Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2024

Oona Virta

Tutkimus yrityksen henkilöstön tietoturvatietämyksestä

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

Opinnäytetyö (AMK) | Tiivistelmä

Turun ammattikorkeakoulu

Tieto- ja viestintätekniikka

2024 | 49 sivua

Oona Virta

Tutkimus yrityksen henkilöstön tietoturvatietämyksestä

Tietoturvan tärkeys on noussut selvästi nyky-yhteiskunnassa, ja nykyään kaikkien alojen yritysten henkilöstöllä pitää olla ymmärrystä tietoturvan tärkeydestä ja siitä, mitä se käytännössä tarkoittaa. Tärkeää on myös henkilöstön oikeanlainen koulutus tietoturvaan ja yrityksen käytäntöihin tietoturvauhka tilanteiden varalta.

Tämän opinnäytetyön tarkoituksena oli selvittää yrityksen henkilöstön tietämys tietoturvasta ja sen tärkeydestä. Opinnäytetyössä perehdyttiin yrityksessä voimassa oleviin ohjeistuksiin ja koulutuksiin.

Yrityksen henkilöstölle toteutettiin verkkokysely, joka sisälsi kysymyksiä yrityksen koulutuksista, ohjeistuksista ja normaaleista tietoturvakäytännöistä. Tulosten perusteella henkilöstöllä on kohtuullisen hyvä käsitys yrityksen tietoturvasta, ja siitä mitä se käytännössä tarkoittaa.

Löydetyt heikkoudet johtuivat enimmäkseen henkilöstön heikosta kouluttamisesta. Jatkotoimenpiteeksi luotiin suunnitelma koulutuksen päivittämisestä. Koulutukset tullaan jatkossa kääntämään myös ruotsiksi.

Opinnäytetyön ansiosta yrityksen on helppo lähteä kehittämään koulutuksiaan ja yritys sai tarkan kuvan henkilöstönsä tietoturva tasosta.

Asiasanat:

tietoturva, tietosuoja, koulutus, yritys

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information and Communications Technology

2024 | 49 pages

Oona Virta

A Study on the company’s staff’s cybersecurity knowledge

This thesis purpose was to figure out company’s staff’s knowledge regarding cybersecurity and the importance of it. In the thesis we will orientate in company’s information security and data protection policies, training of those and the trainings comprehensives.

A web survey was made to the company’s staff that included questions about company’s information security training, information security and data protection policies and of normal information security practices. The survey was separated to company’s four different business operation areas so that we can achieve the most precise knowledge about staff’s knowledge. Based on the results staff has a reasonably good understanding for company’s information security and what that means in practice.

The found weaknesses mainly arise from staff weak training, so the plan will be to update the existing training. In future the training will be also translated to Swedish.

The thesis study was success and the company got precise information about staff’s information security knowledge and they can now easily start improving existing trainings.

Keywords:

information security, data protection, training, company

Sisältö

Liitteet

Liite 2. Tietoturvakyselyn tulokset

Kuviot

1 Johdanto

Tietoturva on nykymaailman yksi tärkeimmistä asioista, josta jokaisen pitää ymmärtää edes jotain. Työmaailmassa yritykset käsittelevät arkaluontoisia dokumentteja, kuten henkilötietoja ja yrityksen omia dokumentteja. Tämän takia on hyvin tärkeää, että yrityksen henkilöstö ymmärtää tietoturvan tärkeyden ja osaa tehdä työnsä sitä noudattaen. Tärkeää on myös henkilöstön oikeanlainen kouluttaminen tietoturvauhkia vastaan.

Tämän opinnäytetyön tarkoituksena on perehtyä toimeksiantajan, suomalaisen palveluyhtiön, henkilöstön tietämykseen tietoturvasta. Tietoturvauhat liittyvät nykyään useammin ihmiseen ja ihmisen piittaamattomuuteen. Yrityksissä onkin tärkeää saada ihmiset eli henkilöstö ymmärtämään tietoturvaa ja noudattamaan sitä. (Järvinen 2022, 32.) Opinnäytetyöllä yritetään saada vastaus siihen, millä tasolla henkilöstön tietämys on.

Henkilöstön tietämyksen taso selvitetään henkilöstölle toteutettavalla kyselyllä. Kyselyn avulla on tarkoitus myös selvittää, onko yksi koulutus riittävä kaikille liiketoiminta-alueille vai tarvitseeko joillakin liiketoiminta-alueilla olla omat koulutuksensa. Yrityksen neljä liiketoiminta-aluetta on: asiakaspalvelu, ICT, tietoliikenne ja hallinto.

Aiheesta on tehty erilaisia tutkimuksia ja opinnäytetöitä aikaisemminkin. Aiheesta löytyy myös kirjallisuutta, kuten Petteri Järvisen Yrityksen tietoturvaopas vuodelta 2022, jossa käydään läpi kirjoittajan pitämiä tietoturvakoulutuksia 20 vuoden ajalta ja kerrotaan tietoturvaan liittyvistä vaaroista ja uhista. Kirjasta saadaan viitteitä siihen, millainen yrityksien tietoturvan kannattaisi olla.

2 Tietoturva ja tietosuoja

2.1 Tietoturva

Kyberuhat ja tietojenkalastelut ovat tämänpäiväisessä maailmassa arkisia asioita ja jokaisen pitäisi olla tietoinen, miten kyberuhan tunnistaa ja mitä sellaisen kohdatessaan pitäisi toimia. Tätä asiaa kutsutaan tietoturvaksi, ja sen merkitys on suuri pienien kuin suurienkin yrityksien toiminnassa (Jurvanen 2024). Tietoturvan tärkeyden ymmärtäminen on suuri asia tämänpäiväisessä yhteiskunnassa, ja jokaisen pitäisi ymmärtää omien tietojensa tärkeys. Vaikka moni voi ajatella, että heillä ei ole mitään arkaluonteisia tietoja, näin ei kuitenkaan ole. Yrityksissä pitää osata ymmärtää yrityksien tietojen tärkeys ja se, että henkilöstön teot vaikuttavat siihen, että tieto ei joudu kyberuhkien kohteeksi. Yrityksen koolla ei ole väliä, koska jokaisessa yrityksessä on rahanarvoisia tietoja suojattavana. (Järvinen 2022, 32.)

Yrityksien datan suojaamiseksi on kehitetty lainsäädäntöjä, joita yritysten on noudatettava. Näistä ainakin GDPR-asetus ja NIS2-direktiivi ovat lakisäädöksiä, jotka koskevat toimeksiantajaa. Toimeksiantajan ohjeistuksissaan mainitaan, että yrityksen tietoturvapolitiikka ja ohjeistukset myötäilevät näitä lakisäädöksiä.

2.2 NIS2 – EU:n kyberturvallisuusdirektiivi

NIS2 (The Network and Information Security 2) -direktiivi on lainsäädäntö, joka koskee kyberturvallisuutta ja vaikuttaa EU:n jäsenvaltioita. Se on päivitetty versio vuonna 2016 otetusta EU:n kyberturvallisuussäännöistä. Kyberturvallisuussäännöt nykyaikaistettiin, jotta yhteiskunta voi jatkaa digitalisaation lisääntymistä ja kyberturvallisuuden laajentamista. (Europen Commission 2023.) Direktiivi astuu virallisesti voimaan lokakuussa 2024 ja on paljon tiukempi ja laajempi, kuin aikaisempi direktiivi. NIS2:n laajuus näkyy siitä, että yrityksien täytyy pitää huolta koko toimitusverkostaan, ja suojata ja valvota

sitä tietoturvauhilta. Yritysten on myös ilmoitettava tietosuojaloukkauksesta ennakkovaroitus 24 tunnin sisällä. (Luoma 2024.)

2.3 Tietosuoja-asetus GDPR

Tietosuoja on jokaisen ihmisen perusoikeus, ja sen tarkoituksena on turvata henkilön oikeuksien ja vapauksien toteutumisen hänen henkilötietojensa käsittelyssä (Tietosuojavaltuutetun toimisto n.d.).

GDPR (General Data Protecting Regulation) eli yleinen tietosuoja-asetus koskee EU:ssa kaikkia yrityksiä ja organisaatioita, jotka keräävät millään tavalla henkilödataa. Henkilödata on tietoa, jolla henkilö voidaan tunnistaa tai on tunnistettavissa. Henkilödataan kuuluu esimerkiksi nimi, osoite ja IP-osoite. (Europa 2022.)

GDPR määrittelee yhteiset säännöt jokaiselle yritykselle tai organisaatiolle, joka käsittelee henkilötietoja. Sääntöihin kuuluu esimerkiksi se, että yrityksessä on oltava tietosuojavastaava, jos yritys käsittelee tietoja laajasti. Samalla GDPR vahvistaa olemassa olevia oikeuksia käyttäjille, ja lakiasetus auttaa käyttäjiä hallitsemaan henkilötietojaan paremmin. Lakiasetus sisältää käyttäjille esimerkiksi helpomman pääsyn omiin tietoihinsa ja tiedon siitä, että miten kyseistä tietoa käsitellään. Käyttäjillä on oikeus myös siirtää tietonsa paikasta toiseen tai tulla unohdetuksi eli saada tietonsa poistetuksi järjestelmästä. (Euroopan parlamentin ja neuvoston asetus 2016/679/EU.)

3 Yrityksen tietoturvaohjeistus

3.1 Tietoturvapolitiikka

Yrityksellä on voimassa oleva tietoturvapolitiikka dokumentti, joka on saatavilla suomeksi ja on koko henkilöstön luettavissa. Ruotsiksi kyseistä dokumenttia ei ole saatavilla. Kyseinen dokumentti kattaa asiat tietoturvan tavoitteesta, sen ohjaavista tekijöistä, tietoturvan vastuualueista ja tietoturvarikkomusten seuraamuksista. Kyseisessä dokumentissa käydään läpi myös muita tietoturvapolitiikkaan liittyviä asioita, mutta niiden arkaluontoisuuden takia, niitä ei käydä läpi tässä opinnäytetyössä. (Toimeksiantajan ohjeistus 2023.)

Yrityksessä tietoturvallisuudella tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Näin ollen tietoturvallisella toiminnalla taataan organisaation toiminnan jatkuminen sekä normaalioloissa että poikkeustilanteissa. Ohjaavista tekijöistä dokumentissa mainitaan, että yrityksen tietoturvaa ohjaa kansalliset ja kansainväliset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Tietoturvavastuu on dokumentissa jaettu kolmeen osaan tietohallinnon, esihenkilöiden ja työntekijöiden välille. Näiden kolmen osan välillä jakautuu tehtävät, jotka koskevat tietoturvatyön organisoimista, virhetilanteessa kerätyn tiedon raportoimista, tiedotus tietoturvallisuuteen liittyvistä asioista ja havaittujen tietoturvauhkien ilmoittaminen. Tietoturvarikkomuksesta rikkomuksen tekijä saatetaan edesvastuuseen teostaan ja häntä vastaan ryhdytään rikkomuksen luonteen vaatimiin toimenpiteisiin. (Toimeksiantajan ohjeistus 2023.)

3.2 Tietosuojapolitiikka

Tietoturvapolitiikan lisäksi yrityksellä on voimassa oleva tietosuojapolitiikka, jossa kerrotaan henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteita ja menetelmiä yrityksessä. Kyseinen politiikka on suomeksi ja on

koko henkilöstön saatavilla helposti. Dokumenttia ei kuitenkaan ole saatavilla ruotsiksi. (Toimeksiantajan ohjeistus 2023.)

Tietosuojapolitiikassa on myös käyty läpi jokaisen vastuualueet ja tiedon oikeanlainen organisointi. Esihenkilöiden tehtävänä on raportoida omassa yksikössään kerätyt tiedot virhetilanteista tietohallintoon tai suoraan tietosuojavastaavalle. Esihenkilöillä on myös vastuu pitää huoli, että omat vastuualueen työntekijät tietävät ohjeiden ja velvoitteiden merkityksen ja mahdolliset seuraamukset. Itse työntekijöiden pitää huolehtia omalta osaltaan tietosuojaan liittyvistä asioista. Työntekijöillä on myös vastuu ilmoittaa kaikista havaituista tai epäilystä herättävistä tietosuojaan liittyvistä havainnoista tietosuojavastaavalle. (Toimeksiantajan ohjeistus 2023.)

Ohjeistuksessa on myös hyvin käyty läpi, mistä lainsäädännöistä ohjeistus koostuu ja miten tietosuojaa toteutetaan yrityksessä.

4 Tietoturvakoulutus

4.1 Tietoturvakoulutukset yleisesti

Tietoturvakoulutuksen tärkeys nyky-yhteiskunnassa on suuri, sillä sen avulla yrityksen tai organisaation henkilöstölle pystytään nopeasti kertomaan ja opettamaan yrityksen tai organisaation tietoturva-asiat. Vaikka monissa yrityksissä onkin nykyään tietoturvaohjelmistoja käytössä, jotka pitävät huolen siitä, että mitään ei toivottua ei järjestelmille tapahtuisi, on silti otettava huomioon inhimillinen tekijä. Ihminen on loppujen lopuksi se heikoin lenkki tietoturvassa ja monet tietoturvaloukkaukset johtuvat yleensä käyttäjän virheistä tai tietämättömyydestä. (Perttunen 2023.)

Tietoturvakoulutuksilla on siis tavoitteena minimoida nuo ihmisen tekemät virheet. Olkoon yritys sitten kuinka suuri tai pieni, on aina tilanteita, kun käyttäjä tekee jotain tietoteknisillä laitteilla. Ihmiset osaavat olla huolimattomia ja väsyneitä, jolloin heitä on helppo huijata. Tietoturvan tärkein tavoite yrityksessä pitäisi olla ihmisten kouluttaminen asian suhteen. (Järvinen 2022, 23.)

Pelkästään yksi hyvä tietoturvakoulutus ei kuitenkaan enää riitä, sillä tietoturva muuttuu ja kehittyy jatkuvasti. Samoin niitä kohtaan olevat uhat. Tämän takia tietoturvakoulutus on prosessi, joka vaatii jatkuvaa kehittymistä. Yrityksen onkin pidettävä huolta, että koulutusta kehitetään, ja henkilöstö saa tarvitsemansa koulutukset. (Perttunen 2023.)

4.2 Toimeksiantajan koulutukset

Yrityksellä on olemassa tietoturva- ja tietosuojakoulutukset. Heiltä löytyy myös erillinen kertauskoulutus, johon on yhdistetty molemmat osa-alueet. Kaikki koulutukset on toteutettu verkkokoulutuksina. Tietoturva- ja tietosuojakoulutukset löytyvät vain suomeksi, ja kertauskoulutus löytyy suomeksi kuin ruotsiksikin. Tietoturvakoulutus alkaa kertomalla tietoturvaan liittyvistä asioista. Koulutuksessa kerrotaan tietoturvan tärkeydestä ja siitä mitä

uhkia siihen kohdistuu. Uhiksi luokitellaan esim. haittaohjelmat, vakoilu ja väsytyshyökkäykset. Koulutuksessa on käyty läpi myös erilaisia haittaohjelmia ja niiden toimintatapoja. Listattuja haittaohjelmia on esim. virukset, madot ja troijalaiset. Seuraavaksi koulutuksessa on käyty läpi, miten tietoturvasta huolehditaan yrityksessä. Koulutuksen tässä osassa käydään läpi tietojen käsitteleminen, tietokoneen turvallinen käyttö, internetin ja sähköpostin käyttö. Koulutuksen lopussa käydään läpi yrityksen tietoturvaa ohjaavat tekijät. Lopusta löytyy myös ohjeistus käyttäjille siitä, miten tehdään ilmoitus tietosuojaa tai tietoturvaa koskevista havainnoista. Tietoturvakoulutuksessa on kaksi monivalintakysymystä, joissa kysytään, mitä ohjelmia käyttäjät saavat itse asentaa koneelle ja saavatko he antaa omia tunnuksiaan eteenpäin.

Tietosuojakoulutus alkaa tietosuojaan liittyvillä yleistiedoilla ja kysymyksillä. Kysymyksissä käydään läpi mitä tietosuoja on ja miten tietosuoja liittyy yrityksen työtehtäviin. Koulutuksen alussa on käyty myös läpi tietosuojan keskeiset termit, rekisteröidyn oikeudet ja tietosuojavastuut yrityksessä. Koulutus jatkuu tästä kertomalla tarkemmin, mitä kuuluu työntekijän vastuisiin ja velvoitteisiin tietosuojan osalta ja mitä työntekijöiden pitää muistaa erityisesti. Seuraavana koulutuksessa käydään läpi, miten henkilötietoja käsitellään päivittäin ja tähän osaan kuuluu opetus henkilötietojen käsittelystä. Koulutuksen lopussa tulee ohjeistus siihen, miten ongelmatilanteissa kuuluu toimia ja mistä käyttäjät löytävät tarkempia tietoja. Tietosuojakoulutuksessa on 10 monivalintakysymystä, joiden kysymykset vaihtelevat aihealueen sisällä. Kysymyksissä kysytään esim. mihin työtehtäviin tietosuoja yrityksessä liittyy, voiko käyttäjä tallentaa omalle työasemalleen asiakkaiden henkilötietoja ja mihin salasanoja saa tallentaa.

Yrityksellä on tehty yksi kertauskoulutus, joka sisältää tietoturvaan ja tietosuojaan liittyvät ohjeistukset. Kertauskoulutusta on päivitetty ja tämänhetkinen kertauskoulutus on vuodelta 2023. Kertauskoulutus alkaa kertomalla tietosuojan ja tietoturvan merkityksestä, ja miten käyttäjän tekemät valinnat vaikuttavat yrityksen tietosuojaan ja tietoturvaan. Seuraavaksi koulutuksessa käydään läpi yrityksen tietoturva- ja tietosuojapolitiikat ja mistä

käyttäjä voi kyseiset dokumentit löytää. Kertauskoulutuksessa kerrotaan tietoturvaan liittyvien häiriöiden ilmoittamisesta ja esimerkkejä häiriöistä, kuten tietoturvakoulutuksessa oli myös kerrottu. Kertauskoulutuksessa on käyty läpi esimerkkejä kalasteluviesteistä, ja ohjeita tekoälypalveluiden käyttöön. Kertauskoulutuksessa on käyty läpi myös tietoturvan ja tietosuojan noudattamisesta etätyötä tehdessä ja mahdollisista uhista, joita etätyössä voi tulla vastaan. Työsähköpostin käyttö, puhtaan näytön ja pöydän periaatteet ja kulunvalvontaan liittyvät ohjeistukset on myös käyty kertauskoulutuksessa yksityiskohtaisesti läpi. Kertauskoulutuksen lopussa on kerrattu vielä työntekijän tietosuojavastuut ja -velvoitteet. Kertauskoulutuksessa itsessään on vain kaksi monivalintatehtävää joihin käyttäjän pitää vastata. Ensimmäisessä kysymyksessä kysytään mitä käyttäjän pitää tehdä, jos epäilee koneellaan virustartuntaa ja toisessa kysytään voiko käyttäjä jättää työasemansa autoon yksinään.

5 Tietoturvakysely

Henkilöstön tietoturvatietämys taso selvitettiin toteuttamalla henkilöstölle verkkokysely. Kyselyä varten käytiin läpi yrityksen tietoturva- ja tietosuojapolitiikkoja ja nykyisiä koulutuksia, saaden paremman kuvan siitä, mitä asioita henkilöstön pitäisi tietää.

5.1 Kyselyn laatiminen

Tässä luvussa on listattu kysymykset, jotka sisältyivät verkkokyselyyn. Kyselyn vastausvaihtoehdot on listattu liitteessä 2. Kysymykset ovat laaja kattaus niin yleistietämys kysymyksiä tietoturvasta ja tietosuojasta, yrityksen tietoturvaan liittyviä kysymyksiä kuin mielipidekysymyksiä. Kysymykset ovat enimmäkseen samat kaikille, mutta muutama poikkeus löytyy.

1. Valitse liiketoiminta-alueesi
2. Sinun on keksittävä uusi salasana, minkä keksit?
3. Missä säilytät järjestelmiesi salasanoja?
4. Järjestelmä kertoo salasanani vanhentuneen, mitä teen.
5. Työkaverini tunnukset menevät lukkoon ja hän pyytää neuvoani, mitä teen?
6. Soittava asiakas pyytää itselleen järjestelmänvalvojan tunnuksia, mitä teen? (kysymys vain ICT-puolelle)
7. Olet tuonut asiakkaalle tunnukset, miten toimitat ne hänelle? (kysymys vain ICT-puolelle)

Ensimmäisellä kysymyksellä selvitetään mihin liiketoiminta-alueeseen vastaaja kuuluu. Ensimmäisen kysymyksen jälkeen aukeaa vastaajalle hänen liiketoiminta-alueeseensa liittyvät kysymykset. Selvittämällä vastaajan liiketoiminta-alue saadaan tieto siitä, millainen tietämys jokaisen liiketoiminta-alueen henkilöstöllä on. Tämän jälkeen kysymykset painottuvat tunnuksiin ja niiden ylläpitoon. Tunnusten oikeanlainen hallinta on tärkeää tietoturvan kannalta, ja yrityksen tietoturvakoulutuksessa on myös käyty läpi tunnusten

hallintaan liittyvät ohjeistukset. Kysymykset kuusi ja seitsemän ovat vain ICT-puolelle suunnattuja kysymyksiä, koska tunnusten luominen kuuluu siellä olevien työnkuvaan.

8. Havaitset tietoturvahäiriön, mitä teet?
9. Tietokoneeni ilmoittaa virustorjunnan olevan pois päältä, mitä teen?
10. Löydät konttorin tiloista yksinäisen muistitikun, mitä teet?
11. Esihenkilöltäsi tulee sähköpostia, jossa hän pyytää sinua hankkimaan lahjakortteja firman juhliin. Mitä teet?

Seuraavat neljä kysymystä painottuvat yleiseen tietoturvaan. Yrityksen koulutuksissa on käyty läpi kyseisiin tilanteisiin liittyvät ohjeistukset. Kysymykset esitetään kaikille vastaajille, koska kaikkien pitää tietää, miten näissä tilanteissa toimitaan.

12. Saako tekoälyltä (esim. ChatGPT) kysyä työhöni liittyviä asioita?
13. Mitä laitteita voit kytkeä työkoneeseesi?
14. Mitä puhtaan pöydän periaate tarkoittaa?
15. Poistun työpisteeltäni, mitä teen?
16. Olet löytänyt loistavan ohjelmiston, joka auttaisi minua työnteossa, mitä teen?
17. Etätyöntekijä, millaisessa tilassa teet töitä?
18. Mihin kaikkeen voin työsähköpostiani käyttää?
19. Millä näppäin yhdistelmällä lukitsen koneeni?
20. Henkilö on tulossa huoltamaan palvelinkeskuksessa olevaa järjestelmää, mitä teen? (Kysymys vain ICT ja tietoliikenne puolille.)

Kysymykset 12–20 kohdistuvat jokapäiväiseen työelämään. Yrityksessä ei ole vielä käytössä tekoälyohjelmia yrityslisenssillä, mutta suunnitelmassa on. Tämän takia kysymyksessä 12 selvitetään henkilöstön käyttäytymistä tekoälyn kanssa. Yrityksen koulutuksissa oli myös käyty läpi tekoälyyn liittyvät ohjeistukset. Kysymykset 13–19 ovat kysymyksiä tilanteista, joihin enemmistö yrityksessä kohta. Esimerkiksi jokainen työntekijä poistuu työpisteeltään ja käyttää työsähköpostia, joten nämä kysymykset esittämällä saadaan tietoon,

miten moni vastaaja noudattaa yrityksen ohjeistuksia. Kysymys 20 on vain ICT- ja tietoliikennepuolen henkilöille, koska siellä olevilla on oikeus palvelinkeskukseen.

21. Tiedän mitä minun pitää tehdä, jos havaitsen tietomurron.
22. Milloin viimeksi olet suorittanut työpaikan tarjoaman tietoturvakoulutuksen?
23. Koetko, että nykyinen tietoturvakoulutus on riittävän kattava sinun työtehtäviisi liittyen?
24. Mistä löydät yrityksen tietoturvapolitiikan?
25. Miten hyvin nykyinen tietoturvakoulutus on valmistanut sinut tunnistamaan ja reagoimaan tietoturvauhkiin?
26. Miten arvioisit nykyisen tietoturvakoulutuksen selkeyttä ja ymmärrettävyyttä?
27. Millainen koulutusmuoto tukisi parhaiten sinun oppimistasi?
28. Miksi tietoturva on tärkeää yrityksemme kannalta?

Kysymykset 21–28 liittyvät henkilöstön käyttäytymiseen tietomurron aikana, henkilöstön koulutuksen tilanteeseen ja mielipidekysymyksiä yrityksen nykyisestä koulutuksesta. Yrityksen koulutuksissa on monesti käyty läpi, miten henkilöstön pitää toimia tietomurron havaitessaan. Kysymys on yksinkertainen, mutta tärkeä. Yrityksellä ei ole tarkkaa koulutusaikaa henkilöstölle, joten kysymyksellä 22 selvitetään, milloin vastaaja on viimeisemmän kerran suorittanut yrityksen tarjoamat tietoturva- ja tietosuojakoulutukset. Lopuilla kysymyksillä tahdotaan selvittää henkilöstön mielipidettä nykyisestä koulutuksesta, jotta seuraavista koulutuksista voidaan tehdä henkilöstölle mieluisempia.

Näiden kysymysten avulla on tarkoitus saada ymmärrystä siihen, millä tasolla henkilöstön tietämys on ja tarvitseeko olemassa oleville koulutuksille tehdä jotain.

5.2 Kyselyn jakelu

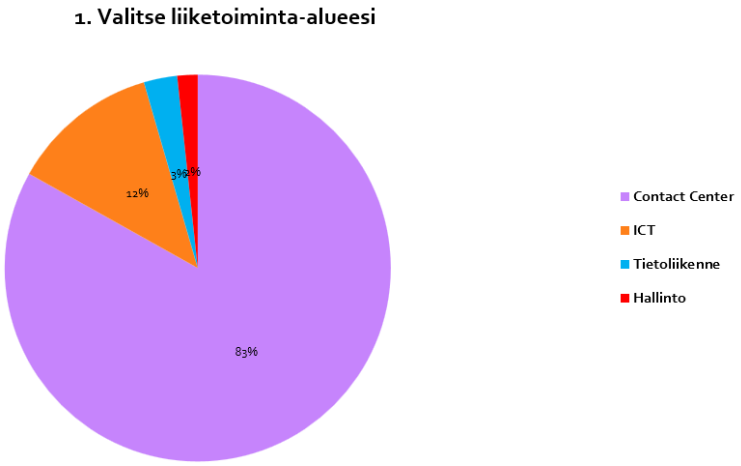
Tavoitteena on saada mahdollisimman monen työntekijän vastaus kyselyyn ja kyselyn jakaminen on osa tätä. Ensimmäinen suunnitelma oli pyytää lupaa käyttää yrityksen Service Deskin sähköpostiosoitetta, ja lähettää kysely sitä kautta kaikille. Tämän avulla kyselyn lähettäjän tiedot olisivat pysyneet salattuna, samoin kyselyn todellinen tarkoitus. Kyselyn oleminen osa opinnäytetyötä, tahdottiin pitää salassa, koska oli pelko, että tämä tieto vähentäisi vastauksia.

Suunnitelmaa kuitenkin muutettiin, kun keskusteltiin yrityksessä olevan ohjaajani kanssa kyselyn jakelusta. Hän ehdotti, että oltaisiin yhteydessä henkilöön, joka vastaa yrityksen viestinnästä. Kyseinen henkilö suostui tässä auttamaan, ja hänen avullaan saatiin kysely jakoon niin, että kyselyn todellinen syy pysyi salassa.

Kyselyn päädyttiin lähettämään 322 henkilölle ja tämä kattaa yrityksen henkilöstön asiakaspalvelu, ICT, tietoliikenne ja hallinnon puolelta. Yrityksen johtoon emme nähneet syytä lähettää kyselyä.

6 Kyselyn vastaukset

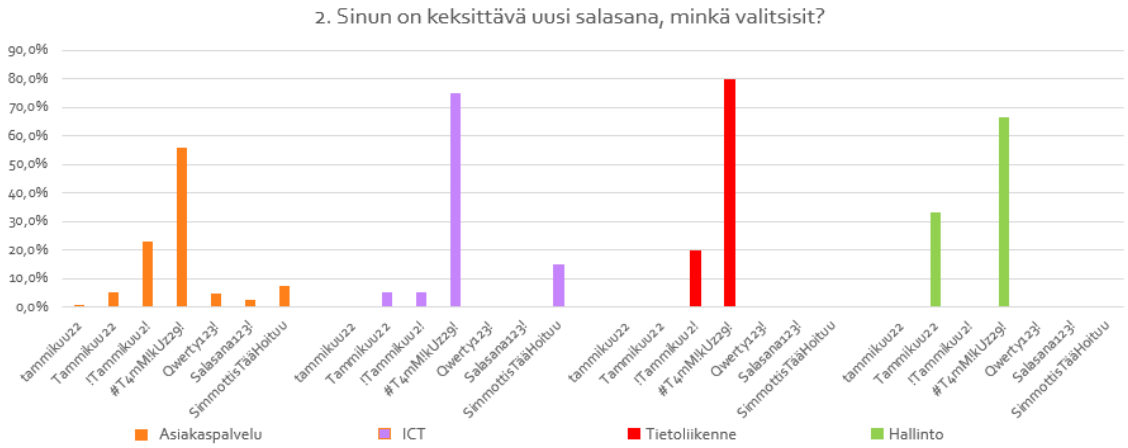
Kysely lähetettiin 322 henkilölle ja siihen vastasi 181 henkilöä. Vastausprosentti oli 56 %. Vastausprosentti jakautui seuraavanlaisesti liiketoiminta-alueiden välille: asiakaspalvelu 83 %, ICT 12 %, tietoliikenne 3 % ja hallinto 1 % (Kuvio 1). Tietoliikenteen ja hallinnon puolelta olisi tahdottu vielä vähän enemmän vastauksia, mutta asiakaspalvelu ja ICT-puoleen verrattuna ne ovat selvästikin pienempiä liiketoiminta-alueita henkilöstön puolelta, joten pienempi vastausprosentti niistä on ymmärrettävää.



Kuvio 1. Liiketoiminta-alueiden vastausprosentit.

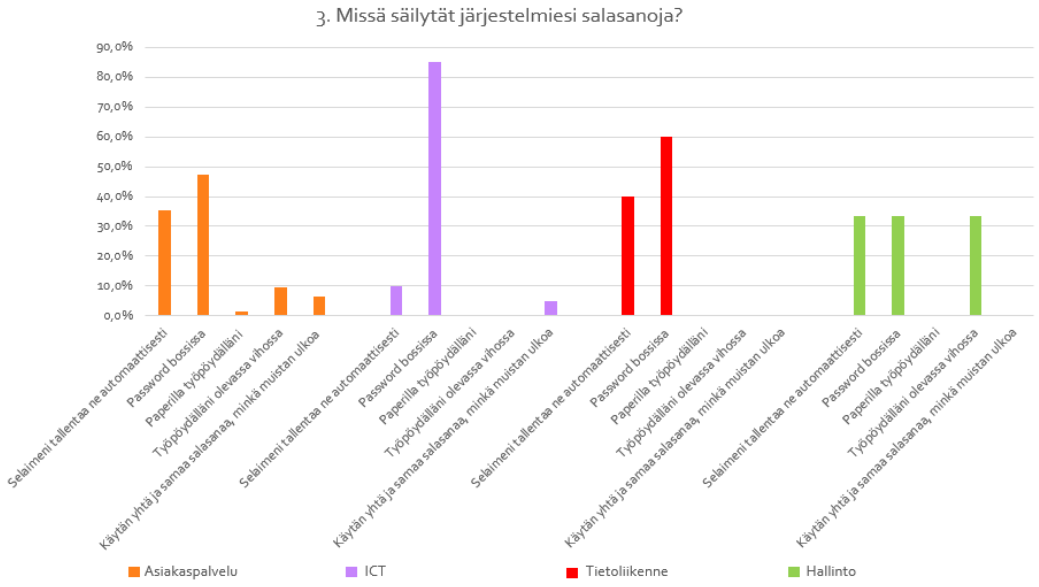
Seuraavana oli vuorossa selvittää, millaisen salasanan käyttäjät itselleen valitsisivat. Vaihtoehdot oli käyttäjille jo annettu, eikä vastaajien tarvinnut itse luoda mitään salasanoja. (Liite 1.) Näin vältyttiin siltä, että käyttäjä kirjoittaisi oman salasanansa vastaukseksi. Jokaiselta liiketoiminta-alueelta enemmistö vastaajista valitsisi itselleen hankalimman salasanan, joka täyttää yleisimmät salasanavaatimukset hyvin. Seuraavaksi eniten vastauksia sai salasana vaihtoehdot, joissa oli murresanoja tai täytti nykyisten salasanavaatimusten minimivaatimukset. (Kuvio 2.) Yrityksen omissa ohjeistuksissa on kerrottu salasanan minimivaatimukset. Salasana vaihtoehdoista vain yksi täytti nämä kaikki vaatimukset, ja enemmistö sen oli valinnutkin. Salasanojen yleisiä

sääntöjä on esimerkiksi salasanan pituus, sillä mitä pidempi salasana on sitä parempi. Salasanassa olevaa sanaa ei kuitenkaan saisi löytyä mistään sanakirjasta. Salasanassa olevan sanan ollessa vieraskielinen tai harvinainen ei takaa salasanan varmuutta, sillä hakkereilla on pääsy jopa miljoonien sanojen luetteloihin, joista he voivat lähteä ratkomaan salasanoja. Salasanoja voi luoda yhdistämällä sanoja ja tekemällä kirjoitusvirheitä. (Järvinen 2022, 94.)



Kuvio 2. Kysymyksen kaksi vastaus prosentit liiketoiminta-alueittain.

Kyselyn avulla selvitettiin myös se, että monet käyttäjät tallentavat salasanansa joko salasanojen hallintaohjelmaan tai antavat selaimensa tallentaa salasanansa. Osa myös säilyttää salasanojaan fyysisellä viholla. (Kuvio 3.) Ohjeistuksissa ja koulutuksissa on selvästi kerrottu, että salasanoja ei saisi säilyttää työpöydällä paperilla, ja saman salasanan käyttämistä on pyydetty välttämään. Ohjeistuksissa ei ole kerrottu missä käyttäjien olisi parasta säilyttää salasanoja, kuitenkin yrityksellä on käytössä salasanojen hallintaohjelma, jonka käyttöä on henkilöstölle suositeltu. Vaikka vain pieni osa vastaajista säilyttää salasanojaan fyysisesti paperilla, olisi käyttäjille helpompaa, jos koulutuksissa kerrottaisiin minne salasanat kannattaa tallentaa.



Kuvio 3. Vastausprosentit kysymykseen 3 liiketoiminta-alueittain.

Kyselyn avulla tahdottiin myös selvittää, miten käyttäjät toimivat tilanteessa, jos heidän salasanansa on vanhentunut. Liitteestä 2 voidaan nähdä, että asiakaspalvelun, ICT:n ja hallinon puolella yli 60 % vastaajista vaihtaisi salasanansa kokonaan uuteen ja monimutkaisempaan. Tietoliikenteenpuolella 60 % vastaajista vaihtaisi salasanansa samanlaiseen kuin nykyinenkin salasana on. Yrityksen ohjeistuksen mukaan, käyttäjien on vaihdettava salasanansa erilaiseen ja yksilölliseen salasanaan vanhan salasanan vanhentuessa. Enemmistö vastaajista on kyselyn mukaan tämän ymmärtänyt hyvin.

Seuraavassa kysymyksessä tahdottiin selvittää, miten henkilöstö reagoisi siihen, kun työkaverin tunnukset olisivat lukossa (Liite 1). Tähän enemmistö vastaajista oli vastannut neuvovansa työkaveriaan olemaan yhteydessä Service Deskiin. Vain hyvin pieni osa vastaajista olisi ollut tekemättä mitään tässä tilanteessa. (Liite 2.) Tietoturvakoulutuksessa on esitetty samanlainen kysymys, ja siinäkin oikeana vastauksena on neuvoa käyttäjää olemassa yhteydessä Service Deskiin. Kysymystä ei esitetty ICT-puolelle, koska enemmistöllä siellä olevilla on oikeudet avata lukittuneet tunnukset.

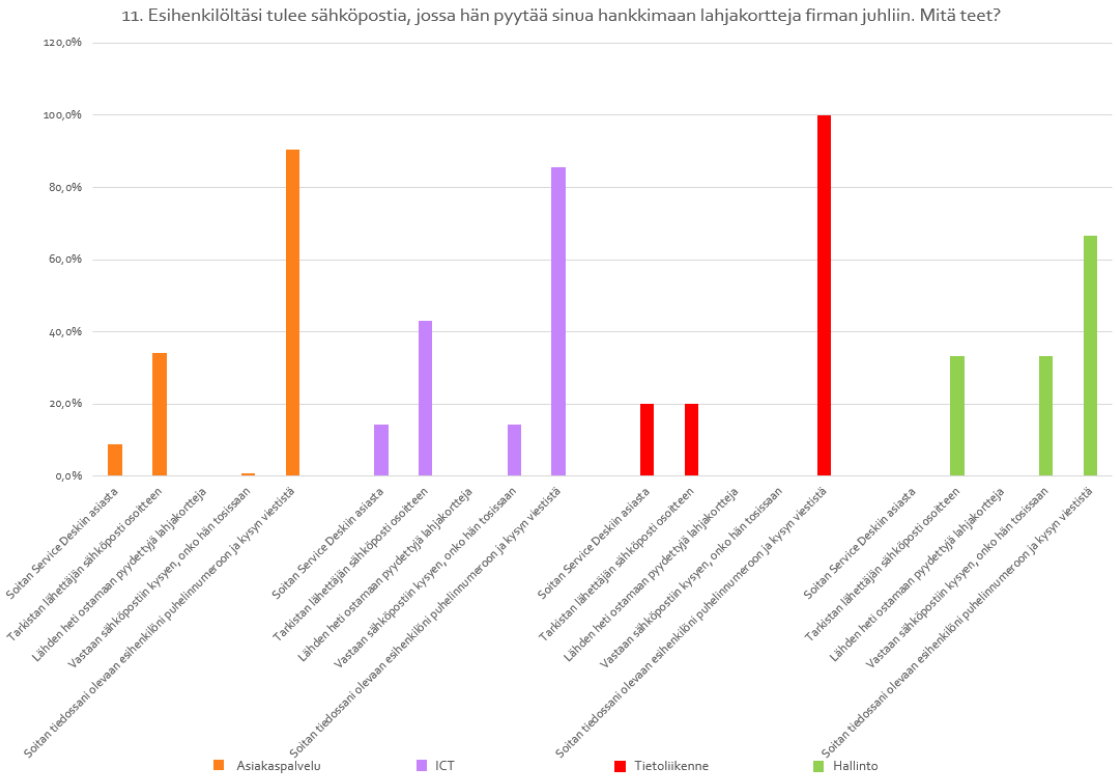
ICT-puolella työntekijät voivat tarvittaessa tehdä järjestelmänvalvojan tunnuksia käyttäjälle. Kuitenkin on tärkeää, että tunnukset luodaan vain siinä tilanteessa, kun oikea taho on niitä pyytänyt, ja niiden toimittaminen täytyy tehdä myös oikealla tavalla. Vastaajista 86 % oli sitä mieltä, että tunnukset luodaan vain siinä tilanteessa, jos käyttäjän esihenkilö niitä pyytää ja vastaajista loput ei tekisi tunnuksia (Liite 2). Liitteestä 2 nähdään, että 48 % vastaajista toimittaa tunnukset myös salattuna sähköpostina tunnusten tilaajalle tai tekstiviestinä. Tietosuojakoulutuksessa on käyty läpi, että tunnukset toimitetaan asiakkaille aina salattuna sähköpostina. Kysymykseen seitsemän ei ole erillistä kohtaa yrityksen tietoturvakoulutuksessa, mutta yleisenä käytäntönä on se, että tietyt esihenkilöt pyytävät uusia tunnuksia tarvittaessa. Vastaukista päätellen enemmistö on näistä tietoinen, vaikka osa vastaajista toimittaisikin tunnuksia eri tavalla.

Kun henkilöstön eteen tulisi tietoturvahäiriö, melkein kaikki vastaajista tietäisi ilmoittaa asiasta nopeasti esihenkilölleen tai tietoturvavastaavalle. Tilanteessa, jossa käyttäjä huomaisisi virustorjunnan olevan tietokoneelta pois päältä, olisi 80 % vastaajista suoraan yhteydessä Service Deskiin. Osa vastaajista yrittäisi myös käynnistää tietokoneensa uudelleen, jos huomaisivat virustorjunnan olevan pois päältä. ICT-puolen vastaajista 67 % saisi itse aktivoitua virustorjunnan takaisin päälle. (Liite 2.) Yrityksen koulutuksissa on käyty läpi tarkasti, miten henkilöstön kuuluu toimia tietoturvahäiriön havaitessa ja kyselyn perusteella asia on henkilöstölle selvä. Koulutuksen neuvojen mukaan, henkilön pitää ilmoittaa havainnoistaan nopeasti tietoturvavastaavalle tai esihenkilölleen. Virustorjunnan päällä olemisesta on myös mainita koulutuksissa, ja sen pitää olla aina päällä. Koulutuksissa ei ole erillistä merkintää siitä mitä tehdä, jos virustorjunta on pois päältä. Yleisesti ohjeistetaan kuitenkin olemaan tällaisissa tilanteissa yhteydessä Service Deskiin.

Tilanteessa, jossa työntekijä löytäisi toimistolta muistitikun, olisi kyselyn perusteella asiakaspalvelun, tietoliikenteen ja hallinnon puolen vastaajista yli 80 % valmis soittamaan Service Deskille asiasta tai ilmoittamaan esihenkilölleen löytyneestä muistitikusta. Seuraavaksi eniten vastaajat

laittaisivat tässä tilanteessa muistitikun näkyvälle paikalle siinä toivossa, että sen omistaja löytäisi sen. (Liite 2.) Yrityksen koulutuksissa kerrotaan, että epäilyttävistä tavaroista pitää heti ilmoittaa esihenkilölle, lähivalmentajalle tai vuorovastaavalle. Koulutuksessa kerrotaan myös, että ulkopuolelta tulleet muistitikut tai muut muistivälineet täytyy tarkastaa virustorjuntaohjelmalla ennen käyttöä. Kyberrikolliset voivat kuitenkin jättää haitallisia USB-laitteita yrityksen henkilöstön löydettäviksi, ja vain yhden uteliaan käyttäjän tarvitsee löytää syötiksi jätetyn laitteen ja kytkeä se koneeseensa haavoittuvuuden aikaansaamiseksi. Yritysten olisi hyvä kieltää vieraiden USB-laitteiden kytkeminen sisäverkossa oleviin koneisiin. (Järvinen 2022, 63.)

Seuraavan kysymyksen kohdalla oli laajasti vaihtelua vastauksissa. Vaikka asiakaspalvelun, ICT:n ja tietoliikenteen vastaajista yli 80 % olisikin yhteydessä esihenkilöönsä, saatuaan epäilyttävän viestin esihenkilön nimissä, osa vastaajista tekisi myös toisin. Seuraavaksi eniten kyselyyn vastanneista tarkastaisi lähettäjän sähköpostiosoitteen, ja osa myös soittaisi Serivce Deskiin asiasta. (Kuvio 4.) Yritksen koulutuksissa kehoitetaan käyttäjiä avaamasta erikoisista osoitteista tulleita sähköposteja tai tarkistamaan lähettäjän osoite, ennen kuin viestin kanssa tekee mitään. Kaikkein turvallisin tapa yrityksen silmissä, olisi olla tekemättä mitään viestin kanssa, tuhota se suoraan ja ilmoittaa asiasta Service Deskiin tai tietosuojavastaavalle.



Kuvio 4. Kysymyksen 11 vastausprosentit.

Kyselyssä oli myös mukana kysymys tekoälyn käytöstä työasioihin (Liite 1). Tekoälyn käytöstä olivat vastaajat myös laajasti erimieltä. Asiakaspalvelupuolella yli 40 % mielestä tekoälyä ei saa käyttää, ICT-puolella melkein 60 % mielestä tekoälyä saa käyttää yleisiin asioihin, ja tietoliikenteen ja hallinnon puolella yli 30 % mielestä sitä saa käyttää yleisiin asioihin tai eivät tiedä, mihin sitä saa käyttää. (Liite 2.) Yrityksen ohjeistuksien mukaan tekoälyyn ei saa syöttää mitään henkilötietoja tai yrityksen arkaluontoista dataa. Yrityksen neuvona on, että julkisissa tekoälypalveluissa saa käyttää ainoastaan sellaista tietoa, joka voisi löytyä kaikkien saatavilta.

Seuraavassa kysymyksessä selvitettiin henkilöstön tietämystä työpisteen turvallisesta käytöstä, ja kysyttiin mitä laitteita he saavat työkoneeseensa liittää (Liite 1). Yli 80 % vastaajista asiakaspalvelun, ICT:n ja tietoliikenteenpuolelta kytkisi vain työpaikalta saatuja laitteita koneisiinsa. Pieni osa vastaajista oli vastannut, että myös henkilökohtaisia laitteita saisi liittää työkoneeseen. (Liite 2.) Yrityksen koulutuksissa myös kerrotaan, että vain yritykseltä saamia laitteita

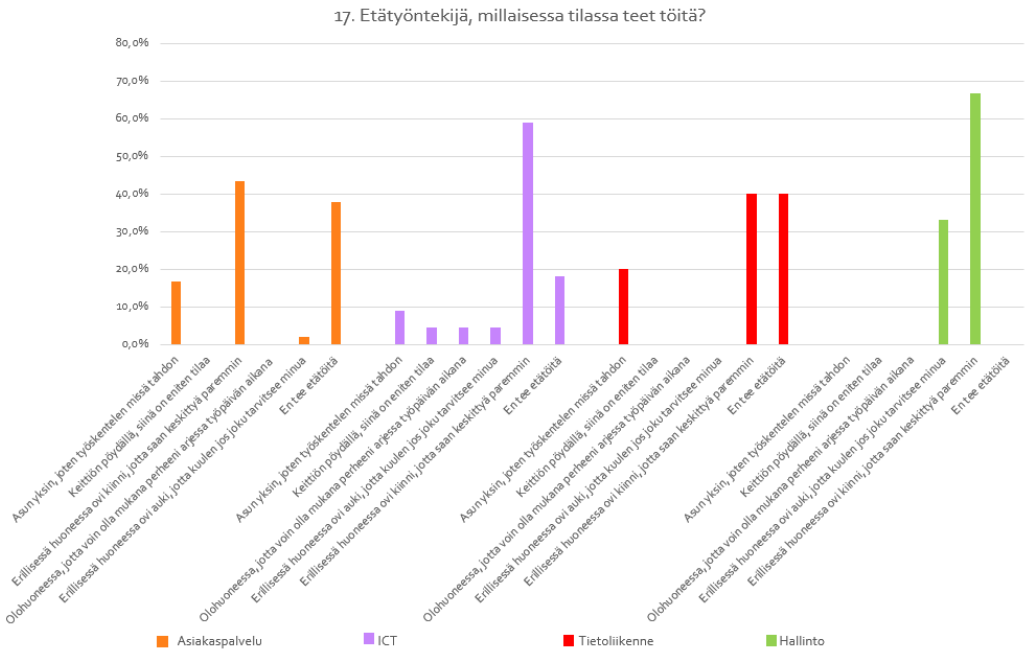
saa liittää koneeseen. Poikkeuksia kuitenkin on myös, sillä henkilöstössä on henkilöitä, jotka tarvitsevat henkilökohtaisia avustuslaitteita koneeseensa työnsä tekemiseksi.

Työpisteeseen liittyen yli 80 % vastaajista oli tietoisia siitä, että puhtaan pöydän periaate tarkoittaa, että työpaperit laitetaan pois näkyvistä työpäivän jälkeen. Myös yli 80 % vastaajista asiakaspalvelun, ICT:n ja tietoliikenteenpuolelta oli tietoisia, että kone pitää lukita työpisteeltä poistuessa. (Liite 2.) Koulutuksissa on selvästi käyty läpi, mitä puhtaan pöydän periaatteella tarkoitetaan ja se, että kone täytyy lukita työpisteeltä poistuessa. Vaikka koulutuksissa ei kerrotakaan miten koneen voi lukita, on tapoja monia ja lopputulos on tässä tilanteessa tärkein. Koneen lukitsiminen työpisteeltä poistuessa pitäisi olla itsestäänselvyys käyttäjille. Vaikka koneissa onkin automaattinen asetus, että kone mene tietyn ajan kuluessa lukkoon, voi pienessäkin ajassa joku tutkia koneella auki olevia tietoja käyttäjän ollessa poissa. (Järvinen 2022, 183.)

Vaikka peruskäyttäjät eivät pysty juurikaan mitään ylimääräisä ohjelmia asentamaan, on silti tärkeää, että he tietävät, miten kuuluu siinä tilanteessa toimia, jos he haluaisivat jonkin tietyn ohjelmiston koneeseensa (Liite 1). Kaikki vastaajat olivat samaa mieltä siitä, että kysyisivät esihenkilöltään lupaa sovellusten asentamiseen (Liite 2). Peruskäyttäjille ei yrityksessä anneta järjestelmänvalvojan oikeuksia, mutta joitain ohjelmia myös peruskäyttäjä pystyy asentamaan. Ohjelmat, joita käyttäjä voi asentaa omien tiedostojen joukkoon ovat ohjelmia, joita peruskäyttäjät pystyvät asentamaan. Ohjelmat, jotka tarvitsevat pääsyn koneen omiin ohjelmakansioihin tarvitsevat järjestelmänvalvojan oikeudet. Haittaohjelmien asentaminen on siis mahdollista myös peruskäyttäjän oikeuksilla. (Järvinen 2022, 41.) Yrityksen koulutuksissa on selitetty, että jos haluaa asentaa jonkun ohjelman koneeseen, pitää siitä keskustella esihenkilön kanssa.

Seuraavassa kysymyksessä tahdottiin selvittää, millaisessa tilassa etätöitä tekevät työskentelevät (Liite 1). Jokaisen liiketoiminta-alueen vastaajista yli 40 % tekisi etätöitään erillisessä huoneessa ovi kiinni. Seuraavaksi eniten etätöitä tekeviä ovat yksin asujia, joten heillä ei ole juurikaan rajoitteita omassa

asunnossaan. Loput vastaajista eivät tee etätöitä ollenkaan tai työskentelevät avoimessa tilassa. (Kuvio 5.) Etätöiden ohjeistus yrityksessä on se, että etätöitä tehdään suljetussa tilassa niin, ettei kukaan ulkopuolinen näe koneesi näyttöä tai kuule mitä puhut puhelimessa.



Kuvio 5. Kysymyksen 17 vastaukset.

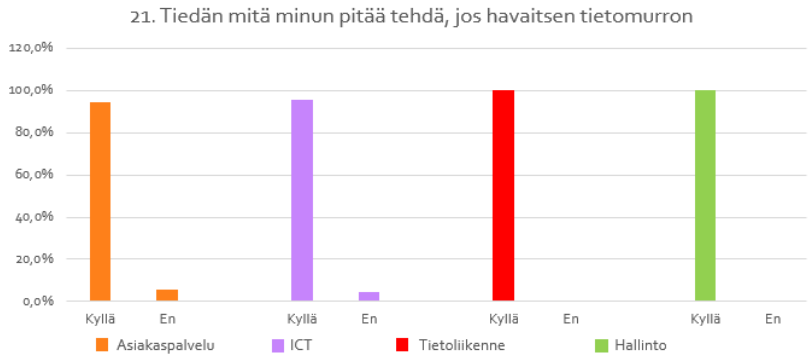
Työsähköpostin käyttö on jokaisen henkilöstöön kuuluvan arkipäivää, joten tietoturvan kannalta on tärkeää tietää, mihin henkilöstö työsähköpostiaan käyttää (Liite 1). Yli 60 % jokaisen liiketoiminta-alueen vastaajista käyttää työsähköpostiaan vain työasioihin liittyviin tilanteisiin. Loput vastaajista oli sitä mieltä, että työsähköpostia saa käyttää myös henkilökohtaisiin tärkeisiin asioihin. (Liite 2.) Yrityksen ohjeistuksissa ja koulutuksissa on käyty läpi, että työsähköposti on tarkoitettu ainoastaan työasioiden hoitamiseen. Suurin osa vastaajista on siis tietoisia mihin kaikkeen työsähköpostin voi laittaa.

Yrityksen tietoturvakoulutuksissa on käyty läpi se, että työpisteeltä poistuessa pitää kone muistaa lukita. Niissä ei kuitenkaan ole kerrottu, miten tämä tehdään. Kyselyn perusteella yli 50 % vastaajista jokaiselta liiketoiminta-alueelta käyttää

koneensa lukitsimiseen pikanäppäinyhdistelmää Windows + L. Seuraavaksi eniten (n. 30 %) vastaajista lukitsee koneensa näppäinyhdistelmällä ctrl + alt + delete. (Liite 2.) Tätä vaihtoehtoa ei ollut suoraan kyselyssä, mutta vastaajat olivat laittaneet sen vapaasti kirjoitettavan vastauksen kohdalle tässä kysymyksessä. (Liite 1.)

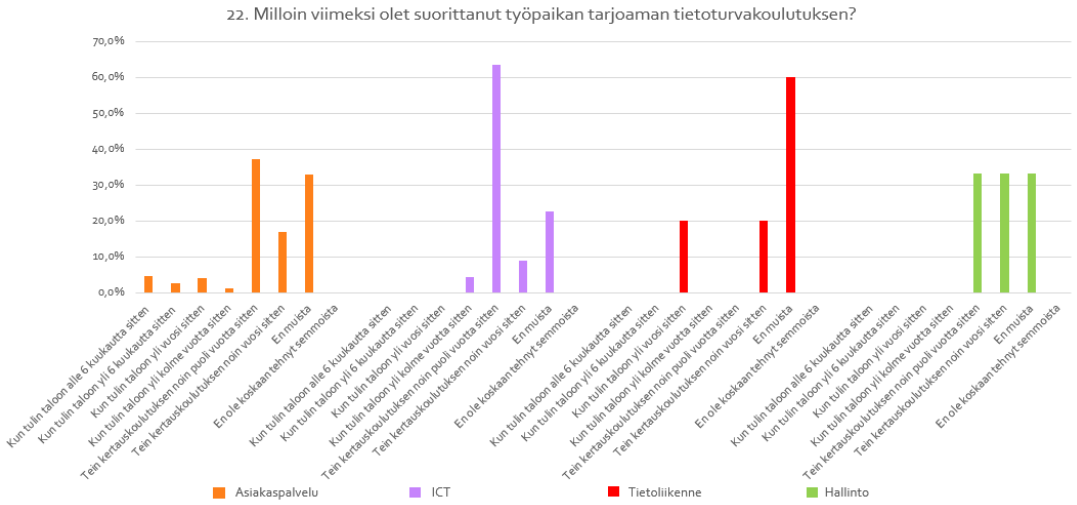
ICT ja tietoliikennepuolella on joitain käyttäjiä, joilla on oikeus päästä yrityksen palvelinkeskukseen. On siis tärkeää, että nämä oikeudet omaavilla on ymmärrys sitä, miten toimitaan tilanteessa, kun palvelinkeskukseen tahtoo joku ulkopuolinen tulla. (Liite 1.) Yli 50 % vastaajista ei näitä oikeuksia ollut, mutta heillä, joilla oikeudet on, olisivat huoltohenkilön kanssa palvelinhuoneessa koko operaation ajan tai he eivät päästäisi henkilöä ollenkaan tiloihin. (Liite 2.) Yleisessä tietoturvakoulutuksessa ei ollut tähän asiaan mitään mainittu, mutta yleinen periaate yrityksessä on se, että jos työntekijä on päästänyt ulkopuolisen henkilön taloon sisään, työntekijä on tämän henkilön seurassa koko ajan. Myös siinä tilanteessa, jos huoltohenkilö on tulossa huoltamaan palvelinkeskusta.

Kyselyllä tahdottiin selvittää henkilöstön tietämystä tietoturvasta, joten kysely sisälsi myös yksinkertaisen kysymyksen siitä, tietävätkö käyttäjät mitä heidän pitää tehdä tietomurron huomatessaan (Liite 1). Vastaajista yli 80 % on sitä mieltä, että he tietävät, mitä kuuluu tehdä (Kuvio 6).



Kuvio 6. Vastausprosentti tietomurron havaitsemisesta.

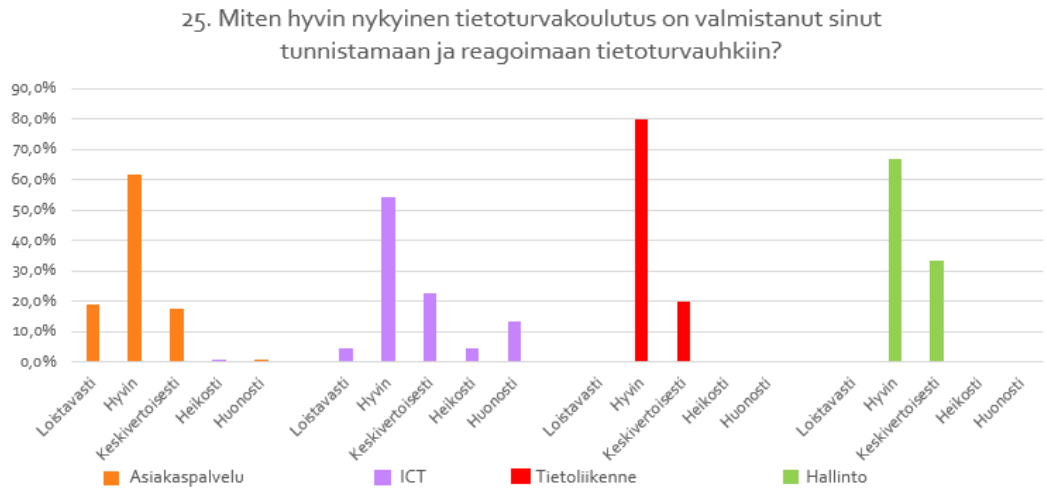
Seuraavassa kysymyksessä selvitettiin, milloin käyttäjät ovat viimeksi tietoturvakoulutuksen tehneet tai kertauskoulutuksen (Liite 1). Yli 30 % vastaajista on suorittanut kertauskoulutuksen noin puoli vuotta sitten, ja seuraavaksi eniten vastaajista olivat aloittaneet työt viimeisen puolen vuoden aikana ja perehdytyksen yhteydessä tehneet koulutuksen. (Kuvio 8.) Yrityksen kertauskoulutuksessa on kerrottu, että kertauskoulutus pitäisi suorittaa puolen vuoden välein. Enemmistö vastaajista on vastausten mukaan pysyneet halutussa aikarajassa, vaikka osa vastaajista ei muista milloin koulutuksen on suorittanut.



Kuvio 7. Kysymyksen 22 vastaukset.

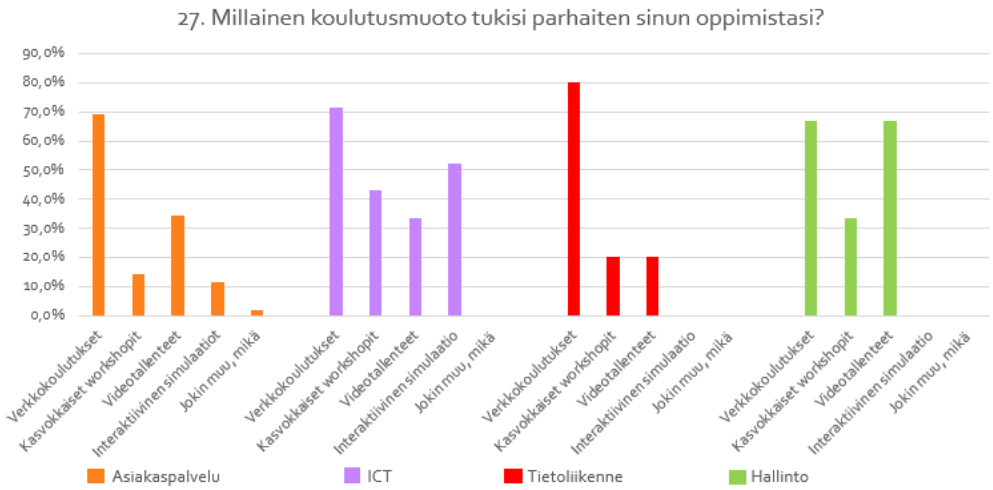
Kyselyn viimeisimmät kysymykset kohdistuivat nykyiseen tietoturvakoulutukseen ja sen riittävyyteen (Liite 1). Kun kysyttiin, onko nykyinen koulutus tarpeeksi kattava käyttäjän työtehtävään liittyen, yli 80 % jokaisen liiketoiminta-alueen vastaajista oli sitä mieltä, että nykyinen tietoturvakoulutus on riittävä (Liite 2). Kyselyn seuraavaan kysymykseen vastaajat saivat kirjoittaa oman vastauksensa (Liite 1). Enemmistö vastaajista oli tietoisia siitä, mistä yrityksen tietoturvapolitiikka löytyy, ja osa jopa antoi vastaukseksi tarkan polun mistä sen löytää. Vain hyvin pieni osa vastaajista ei ollut tietoinen sen sijainnista. Kyselyllä tahdottiin myös selvittää henkilöstön mielipidettä siihen,

miten hyvin nykyinen koulutus on valmistanut heitä reagoimaan tietoturvauhkiin (Liite 1). Asiakaspalvelun, tietoliikenteen ja hallinon vastaajista yli 60 % mielestä nykyinen koulutus on valmistanut heidät tunnistamaan tietoturvauhan hyvin tai keskivertoisesti. ICT-puolen vastaajista yli 50 % oli samaa mieltä. (Kuvio 8.) Tietoturvakoulutuksen selkeyttä ja ymmärrettävyyttä vastaajista yli 60 % arvioisi arvosanalla neljä asteikolta 1–5 (Liite 2).



Kuvio 8. Vastaukset kysymykseen 25.

Kyselyllä tahdottiin myös tietää henkilöstön mielipiteet parhaista koulutusmuodoista (Liite 1). Vastaajista yli 60 %:n mielestä paras koulutusmuoto heille olisi verkkokoulutus. Seuraavaksi eniten ääniä sai videotallenteet ja kasvokkaiset workshopit koulutusmuotona (Kuvio 9).



Kuvio 9. Käyttäjien mielestä oppimista parhaiten tukevat koulutusmuodot.

Kyselyn viimeisellä kysymyksellä tahdottiin selvittää, ymmärtääkö henkilöstö tietoturvan tärkeyden (Liite 1). Kaikilla kysymykseen vastaajilla oli hyvin tiedossa tietoturvan tärkeys ja sen tärkeyttä kuvattiin seuraavin sanoin:

> ”Tietoturva on yksi liiketoimintamme tärkeimmistä edellytyksistä, että voimme toimia alalla.”
>
> ”Asiakkaiden tiedot tulee turvata.”
>
> ”Yrityksemme käsittelee paljon tietoja, joiden ei kuulu päästä vieraiden käsiin joten, esim. siksi meidän kaikkien on hyvä ottaa tietoturvaan liittyvät asiat huomioon.”
>
> ”Tietoturva auttaa suojaamaan yrityksen työntekijöitä, asiakkaita, sekä yrityksen omia toimintamalleja ja periaatteita.”
>
> ”Että yrityksen ja asiakkaiden luottamukselliset tiedot pysyvät suojassa.”

Jo pienestä osaa vastauksista voi päätellä, että henkilöstö tietää ja ymmärtää minkä takia tietoturvaan pitää panostaa ja pitää yllä.

7 Tulosten yhteenveto

Tulosten perusteella voidaan sanoa, että yrityksen henkilöstö on enimmäkseen hyvin tietoisia tietoturvasta ja sen tärkeydestä. Henkilöstö on sisäistänyt tietoturvakoulutuksissa olleet opit ja koulutuksien tärkeyden. Vaikka jokaisella liiketoiminta-alueella on ollut täysin samat koulutukset, ei se ole tehnyt suuria eroja liiketoiminta-alueiden välille.

Heikkouksia tai huolenaiheita heräsi kuitenkin kyselyn joidenkin kysymysten kohdilta. Salasanojen säilyttämisestä ja niiden eroavaisuuksista on yrityksen koulutukissa mainittu, mutta on kuitenkin monta käyttäjää, jotka tallentavat salasanojansa paperille tai viholle ja pitävät näitä työpisteen lähellä. Muutama vastaaja myös käyttää vain yhtä ja samaa salasanaa jokaiseen palveluun, mikä on riski itsessään ja vielä suurempi, jos käyttäjän salasana on heikko. Osa vastaajista myös jättäisi toimistolta löytyneen muistitikun siihen paikkaan, mutta ICT-puolella muutama vastaajista ei tekisi mitään muistitikun löytäessään. On ymmärrettävää, että asiakaspalvelu tai hallinto puolella työntekijä ei tekisi muistitikun löytäessään mitään, mutta ICT-puoli vastaa yrityksen laitteista ja niiden kunnossapidosta, joten heillä pitäisi olla tarkempi ohjeistus, miten toimitaan siinä tilanteessa, kun toimiston tiloista löytyy yksinäinen muistitikku.

Myös pieni osa ICT-puolen vastaajista vastaisi heille tulleeseen sähköpostiin, jossa heidän esihenkilönsä nimissä, heitä pyydetään ostamaan lahjakortteja. Yrityksen tietoturvakoulutuksissa on tämäkin tilanne käyty tarkkaan läpi, joten on lievästi huolestuttavaa, että jotkut käyttäjät menisivät sähköpostiin vastaamaan. Vaikka kysymyksen vastausvaihtoehto olikin muotoiltu muotoon, josta voisi ymmärtää, että vastataan viestiin vain lisätietoja kysyäkseen, on silti suositeltavampaa tarkistaa lähettäjän sähköpostiosoite ensin. Vastaamalla sähköpostiin saa lähettäjä tiedon, että käyttäjän sähköpostiosoite on voimassa oleva.

ICT-puolen vastaajista osan mielestä nykyinen tietoturvakoulutus ei myöskään ole valmistanut heitä tunnistamaan ja reagoimaan tietoturvauhkiin, ja tämä on

ymmärrettävää. Nykyiset koulutukset eivät sisällä mitään tietoa siitä, miten ICT-puolen henkilöstön pitäisi toimia tietoturvauhan kohdatessaan. Kyseiset henkilöt vastaavat yrityksen omasta ja asiakkaiden tietoteknisistä laitteista ja olisi tärkeää, että jos joku ilmoittaa mahdollisesta uhasta, he osaisivat myös siihen reagoida oikein.

8 Mahdolliset jatkotoimenpiteet

Kyselyn tuloksista selvisi, että suurin osa yrityksen henkilöstöstä tietää tietoturvan perusasiat, ja sen mitä tietoturvahäiriön sattuessa pitäisi toimia. Kysely ei herättänyt mitään suurta huolenaihetta yrityksen henkilöstön koulutuksesta ja tietämyksestä, on yrityksen menetelmissä silti kehittämisen varaa.

Koulutuksissa pitää panostaa siihen, että se sisältäisi enemmän esimerkkejä ja vaatisi käyttäjiltä enemmän aktiivisuuta. Nykyinen koulutus ei vaadi käyttäjältä paljoakaan sen suorittamiseksi. Tietoturva- ja tietosuojakoulutukset ovat tärkeitä asioita, joten niiden toteuttaminen on kannattavaa tehdä hyvin. Kun henkilöstö tietää selvästi yrityksen ohjeistuksen, on henkilöstön työnteko helpompaa.

Kyselyn kautta selvisi myös se, että henkilöstön mielestä selvästi paras koulutustapa olisi verkkokoulutukset ja kyseinen koulutusmuoto onkin yrityksellä käytössä. Asiakaspalvelupuolella 34 % vastaajista kannattivat myös videotallenteiden muodossa olevaa koulutusta. ICT-puolella 52 % vastaajista kannatti interaktiivista simulaatiota. Interaktiivisen simulaation avulla käyttäjät pääsivät käytännössä kokeilemaan mitä tietoturvauhan sattuessa pitäisi toimia. Tästä eniten hyötyisi ICT-puoli, koska heille voi tulla tietoturvauhkien hoitamista eteensä. Videotallenteet taas voisivat olla osa verkkokoulutusta, vaikka esimerkkien muodossa. Esimerkki videoita voisi sijoittaa koulutuksessa kohtiin, jossa kerrotaan miten käyttäjien pitäisi tietyssä tilanteessa toimia, ja tähän yhdistettäisiin video, josta näkee mitä ohjeistus käytännössä tarkoittaa.

Tärkein lisä koulutukseen olisi ruotsinkielisen koulutuksen lisääminen. Nykyisestä koulutusmateriaalista löytyy ruotsiksi vain kertauskoulutuksen materiaali, mutta ei tietoturva- tai tietosuojakoulutusta. Tietosuoja- ja tietoturvapolitiikat kannattaisi myös olla ruotsiksi. Nykyisiin koulutuksiin pitäisi myös lisätä lisää interaktiivisia kohtia esim. tehtäviä ja kysymyksiä. Koulutuksia parantaisi myös osa, jossa kerrotaan mitä asioita käyttäjät eivät saa tietyissä

tilanteissa tehdä. Näin ollen käyttäjä saa selvän tiedon siitä, mitä ei saa tehdä ja mitä saa tehdä.

Kyselyn perusteella oma koulutus jokaiselle liiketoiminta-alueelle ei ole tarpeellista. Jokaisen liiketoiminta-alueen vastaajista enemmistö oli sitä mieltä, että nykyinen koulutus on valmistanut heidät tunnistamaan ja reagoimaan tietoturvauhkiin hyvin.

9 Lopuksi

Opinnäytetyön tavoitteena oli auttaa yritystä selvittämään oman henkilöstönsä tietoturvatietämystä ja samalla selvittää se, onko nykyinen tietoturvakoulutus riittävä nykyisessä muodossaan, vai tarvitseeko se muokkausta. Tutkimuksen suorittamiseksi henkilöstölle luotiin verkkokysely, joka sisälsi kysymyksiä yleisesti tietoturvasta ja yrityksen omista tietoturva- ja tietosuojakoulutuksista. Kysely luotiin niin, että pystytiin selvittämään jokaisen liiketoiminta-alueen henkilöstön tietämys erikseen. Kyselyn lisäksi perehdyttiin yrityksen tietoturva- ja tietosuojapolitiikkaan, ohjeistukseen ja koulutuksiin.

Tutkimuksen alkuvaiheessa hankaluutta tuotti kysymysten luominen. Kysymysten oli tärkeää olla sellaisia, että niillä pystytiin selvästi näkemään ja arvioimaan henkilöstön tietoturvatietämys.

Kysely lähetettiin koko henkilöstölle, paitsi yrityksen johdolle. Kyselyyn vastasi 181 henkilöä ja vastausprosentti oli 56 %. Kyselyn avulla saatiin selvyyttä yrityksen henkilöstön tietoturvatietämys tasosta ja kyselyn perusteella henkilöstön tietämys on yleistasolla hyvä. Millään liiketoiminta-alueella ei ollut suuria heikkouksia, eikä näiden alueiden tietämykset eronneet toisistaan suuresti. Kyselystä selvisi kuitenkin pieniä puutteita, jotka pystytään korjaamaan päivitetyllä koulutuksella.

Tutkimuksessa selvisi, että yritykseltä puuttuu tietoturva- ja tietosuojakoulutukset ja tieto- ja tietosuojapolitiikat ruotsiksi, ja on vain yksi koulutus koko henkilöstölle. Kyselyn perusteella erillisille koulutuksille ei kuitenkaan ole tarvetta, mutta koulutukset ja politiikat tullaan tekemään tulevaisuudessa myös ruotsiksi.

Opinnäytetyön ansiosta yrityksen on helpompi lähteä päivittämään nykyisiä tietoturva- ja tietosuojakoulutuksiaan ja yrityksellä on selvää tietoa siitä, mihin osa-alueisiin koulutuksessa pitää panostaa. Kysely myös selvitti henkilöstön mielestä parhaan oppimismuodon, joten yrityksellä on nyt selvä käsitys, miten nykyiset koulutukset kannattaa päivittää.

Lähteet

Euroopan komissio 2023. Direktiivi toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa (NIS2-direktiivi) digital-strategy.ec.europa.eu. Viitattu 27.3.2024. https://digital-strategy.ec.europa.eu/fi/policies/nis2-directive

Euroopan parlamentin ja neuvoston asetus 2016/679/EU, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti). Viitattu 2.4.2024. https://eur-lex.europa.eu/FI/legal-content/summary/general-data-protection-regulation-gdpr.html

Europa 2022. Yleinen tietosuoja-asetus. Europa.eu. Viitattu 27.3.2024. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Jurvanen, L. 2024. Mitä tarkoittaa tietoturvan käytettävyys eli saatavuus? Savelan. Viitattu 23.3.2024. https://www.savelan.fi/mita-tarkoittaa-tietoturvan-kaytettavyys-eli-saatavuus/

Järvinen, P. 2022. Yrityksen tietoturvaopas. Helsinki: Kauppakamari. Viitattu 23.4.2024. https://kauppakamaritieto-fi.ezproxy.turkuamk.fi/ammattikirjasto/teos/yrityksen-tietoturvaopas-2022#kohta:Yrityksen((20)tietoturvaopas. Vaatii käyttäjätunnuksen.

Luoma, I. 2024. NIS2 direktiivi astuu voimaan lokakuussa 2024. CGI. Viitattu 27.4.2024. https://www.cgi.com/fi/fi/blogi/tietoturva-ja-kyberturvallisuus/nis2-direktiivi-astuu-voimaan-lokakuussa-2024

Perttunen, A. 2023. Tietoturvakoulutuksen merkitys organisaatiolle. Micro magic. Viitattu 27.3.2024. https://micromagic.fi/story/tietoturvakoulutuksen-merkitys-organisaatioille/

Tietosuojavaltuutetun toimisto n.d. Tietosuoja. Tietosuoja.fi -sivusto. Viitattu 2.4.2024. https://tietosuoja.fi/tietosuoja

Toimeksiantajan ohjeistukset 2023. Tietosuojapolitiikka. Viitattu 3.4.2024

Toimeksiantajan ohjeistukset 2023. Tietoturvapolitiikka. Viitattu 3.4.2024

Tietoturvakyselyn kysymykset ja vastausvaihtoehdot

1. Valitse liiketoiminta-alueesi
    - Contact Center
    - ICT
    - Tietoliikenne
    - Hallinto
2. Sinun on keksittävä uusi salasana, minkä keksit?
    - tammikuu22
    - Tammikuu22
    - !Tammikuu2!
    - #T4mM!kUz29!
    - Qwerty123!
    - Salasana123!
    - SimmottisTääHoituu
3. Missä säilytät järjestelmiesi salasanoja?
    - Selaimeni tallentaa ne automaattisesti
    - Password bossissa
    - Paperilla työpöydälläni
    - Työpöydälläni olevassa vihossa
    - Käytän yhtä ja samaa salasanaa, minkä muistan ulkoa
4. Järjestelmä kertoo salasanani vanhentuneen, mitä teen.
    - Vaihdan salasanani johonkin samanlaiseen kuin nykyinen salasanani on
    - Soitan Service Deskiin ja pyydän heitä pidentämään salasanani käyttöaikaa
    - Vaihdan salasanani kokonaan uuteen ja monimutkaiseen salasanaan
5. Työkaverini tunnukset menevät lukkoon ja hän pyytää neuvoani, mitä teen?
    - Ei ole minun ongelmani

- Annan omat tunnukseni hänen käyttöönsä
- Neuvon olemaan yhteydessä Service Deskiin

6. Soittava asiakas pyytää itselleen järjestelmänvalvojan tunnuksia, mitä teen? (kysymys vain ICT-puolelle)
    - Luon asiakkaalle omat admin tunnukset
    - En tee mitään
    - Kerron asiakkaalle omat admin tunnukseni
    - Selvitän asiaa hänen esihenkilönsä kanssa
    - Kerron asiakkaalle perustietolomakkeella olevan admin tunnuksen
7. Olet tuonut asiakkaalle tunnukset, miten toimitat ne hänelle? (kysymys vain ICT-puolelle)
    - Soitan asiakkaalle ja kerron tunnukset
    - Lähetän ne henkilölle tekstiviestinä
    - Lähetän ne tilaajan sähköpostiin
    - Lähetän ne tilaajan sähköpostiin salattuna
    - Työnkuvaani ei kuulu tunnusten luominen
    - Lähetän ne uuden henkilön henkilökohtaiseen sähköpostiin
8. Havaitset tietoturvahäiriön, mitä teet?
    - Otan asian puheeksi, jos joku siitä puhuu
    - Ilmoitan asiasta heti työkaverilleni
    - Ilmoitan asiasta heti esihenkilölleni tai tietoturvavastaavalle
    - Asia ei kuulu minulle, en tee mitään
    - Minulla on kiire ja tärkeämpääkin tekemistä, ilmoitan asiasta jollekin, kun kerkeän
9. Tietokoneeni ilmoittaa virustorjunnan olevan pois päältä, mitä teen?
    - En mitään, kyllä se siitä päälle tulee
    - Käynnistän koneeni uudelleen
    - Ilmoitan Service Deskille asiasta
    - Minulla on oikeudet laittaa se takaisin päälle (ICT)
10. Löydät konttorin tiloista yksinäisen muistitikun, mitä teet?

- Laitan muistitikun näkyvälle paikalle, että sen omistaja mahdollisesti löytää sen
- Otan tikun mukaani ja laitan sen kiinni koneeseeni, yrittäen selvittää sen sisällöstä kenelle se kuuluisi
- En tee mitään
- Otan tikun talteen ja ilmoitan Service Deskille tai esihenkilölleni löydöstä

11. Esihenkilöltäsi tulee sähköpostia, jossa hän pyytää sinua hankkimaan lahjakortteja firman juhliin. Mitä teet?
    - Soitan Service Deskiin asiasta
    - Tarkistan lähettäjän sähköposti osoitteen
    - Lähden heti ostamaan pyydettyjä lahjakortteja
    - Vastaan sähköpostiin kysyen, onko hän tosissaan
    - Soitan tiedossani olevaan esihenkilöni puhelinnumeroon tai käy hänen työpisteellään kysymässä viestistä
12. Saako tekoälyltä (esim. ChatGPT) kysyä työhöni liittyviä asioita?
    - Ei
    - Vain yleisiä, ei töihin liittyviä asioita
    - Tekoälyltä voi kysyä neuvoja kaikkeen
    - En tiedä
13. Mitä laitteita voit kytkeä työkoneeseesi?
    - Ihan mitä vain, minkä kiinni saa
    - Henkilökohtaisia laitteitani ja työpaikalta saatuja laitteita
    - Työpaikalta saatuja laitteita
14. Mitä puhtaan pöydän periaate tarkoittaa?
    - Että pöytäni on puhdas pölystä ja liasta työpäivän jälkeen
    - En tiedä
    - Että ylimääräisiä kahvikuppeja ei jätetä työpöydälle lojumaan työpäivän jälkeen
    - Että työpaperit laitetaan pois näkyvistä työpäivän jälkeen
    - Ei mitään näistä

15. Poistun työpisteeltäni, mitä teen?
    - En mitään
    - Otan mahdolliset tyhjät kahvikuppini mukaan ja vien ne pesukoneeseen
    - Lukitsen koneeni
    - Sammutan näyttöni
16. Olet löytänyt loistavan ohjelmiston, joka auttaisi minua työnteossa, mitä teen?
    - Asennan sen pikimiten koneelleni, ei tälläisestä asiasta tarvitse ketään häiritä
    - Kerron työkavereilleni kaiken tästä ohjelmasta ja kannustan heitä sen asentamisessa
    - Kysyn ohjelmiston asentamisesta lupaa esihenkilöltäni
17. Etätyöntekijä, millaisessa tilassa teet töitä?
    - Asun yksin, joten työskentelen missä tahdon
    - Keittiön pöydällä, siinä on eniten tilaa
    - Olohuoneessa, jotta voin olla mukana perheeni arjessa työpäivän aikana
    - Erillisessä huoneessa ovi auki, jotta kuulen jos joku tarvitsee minua
    - Erillisessä huoneessa ovi kiinni, jotta saan keskittyä paremmin
    - En tee etätöitä
18. Mihin kaikkeen voin työsähköpostiani käyttää?
    - Ihan mihin vain
    - Työ asioihin ja henkilökohtaisiin tärkeisiin asioihin
    - Työ asioihin
19. Millä näppäin yhdistelmällä lukitsen koneeni?
    - Ctrl + C
    - Windows näppäin + X
    - Ctrl + Alt + Shift +Windows näppäin+ L
    - Ctrl + Alt + nuoli vasemmalle

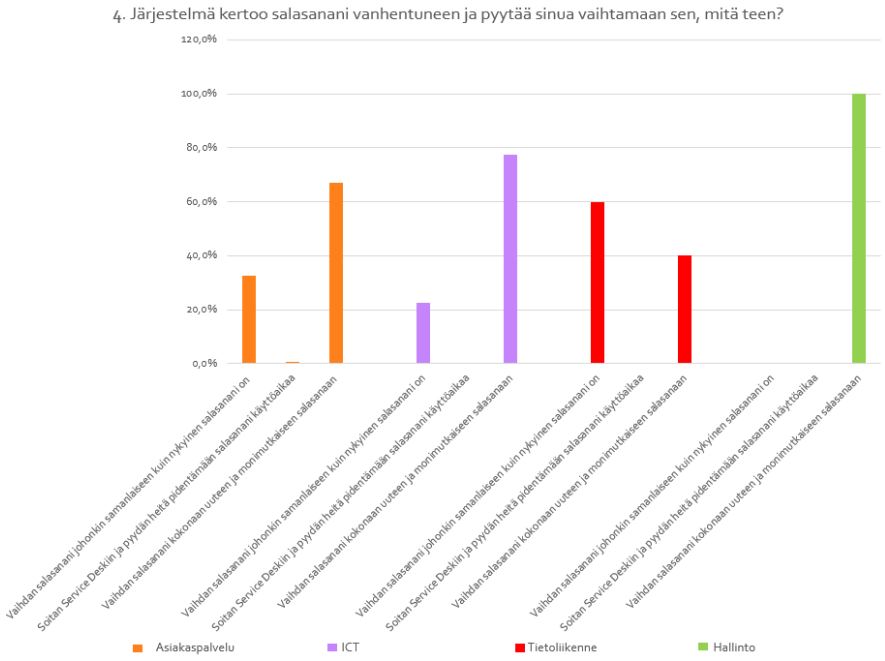
- Windows näppäin + L
- Windows näppäin + P
- Jokin muu, mikä

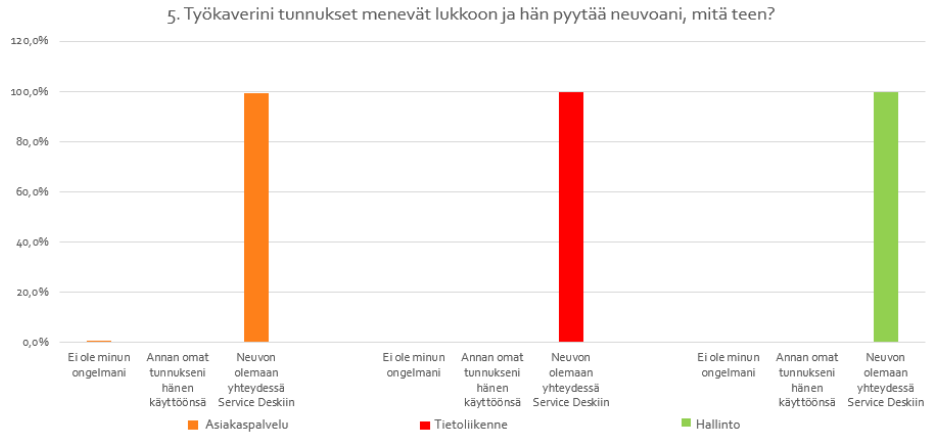
20. Henkilö on tulossa huoltamaan palvelinkeskuksessa olevaa järjestelmää, mitä teen? (Kysymys vain ICT ja tietoliikenne puolille.)
    - Minulla ei ole oikeuksia päästä palvelin huoneeseen tai tälläisiä tilanteita ei tule minulle
    - Päästän henkilön sisälle ja pyydän häntä soittamaan minulle kun on valmis
    - En päästä häntä sinne, en mitenkään voi luottaa tähän henkilöön
    - Päästän hänet sisälle ja olen hänen kanssaan koko operaation ajan.
21. Tiedän mitä minun pitää tehdä, jos havaitsen tietomurron.
    - Kyllä
    - En
22. Milloin viimeksi olet suorittanut työpaikan tarjoaman tietoturvakoulutuksen?
    - Kun tulin taloon alle 6 kuukautta sitten
    - Kun tulin taloon yli 6 kuukautta sitten
    - Kun tulin taloon yli vuosi sitten
    - Kun tulin taloon yli kolme vuotta sitten
    - Tein kertauskoulutuksen noin puoli vuotta sitten
    - Tein kertauskoulutuksen noin vuosi sitten
    - En muista
    - En ole koskaan tehnyt semmoista
23. Koetko, että nykyinen tietoturvakoulutus on riittävän kattava sinun työtehtäviisi liittyen?
    - Kyllä
    - En
24. Mistä löydät yrityksen tietoturvapolitiikan?
25. Miten hyvin nykyinen tietoturvakoulutus on valmistanut sinut tunnistamaan ja reagoimaan tietoturvauhkiin?

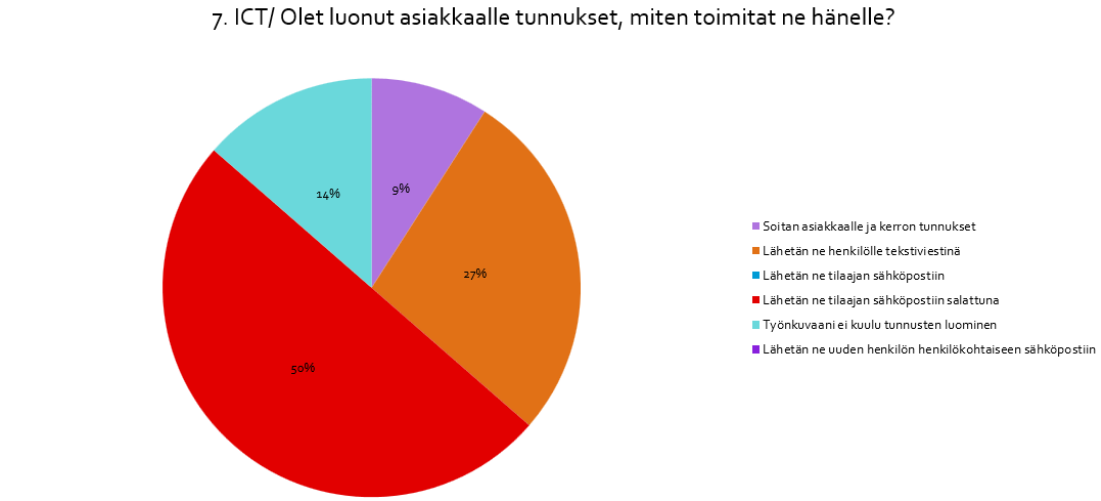
- Loistavasti
- Hyvin
- Keskivertoisesti
- Heikosti
- Huonosti

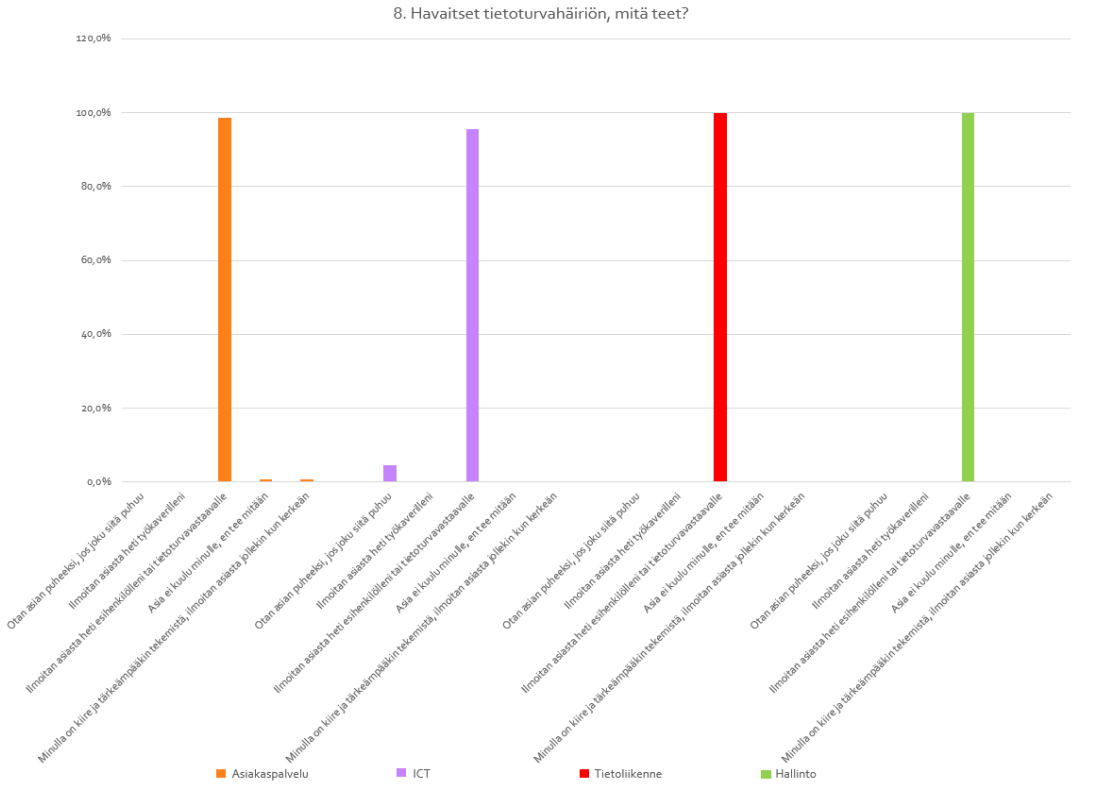
26. Miten arvioisit nykyisen tietoturvakoulutuksen selkeyttä ja ymmärrettävyyttä?
27. Millainen koulutusmuoto tukisi parhaiten sinun oppimistasi?
    - Verkkokoulutukset
    - Kasvokkaiset workshopit
    - Videotallenteet
    - Interaktiivinen simulaatio
    - Jokin muu, mikä
28. Miksi tietoturva on tärkeää yrityksemme kannalta?

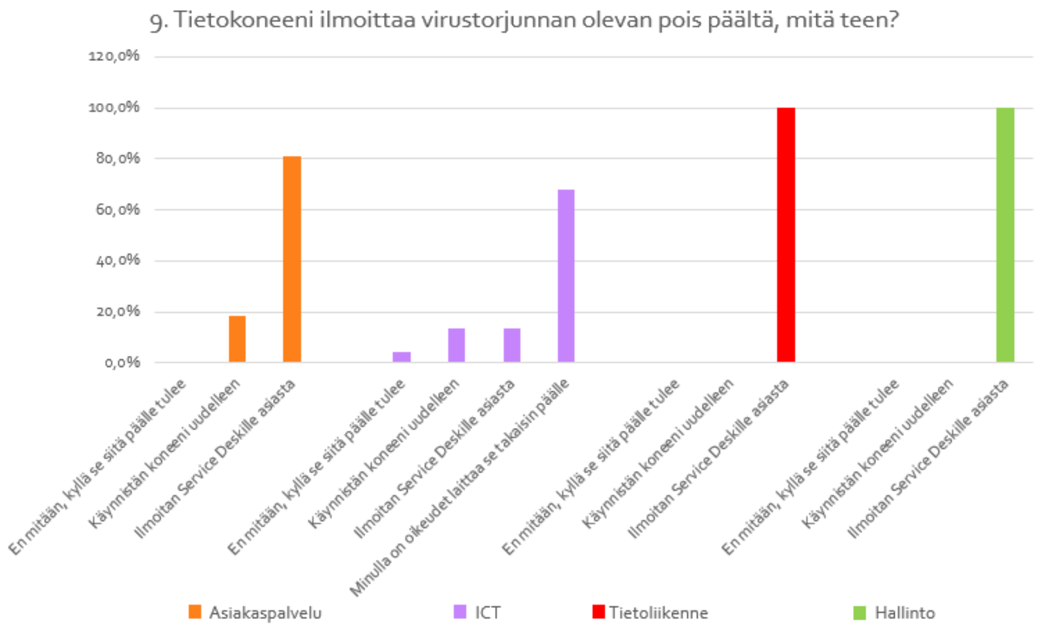
Tietoturvakyselyn tulokset

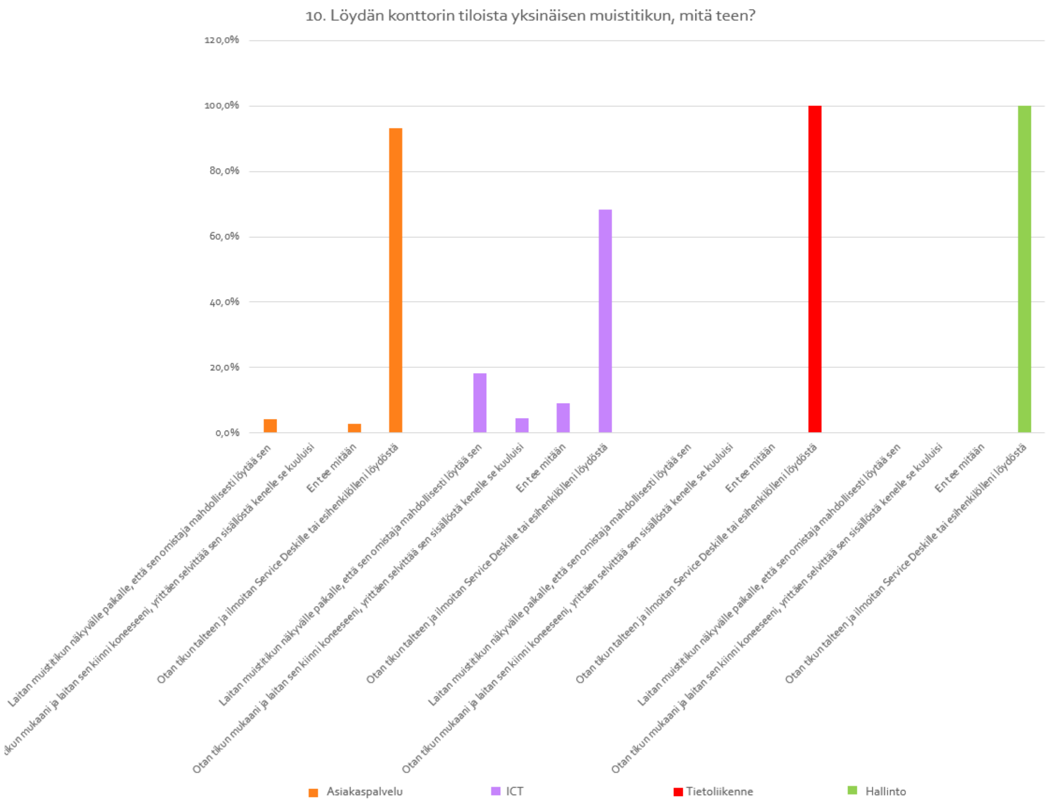


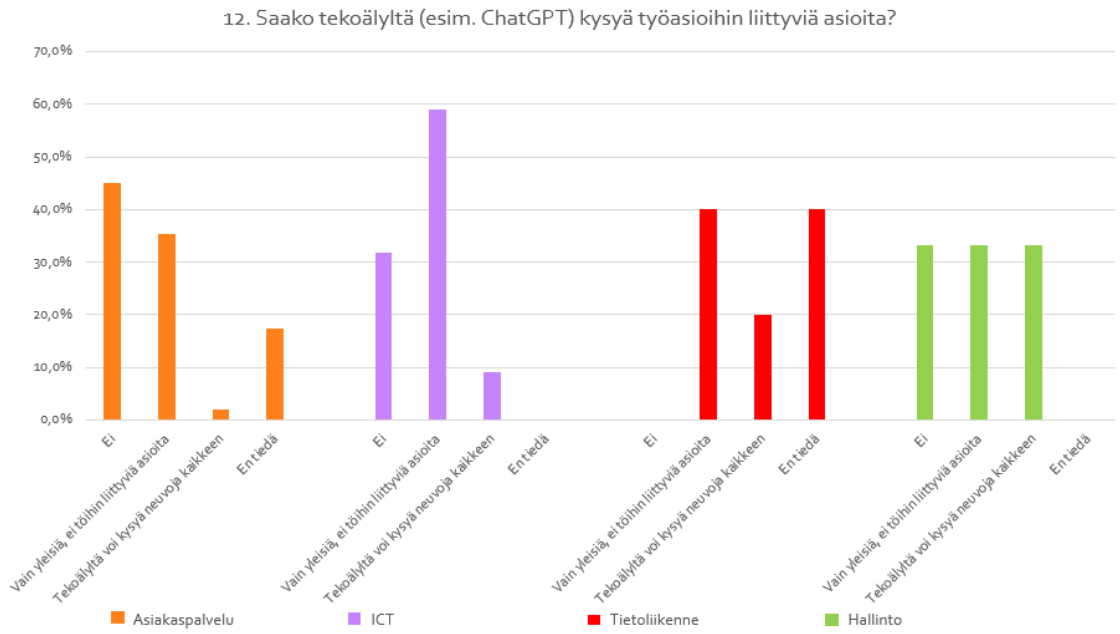


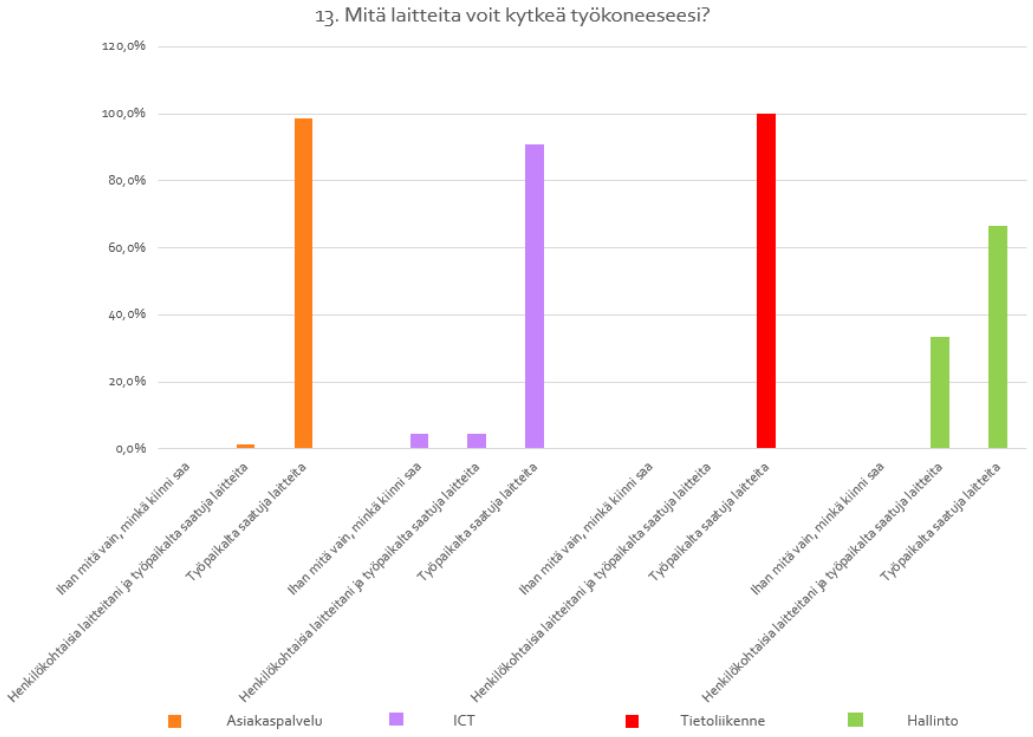

7. ICT/ Olet luonut asiakkaalle tunnukset, miten toimitat ne hänelle?
9%
27%
50%
14%
Soitan asiakkaalle ja kerron tunnukset
Lähetän ne henkilölle tekstiviestinä
Lähetän ne tilaajan sähköpostiin
Lähetän ne tilaajan sähköpostiin salattuna
Työnkuvaani ei kuulu tunnusten luominen
Lähetän ne uuden henkilön henkilökohtaiseen sähköpostiin


8. Havaitset tietoturvahäiriön, mitä teet?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
Otan asian puheeksi, jos joku siitä puhuu
Ilmoitan asiasta heti työkaverilleni
Ilmoitan asiasta heti esihenkilölleni tai tietoturvavastaavalle
Asia ei kuulu minulle, en tee mitään
Minulla on kiire ja tärkeämpääkin tekemistä, ilmoitan asiasta jälkikin kun kerkeän
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto

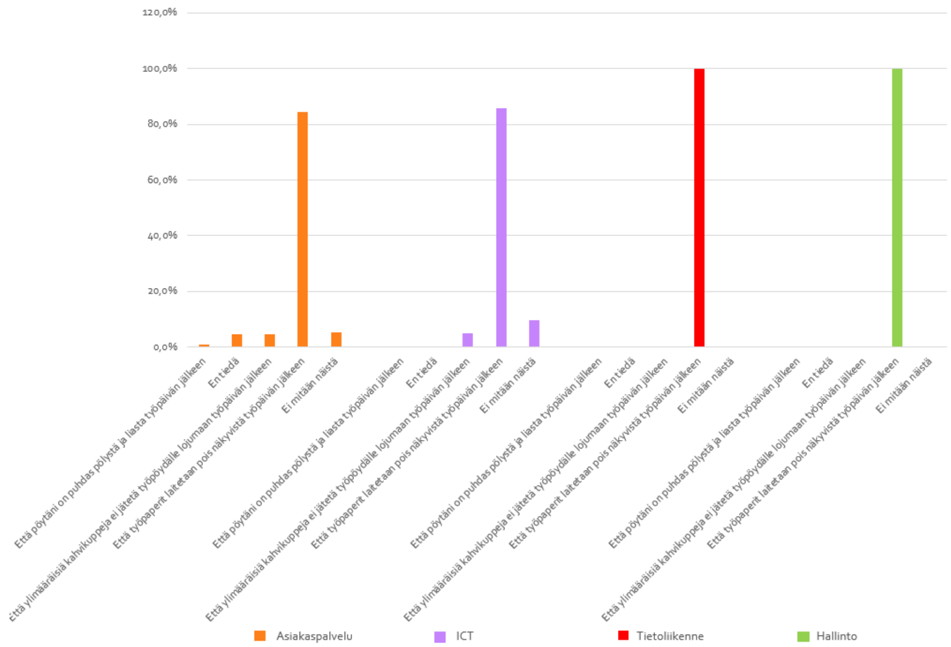

9. Tietokoneeni ilmoittaa virustorjunnan olevan pois päältä, mitä teen?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
En mitään, kyllä se siitä päälle tulee
Käynnistän koneeni uudelleen
Ilmoitan Service Deskille asiasta
En mitään, kyllä se siitä päälle tulee
Käynnistän koneeni uudelleen
Ilmoitan Service Deskille asiasta
Minulla on oikeudet laittaa se takaisin päälle
En mitään, kyllä se siitä päälle tulee
Käynnistän koneeni uudelleen
Ilmoitan Service Deskille asiasta
En mitään, kyllä se siitä päälle tulee
Käynnistän koneeni uudelleen
Ilmoitan Service Deskille asiasta
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto


10. Löydän konttorin tiloista yksinäisen muistitikun, mitä teen?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
Laitan muistitikun näkyvälle paikalle, että sen omistaja mahdollisesti löytää sen
ikun mukaani ja laitan sen kiinni koneeseeni, yrittäen selvittää sen sisällöstä kenelle se kuuluisi
En tee mitään
Otan tikun talteen ja ilmoitan Service Deskille tai esihenkilölleni löydöstä
Laitan muistitikun näkyvälle paikalle, että sen omistaja mahdollisesti löytää sen
Otan tikun mukaani ja laitan sen kiinni koneeseeni, yrittäen selvittää sen sisällöstä kenelle se kuuluisi
En tee mitään
Otan tikun talteen ja ilmoitan Service Deskille tai esihenkilölleni löydöstä
Laitan muistitikun näkyvälle paikalle, että sen omistaja mahdollisesti löytää sen
Otan tikun mukaani ja laitan sen kiinni koneeseeni, yrittäen selvittää sen sisällöstä kenelle se kuuluisi
En tee mitään
Otan tikun talteen ja ilmoitan Service Deskille tai esihenkilölleni löydöstä
Laitan muistitikun näkyvälle paikalle, että sen omistaja mahdollisesti löytää sen
Otan tikun mukaani ja laitan sen kiinni koneeseeni, yrittäen selvittää sen sisällöstä kenelle se kuuluisi
En tee mitään
Otan tikun talteen ja ilmoitan Service Deskille tai esihenkilölleni löydöstä
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto

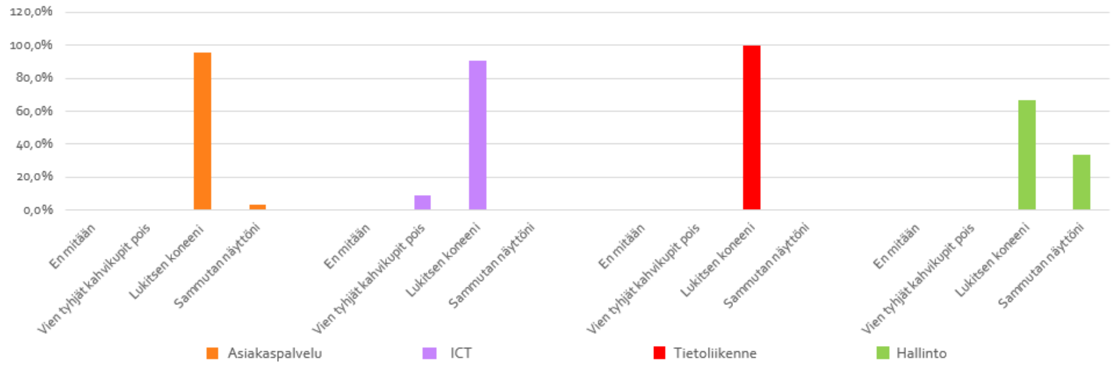

12. Saako tekoälyltä (esim. ChatGPT) kysyä työasioihin liittyviä asioita?
70,0%
60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
Ei
Vain yleisiä, ei töihin liittyviä asioita
Tekoälyltä voi kysyä neuvoja kaikkeen
En tiedä
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto


13. Mitä laitteita voit kytkeä työkoneeseesi?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
Ihan mitä vain, minkä kiinni saa
Henkilökohtaisia laitteitani ja työpaikalta saatuja laitteita
Työpaikalta saatuja laitteita
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto

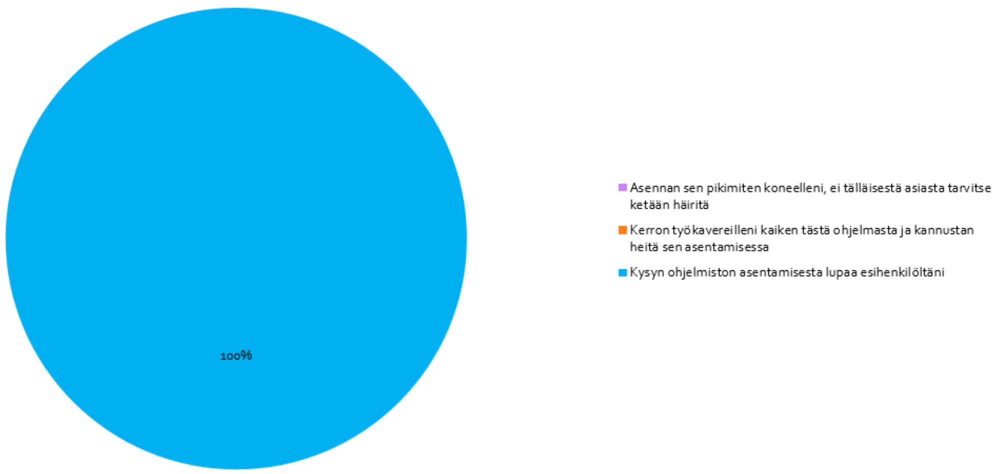
14. Mitä puhtaan pöydän periaate tarkoittaa?

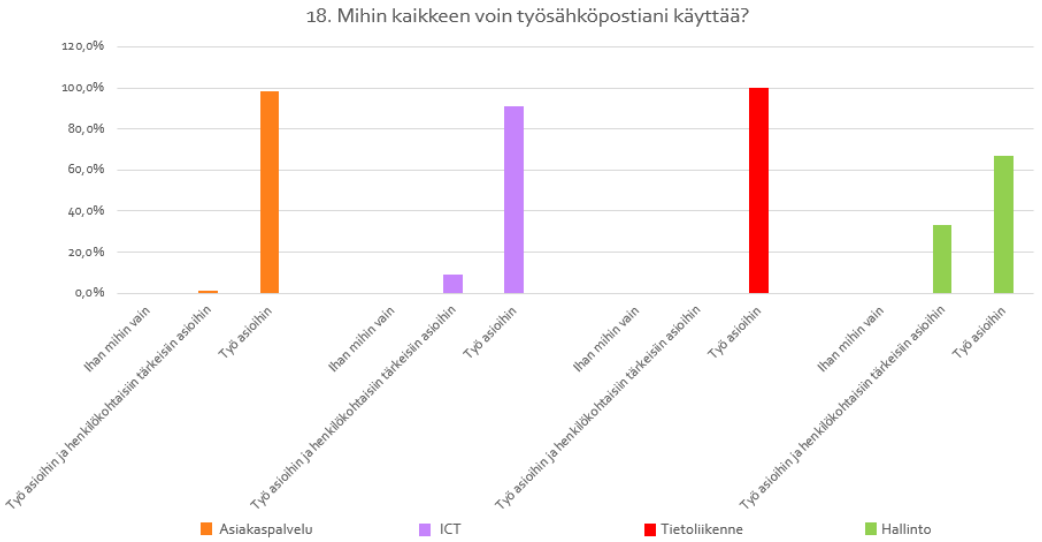


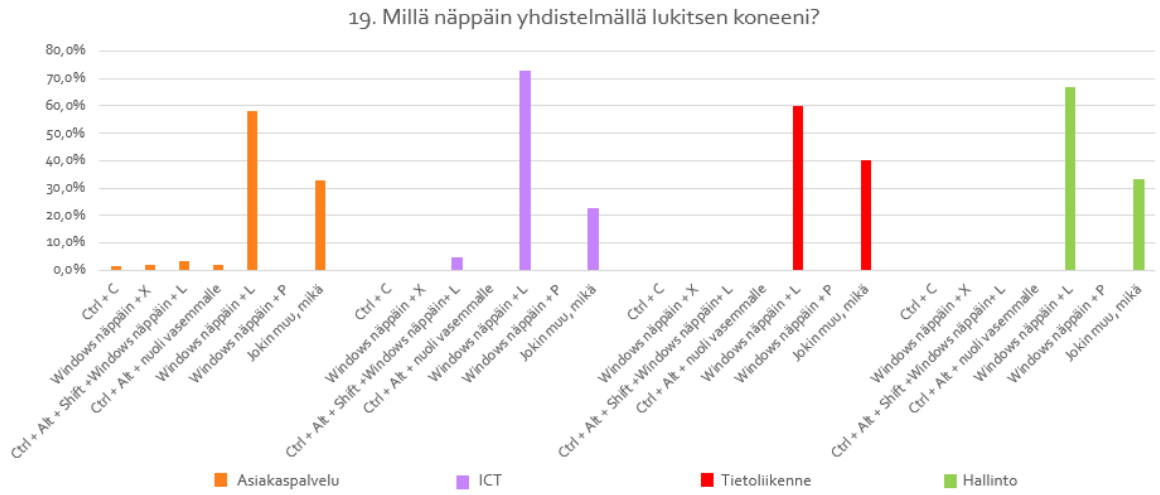
15. Poistun työpisteeltäni, mitä teen?



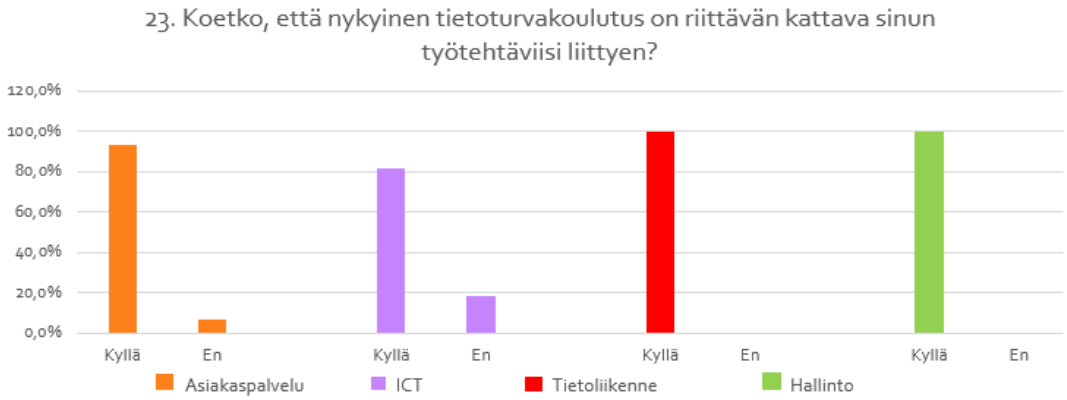
16. CC/Olen löytänyt loistavan ohjelmiston, joka auttaisi minua työnteossa, mitä teen?

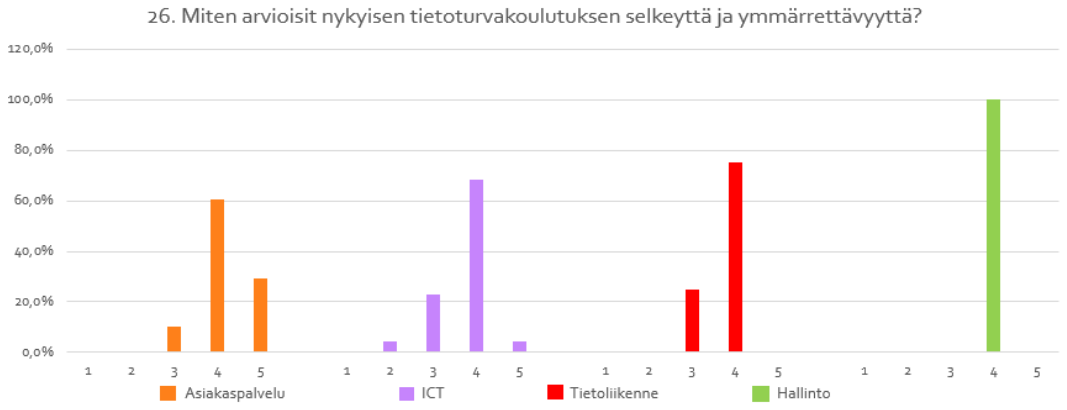



18. Mihin kaikkeen voin työsähköpostiani käyttää?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
Ihan mihin vain
Työ asioihin ja henkilökohtaisiin tärkeisiin asioihin
Työ asioihin
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto


19. Millä näppäin yhdistelmällä lukitsen koneeni?
80,0%
70,0%
60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
Ctrl + C
Windows näppäin + X
Ctrl + Alt + Shift +Windows näppäin + L
Ctrl + Alt + nuoli vasemmalle
Windows näppäin + L
Windows näppäin + P
Jokin muu, mikä
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto


20. Henkilö on tulossa huoltamaan palvelinkeskuksessa olevaa järjestelmää, mitä teen?
90,0%
80,0%
70,0%
60,0%
50,0%
40,0%
30,0%
20,0%
10,0%
0,0%
Minulla ei ole oikeuksia päästä palvelin huoneeseen tai tälläisiä tilanteita ei tule minulle
Päästän henkilön sisälle ja pyydän häntä soittamaan minulle kun on valmis
En päästä häntä sinne, en mitenkään voi luottaa tähän henkilöön
Päästän hänet sisälle ja olen hänen kanssaan koko operaation ajan.
ICT
Tietoliikenne


23. Koetko, että nykyinen tietoturvakoulutus on riittävän kattava sinun työtehtäviisi liittyen?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
Kyllä
En
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto


26. Miten arvioisit nykyisen tietoturvakoulutuksen selkeyttä ja ymmärrettävyyttä?
120,0%
100,0%
80,0%
60,0%
40,0%
20,0%
0,0%
1 2 3 4 5
Asiakaspalvelu
ICT
Tietoliikenne
Hallinto