: en ollenkaan tärkeänä ja 10: erittäin tärkeänä. Kuten kuviosta 24 voi todeta, vastaajista valtaosa (78,6 %) vastasi vaihtoehdolla 9—10 ja vastausten keskiarvo oli 9,17. Kyselyyn vastanneet pitivät siis tietoturvaa erittäin tärkeässä roolissa nykyisessä työssään.



Kuvio 24. Tietoturvan tärkeys

Tämän jälkeen vastaajia pyydettiin arvioimaan omaa tietoturvaosaamista ja -tietämystä. (luku 5.2.8, kysymys 3.) Kysymykset olivat välillä 1: erittäin heikkona ja 10: erittäin vahvana. Enemmistö

(42,9 %) vastasi numerolla 8, eli hyvä tietoturvaosaaminen ja tietämys. Vastauksien keskiarvo oli 7,82, vaikka vastauksissa oli selkeää hajontaa, kuten kuviosta 25 ilmenee.



Kuvio 25. Tietoturvaosaamisen itsearviointi

Kyselyn viimeisessä pakollisessa osiossa kysyttiin, että kokeeko vastaaja tarvitsevansa ohjeistusta työnantajalta tietoturvaan liittyvissä asioissa. (luku 5.2.8, kysymys 3.) Vastaajista suurin osa (64,3 %) vastasi, ettei koe tarvitsevansa ohjeistusta, mutta kuitenkin 10 vastaajaa (35,7 %) vastasi tarvitsevansa apua tietoturvaan liittyvissä asioissa työnantajaltaan. (Kuvio 26.)

Kysymykseen ”Kyllä”-vaihtoehdon valinneiden työalat jakaantuivat seuraavasti: 6 IT-ala, 2 kauppa ja hallinto, 1 terveys ja hyvinvointi, 1 tekniikka ja teollisuus. Puolustusvoimilla työskentelevistä jokainen vastasi, ettei koe tarvitsevansa ohjeistusta työnantajaltaan tietoturva-asioissa.

Kuvio 26. Tietoturvakoulutuksen tarpeen arviointi

7 Tulosten yhteenveto

7.1 Haastattelut ja verkkokysely

Molemmista tutkimusmenetelmistä saadut tulokset olivat hyvin samankaltaisia. Haastatteluja tutkimukseen saatiin kolme kappaletta. Haastattelu lisättiin tutkimusmenetelmäksi verkkokyselyn lisäksi, jotta saataisiin enemmän tutkimusaineistoa. Ennen haastatteluja ja verkkokyselyä toteutettiin kyselyn demonstraatio muutamalle kohdeyrityksen työntekijälle mahdollisten ongelmakohtien löytämiseksi. Testikyselyn seurauksena kysymyksiä lisättiin, muokattiin ja niiden järjestystä kyselyssä muutettiin.

Teemahaastattelussa käytettiin pääasiassa samoja kysymyksiä kuin verkkokyselyssä, mutta haastattelun kulku oli avoimempaa. Haastatteluiden pääteemat olivat samoja, mutta joissain haastatteluissa tietyt kysymykset nostivat esiin lisää kysymyksiä joko haastattelijalta tai haastateltavalta.

Verkkokyselyllä saatiin tuloksiin käytettäviä vastauksia 28 henkilöltä. Jotta tutkimustulokset olisivat yleistettävissä kohderyhmässä, olisi otoksen ollut hyvä olla suurempi. Vastauksissa oli osittain paljon vaihtelua, mutta kyselyn vapaissa kysymyksissä nähtiin reilusti yleistettäviä vastauksia.

7.2 Ilmenneet tietoturvaongelmat

Tutkimuksen yhteydessä havaittiin useita työntekijöistä johtuvia tietoturvariskejä, joita käsitellään tässä luvussa. Hallinnollinen-, henkilöstö- ja käyttöturvallisuus ovat täysin työnantajan vastuulla, eikä niihin perehdytä hallinnollisen turvallisuuden lisäksi. Työnantajien tarjoama ohjeistus tietoturvalliseen etätyöhön oli ollut vähäistä ja tietoturvakoulutusten taso näytti olevan heikkoa osalla verkkokyselyyn ja haastatteluun osallistuneista henkilöistä.

7.2.1 Hallinnollinen turvallisuus

Henkilötietoja käsittelevistä henkilöistä neljännes ei ollut ikinä osallistunut GDPR koulutukseen, eikä 37,5 % osannut kuvailla tietosuojaa tai sen merkitystä. Myös 37,5 % piti mahdollisuutena ulkopuolisten nähdä heidän työlaitteilleen etätöiden aikana ja näistä vastaajista kolmasosa ei käytä

näytön tietosuojakalvoa. Henkilötietoja käsittelevistä vastaajista 43,7 % ei tiennyt milloin sähköpostiviestejä kuuluu salata, vaikka ne sisältäisivät esimerkiksi arkaluonteista tietoa yrityksestä, tai asiakkaiden henkilötietoja.

7.2.2 Fyysinen- ja tietoaineistoturvallisuus

Verkkokyselyyn ja haastatteluihin vastanneista n. 20 % työskentelee julkisilla alueilla. Näistä vastanneista jokainen käy työhön liittyviä puhekeskusteluja julkisilla paikoilla ja 67 % ei käytä näytön tietosuojakalvoa. Puolet näistä vastanneista lukitsee työlaitteensa, kun se jätetään valvomatta. Julkisia verkkoja käyttää vain 1 tutkimukseen osallistunut henkilötietoja käsittelevä henkilö ja tämä henkilö käyttää VPN-yhteyttä satunnaisesti.

Kukaan tutkimukseen osallistunut ei käytä julkisessa käytössä olevia tulostimia tulostamaan työhön liittyviä tiedostoja. Kolmasosa vastanneista ei lukitse tietokonetta, kun se jätetään valvomatta, mutta kaikilla työlaite on kuitenkin suojattu tavalla tai toisella. (ks. Kuvio 11). Neljännes vastanneista joko tiesi tallennuslaitteen olevan salaamaton, tai ei ollut varma salauksesta. Puolet näistä vastanneista käsittelee työssään henkilötietoja ja yksi vastannut työskentelee lisäksi julkisilla alueilla.

7.2.3 Ohjelmisto- ja tietoliikenneturvallisuus

Lähes puolet vastanneista (45,1 %) on saanut ohjeistusta laitteen päivittämisestä työnantajaltaan ja enemmistö (83,8 %) käyttää virustorjuntaohjelmaa työkoneellaan. Vastanneista n. 20 % ei ole vaihtanut etätyössä käytettävän reitittimen oletussalasanaa ja 6,5 % ei ollut varmoja tai tietoisia. VPN-yhteyttä ei tutkimuksen mukaan käyttänyt kun 16,1 % henkilöistä tehdessään etätöitä ja toiset 16,1 % käytti sitä satunnaisesti.

7.3 Parannusehdotuksia

Ilmenneiden tietoturvaongelmien perusteella voidaan todeta, että paras ratkaisu olisi lisätä tietoturvakoulutusten määrää ja asettaa ne pakollisiksi kaikille työntekijöille. Kaikista tutkimukseen osallistuneista henkilöistä kolmasosa kokee tarvitsevansa työnantajaltaan ohjeistusta tai koulutusta tietoturvalliseen etätyöskentelyyn ja n. 80 % näistä henkilöistä käsittelee työssään henkilötietoja.

Mikäli yritys käsittelee EU:n sisällä asuvien yksilöiden henkilötietoja, kuuluu yrityksen tarjota työntekijöilleen GDPR- ja tietosuojakoulutusta. Tietosuojakouluttaminen tulisi toteuttaa varsinkin niille ryhmille, jotka käsittelevät työssään arkaluontoisia henkilötietoja. Koko organisaation kouluttamisella voidaan myös vähentää yleistä riskitasoa ja parantaa yleistä tietosuojan kulttuuria. (Silvola 2018.)

Etätyössä on työntekijän vastuulla huolehtia omasta ja yrityksen tietoturvallisuudesta. Työnantajan olisi syytä ohjeistaa julkisilla alueilla työskenteleviä työntekijöitä käyttämään esimerkiksi salattuja verkkoja, näytön suojakalvoa, virustorjuntaohjelmaa ja levyn salausta, varsinkin jos työntekijä käsittelee arkaluonteisia tietoja. Tietosuojalaki ja -asetus koskee kaikkia tahoja, jotka ovat tekemisissä henkilötietojen kanssa niin kuluttaja-, kuin yrityssektorilla. (Ronkainen n.d.)

Tietoturva-, ja tietosuojakouluttamisen lisäksi olisi suotavaa testata työntekijöiden tietoturvaosaamista esimerkiksi tietojenkalastelu- (engl. *phishing*) tai GDPR-harjoituksilla. Myös laajemmalla tietoturvaharjoituksella saataisiin kartoitettua suurimpia työntekijöistä johtuvia tietoturvariskejä. Tietoturvatestauksen avulla voisi nähdä todellisen syyn, minkä takia tietoturvakoulutusta kuuluisi lisätä työntekijöille.

Etätöiden tietoliikenneturvallisuutta voi parantaa käyttämällä VPN-yhteyttä töiden tekemiseen ja käyttämällä vain salattuja, tai yksityisiä verkkoja. On myös tärkeää huolehtia reitittimen päivittämisestä ja suojaamisesta. (Valtori 2020). Puolustusvoimien työntekijä ja IT-alan ammattilainen sanoi haastatteluissa 1 ja 2, ettei pysty tekemään töitään ilman VPN-yhteyttä. Näin saadaan luotua erittäin tietoturvallinen ratkaisu etänä työskentelyyn.

Työlaite on tärkeä asetella niin, ettei muilla ole mahdollisuutta nähdä sillä olevia tietoja, niin kotitoimistolla kun julkisillakin alueilla. Työlaitteet olisi syytä suojata suojakoodilla, automaattisella näytönlukituksella ja tallennuslaitteen salauksella. Työlaitteella suositellaan käytettäväksi virustorjuntaohjelmaa sekä päivittämään se aina uusimpaan versioon. Sovelluksia työlaitteelle suositellaan asennettavaksi vain luotetuista paikoista ja niistäkin harkiten. Etätyötä tekevä vastaa itse käytössään olevista ulkoisista tallennuslaitteista, joten tämäkin olisi syytä salata. (Siunsote 2020, 16.)

8 Johtopäätökset

Määritettyihin tutkimusongelmiin (luku 4.2) saatiin vastaukset. Useat tietoturvariskit johtuvat tutkimustulosten mukaan selkeästi työntekijöiden tietämättömyydestä tai piittaamattomuudesta. Haastatteluiden ja verkkokyselyn perusteella henkilöt, jotka esimerkiksi käsittelevät ulkopuolisen seurassa arkaluontoista tietoja tai kävivät työhön liittyviä puheluja, tiesivät niiden aiheuttavan omia tietoturvariskejä. Etätyössä työntekijän vastuu tietoturvasta kasvaa huomattavasti, eikä tätä moni tutkimukseen osallistunut ollut ymmärtänyt.

Vastanneiden työalalla oli selkeästi vaikutusta tutkimustuloksissa. IT-alalla ja puolustusvoimilla työskenteleville tietoturvakysymykset eivät juurikaan tuottanut vaikeuksia ja muille ne pääasiassa tuotti. Osa vastanneista koki tarvitsevansa koulutusta turvalliseen etätyöskentelyyn, mutta työntekijät eivät välttämättä sitä osaa, tai uskalla pyytää. Työnantajat ovat tarjonneet heikosti tietoturva-, ja tietosuojakoulutusta työntekijöilleen ja eniten huolta aiheutti niiden henkilöiden tietoturva-osaaminen, jotka käsittelevät työssään henkilötietoja sillä tietosuoja-asetus ja -laki koskee myös yksityishenkilöitä.

Olisi suotavaa luoda pakolliseksi tietoturvakoulutukset kaikille työntekijöille ja lisäksi tietosuojakoulutukset henkilötietoja, tai muita arkaluonteisia tietoja käsitteleville työntekijöille. Yrityksessä olisi suotavaa myös ohjeistaa yleisiä etätyöstä aiheutuvia tietoturvariskejä ja tapoja välttää niitä.

Toimeksiantajan lausunnon mukaan tutkimustulokset vahvistivat näkemystä säännöllisen tietoturvakouluttamisen tarpeesta. Tutkimusaineistoa ja otosta kasvattamalla olisi voinut saada kasvatettua tutkimuksen luotettavuutta, mutta tuloksia voidaan toimeksiantajan mielestä pitää suhteellisen luotettavina. Toimeksiantaja ryhtyy toimenpiteisiin korjatakseen tutkimuksessa selvinneet ongelmakohdat, kuten työntekijöiden tietoturva- ja tietosuojakäytäntöjen puute ja näihin kohdistunut piittaamattomuus. Tutkimuksesta voi jatkokehittää yritykselle tarkastelukriteeristön, jota yritys voi käyttää työkaluna tietoturvallisen etätyöskentelyn saavuttamiseksi.

9 Pohdinta

Opinnäytetyön aihe on erittäin laaja ja sen rajaaminen tuotti paikoittain ongelmia. Otannan valitseminen tutkimukseen oli yksi näistä tapauksista, sillä otannan rajaus vain kohdeyritykseen työntekijöihin olisi vaikeuttanut tutkimustulosten yleistettävyyttä pienen määrän takia. Realististen tutkimustulosten saamiseksi otos valittiin eri yrityksistä ja työaloilta. Työssä vastattiin tutkimuskysymyksiin ja tutkimuksen kaikkiin tavoitteisiin päästiin.

Tutkimuksen luotettavuuden arviointi tehdään validiteetin ja reliabiliteetin näkökulmista. Ulkoinen validiteetti liittyy saatujen tulosten yleistettävyyteen, eli kuinka hyvin tulokset toistuvat vastaavissa ilmiössä tutkimuksen ulkopuolella. (Kananen 2015, 347). Tutkimukseen valittu otos on pieni, mutta se on valittu oikein halutusta kohderyhmästä, siksi koen tutkimustulosten olevan siirrettävissä ja yleistettävissä tähän kohderyhmään. Toimeksiantajan kanssa koimme tutkimuksen keskittyneen oikeisiin asioihin ja vastanneen niihin kysymyksiin, joihin siinä oli tarkoitus.

Reliabiliteetti taas liittyy tutkimustulosten pysyvyyteen, jos tutkimus uusittaisiin. (Kananen 2015, 349). Tutkimuksen ilmiöt, etätyö ja tietoturva ovat molemmat vanhoja sekä epästabiileja ilmiöitä. Etätyöt ovat yleistyneet koronapandemian seurauksena ja nyt etätyösuosituksen poistuessa etätyötä tekevien henkilöiden määrä todennäköisesti laskee. Tietoturvakin on jatkuvasti kehittyvä alue, mutta tutkimuksessa todetut etätyön tietoturvariskit eivät kuitenkaan ole aikaan sidonnaisia, vaan samat riskit ovat mahdollisia tulevaisuudessakin. Tutkimukseen osallistuneiden henkilöiden työaloilla oli suuri vaikutus tuloksiin ja tämä pitäisi ottaa huomioon tutkimusta uusittaessa.

Tutkimustulokset osoittivat etätyön itsessään olevan työskentelymenetelmänä turvallinen ja siihen kohdistuneet riskit lähtöisin pääasiassa työntekijässä, joten työnantajan on siis erittäin tärkeää tarjota työntekijöille tietoturvakoulutusta, tai -ohjeistusta tietoturvalliseen etätyöhön. Tietoturvastandardin, tai -standardien käyttöönotto voisi olla myös pienemmille yrityksille suotavaa, sillä niiden avulla yritys saisi suoraan ohjeistusta yleisen tietoturvatason kasvattamiseksi.

Mikäli toteuttaisin työni uudelleen, miettisin verkkokyselyn kysymyksiä uudelleen ja lisäisin mahdollisesti kysymyksiä tietoturvastandardeista ja toisin esiin niiden hyödyn tietoturvariskien välttämisessä. Toteuttaisin myös verkkokyselyn vasta haastatteluiden jälkeen, sillä haastattelut olisivat

voineet auttaa parempien kysymyksien laatimisessa. Tutkimuksen lisäksi loisin myös auditointikriteeristön tietoturvallisesta etätyöstä kehitystyönä kohdeyritykselle, jota voisi mahdollisesti käyttää myös muissa yrityksissä. Uskon etätyön tietoturvahaasteista löytyvän aihetta myös tuleviin opinnäytetöihin.

Lähteet

Allen, B. 2021. CIA-kolmikko. Julkaistu 15.10.2021. Viitattu 24.03.2022. https://gocoding.org/fi/cia-triad/.

Anttila, T. 2020. Tietoturva ja tietosuoja etätyössä. Päivitetty 25.11.2020. Viitattu 24.04.2022. https://tilitoimistossa.taloushallintoliitto.fi/toimintamallit-ja-tyokalut/tietoturva-ja-tietosuoja-etatyossa

Eurofound. 2020. Living, working and COVID-19. Viitattu 23.03.2022. https://www.eurofound.europa.eu/sites/default/files/ef_publication/field_ef_document/ef20058en.pdf.

F-Secure. N.d. 8 tietoturvavinkkiä etätyön suojaamiseen. Viitattu 20.04.2022. https://www.f-secure.com/fi/home/articles/8-cyber-security-tips-for-remote-work.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Jyväskylä: Jyväskylän ammattikorkeakoulu. Viitattu 03.05.2022.

Karhula, T. 2020. Millainen on hyvä salasana ja kuinka usein se tulisi vaihtaa? Julkaistu 12.05.2020. Viitattu 21.04.2022. https://wisdomic.fi/millainen-on-hyva-salasana-ja-kuinka-usein-se-tulisi-vaihtaa/

Kyberturvallisuuskeskus. 2020a. Tietoturva. Julkaistu 09.08.2020. Viitattu 22.03.2022. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva.

Kyberturvallisuuskeskus. 2020b. Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa 2020. Viitattu 07.04.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Automaatiolaitekartoitus_2020.pdf.

Kyberturvallisuuskeskus. 2020c. Neuvoja salasanan hallintasovelluksen käyttöönottoon. Päivitetty 30.09.2021. Viitattu 21.04.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/neuvoja-salasanan-hallintasovelluksen-kayttoonottoon.

Lindberg, M. 2022. Etätyö tietohallinnon, tietoturvan ja tietosuojan näkökulmasta. Julkaistu 20.02.2022. Viitattu 23.03.2022. https://www.opsec.fi/fi/2020/02/20/etatyo-tietohallinnon-tietoturvan-ja-tietosuojan-nakokulmasta/.

Multisilta, V. 2021. Hybridityö on tullut jäädäkseen. Julkaistu 25.08.2021. Viitattu 07.04.2022. https://insinoori-lehti.fi/tasta-on-kysymys/hybridityo-on-tullut-jaadakseen/.

Päivärinta, E. 2020. Tietoturvan riskitason määrittäminen Android-laitteissa sovellusten ohjelmointirajapintaa käyttäen. Oulun yliopisto, tieto- ja sähkötekniikan tiedekunta, tietotekniikka. Julkaistu 17.03.2020. Viitattu 19.04.2022. http://urn.fi/URN:NBN:fi:oulu-202003171271.

Rantalainen, T. 2018. Yksinkertaiset ohjeet yksinkertaisen salasanan parantamiseksi. Julkaistu 22.11.2018. Viitattu 21.04.2022. https://blog.f-secure.com/fi/yksinkertaiset-ohjeet-yksinkertaisen-salasanan-parantamiseksi/.

Ronkainen, K. N.d. Miten tietosuoja-asetus ja -laki vaikuttavat käytännössä? Viitattu 12.04.2022. https://www.aeondigital.fi/blogi/tietosuojalaki-kaytannossa/.

Salonen, A. 2022. Etätyö on lisääntynyt räjähdysmäisesti – näillä aloilla on eniten avoimia etätyö-paikkoja. Julkaistu 05.01.2022. Viitattu 25.03.2022. https://duunitori.fi/tyoelama/etatyo-avoimet-tyopaikat.

Silvola, V. 2018. Henkilökunnan koulutus osana GDPR:ään valmistautumista. Julkaistu 04.01.2018. Viitattu 28.04.2022. https://blog.wakaru.fi/2018/01/04/henkilokunnan-koulutus-osana-gdpraan-valmistautumista/

Siunsote. 2020. Tietoturva- ja tietosuojakäsikirja. Julkaistu 15.05.2020. Viitattu 28.04.2022. https://www.siunsote.fi/documents/393252/6561097/Tietoturva-+ja+tietosuojak%C3%A4si-kirja+opiskelijoille+%28PDF%29.pdf/25ecbb2d-b5c3-6ad2-d434-45ee68add538

Sosiaali- ja terveysministeriö. 2022. Etä- ja läsnätyön yhdistäminen. Päivitetty 02.03.2022. Viitattu 27.03.2022. https://stm.fi/etatyot-koronavirustilanteessa.

Tietosuoja. N.d. Erityisten henkilötietoryhmien käsittely. Viitattu 25.03.2022. https://tieto-suoja.fi/erityisten-henkilotietoryhmien-kasittely.

Turvaposti. N.d. Salaamaton sähköposti on tietoturvaltaan kuin postikortti. Viitattu 23.04.2022. https://www.turvaposti.fi/index.php?act=why

Työsuojelu. 2020. Etätyö. Päivitetty 15.09.2020. Viitattu 20.04.2022. https://www.tyosuojelu.fi/ty-oolot/tyoymparisto/etatyo.

Työterveyslaitos. N.d. Etätyö, hybridityö ja monipaikkainen työ. Viitattu 20.04.2022. https://www.ttl.fi/teemat/tyoelaman-muutos/etatyo-hybridityo-ja-monipaikkainen-tyo.

VAHTI. 2002. Valtionhallinnon etätyön tietoturvallisuusohje. Viitattu 23.03.2022. https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2002.pdf.

Valtori. 2020. Vinkkejä tietoturvalliseen etätyöhön. Julkaistu 23.03.2020. Viitattu 20.04.2022. https://valtori.fi/-/vinkkeja-tietoturvalliseen-etatyohon.

Liitteet

Liite 1. Verkkokyselyn saateteksti

Tämä kysely on luotu osana opinnäytetyötä ”Tietoturvallinen etätyö”, joka toteutetaan Jyväskylän ammattikorkeakoulussa. Opinnäytetyössä pyritään selvittämään etätyön aiheuttamia tietoturvariskejä ja mahdollisia tapoja välttää ne.

Kysely kohdistuu vain henkilöille, jotka työskentelevät, tai ovat työskennelleet etänä. Jotta tutkimustuloksia voidaan pitää luotettavina, toivotaan mahdollisimman monen henkilön osallistuvan kyselyyn ja vastaamaan kysymyksiin rehellisesti. Kyselyyn vastataan täysin nimettömästi ja tutkimusaineiston käyttö on rajattu vain tähän kyseiseen tutkimukseen. Kysymysten määrä on vastauksista riippuen joko 32, tai 36 kysymystä ja vastaamiseen kuluu aikaa noin 15 minuuttia. Kyselyn vastausaika on rajattu välille 8.4.2022-15.4.2022.

Kiitos jo etukäteen kyselyyn osallistumisesta!

Ville Veijanen