Tietoturvatietoisuuden tason kartoittaminen ja kehityskohteiden selvittäminen yrityksessä X

Meri Penttinen

2022 Laurea

Laurea-ammattikorkeakoulu

Tietoturvatietoisuuden tason kartoittaminen ja kehityskohteiden selvittäminen yrityksessä X

Meri Penttinen

Turvallisuusjohtaminen

Opinnäytetyö

Kesäkuu, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusjohtamisen koulutus
Tradenomi (YAMK)

Meri Penttinen

Tietoturvatietoisuuden tason kartoittaminen ja kehityskohteiden selvittäminen yrityksessä X

Vuosi 2022 Sivumäärä 74

Tämän opinnäytetyön tarkoituksena oli selvittää, henkilöstön tietoturvatietoisuuden taso ja tasoon vaikuttavat tekijät yrityksessä X. Tutkimuksen avulla haluttiin myös laatia kehittämissuunnitelma kohdeorganisaation tietoturvatietoisuuden parantamiseksi ja ylläpitämiseksi. Tämä opinnäytetyö oli tyypiltään tutkimukseen perustuva kehittämishanke.

Opinnäytetyön teoreettinen viitekehys koostui tietoturvan perusteista, tietoturvasuunnittelusta, yleisimmistä tietoturvariskeistä sekä tietoturvatietoisuudesta. Tietoturvan perusteisiin liittyvässä teoriassa käsiteltiin monipuolisesti tietoturvaan liittyviä lakeja ja säännöksiä, sekä tutustuttiin tietoturvan eri osa-alueisiin. Tietoturvasuunnittelussa tutustuttiin tietoturvanhallinta järjestelmään, tietoturvapolitiikkaan sekä tietoturvasuunnitteluun. Tietoturvatietoisuuden teoriassa tarkasteltiin aiheen mittaamista ja kehittämistä sekä tutustuttiin Krugerin ja Kearneyn mittausmenetelmään sekä Martinsin ja Elfin teoriaan aiheesta.

Tämän työn tutkimus toteutettiin sähköisenä kyselynä, joka lähetettiin vastattavaksi kaikille kohdeyrityksen Suomen organisaatiossa työskenteleville henkilöille. Viitekehyksen avulla rakennettiin tietoturvatietoisuuden selvittämiseen käytettävä kyselylomake, joka koostui kolmesta aihealueesta. Nämä aihealueet olivat tietoturvapolitiikka – ja ohjeistus, asenne ja käyttäytyminen sekä tietous. Tämän lisäksi vastaajien taustatiedot kartoitettiin. Kyselyssä vastaajille esitettiin väittämiä ja monivalintakysymyksiä, joista vastaajien tuli valita omaa tietämystä tai mielipidettä vastaava vaihtoehto. Näiden vastausten avulla selvitettiin työntekijöiden tietämystä, asenteita ja käyttäytymistä liittyen tietoturvaan.

Opinnäytetyön tuloksista oli havaittavissa, että tietoisuuden taso organisaatiossa on suhteellisen korkea, mutta asenteet ja käyttäytyminen liittyen tietoturvaan on heikompaa. Työn tutkimuksen tulosten sekä viitekehyksen perusteella tehtiin johtopäätökset tietoturvatietoisuudesta ja luotiin kehitysideoita sen parantamiseksi.

Asiasanat: tietoturva, tietoturvatietoisuus, tietoturvapolitiikka

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Master of Business Administration

Meri Penttinen

Inspecting the Level of Information Security Awareness and Identifying Areas for Development in Company X

Year 2022 Pages 74

The purpose of this thesis was to identify employees' information security awareness level in company X and recognise the factors affecting the level of information security awareness. The aim of the study was to build a development plan to improve and maintain the security awareness in company X. This thesis was a research-based development project.

Theoretical framework of the thesis consists the basics of information security, information security planning, the most common information security risks, and information security awareness. Various features of the basics of information security are introduced, as well as the laws and regulations related to information security were discussed from multiple aspects. In terms of information security planning, the information security management system, information security policy and information security planning were introduced. In the section where information security awareness is outlined, the measurement and development of the topic is examined, and the measurement method of Kruger and Kearney and the theory of Martins and Elf on the topic are introduced.

The research method used in this study was an electronic survey, which was sent to all employees working in company X's Finnish organization. The theoretical framework was used to construct a questionnaire for information security awareness, it consisted of three thematic areas including information security policy and guidance, attitudes and behaviour, and information security knowledge. In the survey, respondents were asked to answer various questions regarding information security. The responses to the questionnaire were used to gather data related to information security awareness in company X.

The results of the thesis showed that the level of information security awareness in organization X is relatively high, but attitudes and behaviour related to information security are weaker. Based on the results of the research and the theoretical framework, conclusions were made about the information security awareness level, and development ideas were created to improve and maintain information security awareness.

Keywords: information security, information security knowledge, information security policy

Sisällys

1 Johdanto

Tietoturvakysymykset nostettiin organisaatioissa esille jo kauan ennen tekniikan nopeaa kehitystä. Yritykset ovat aina olleet huolissaan luottamuksellisten tietojensa ja liikesalaisuuksien suojaamisesta. Kaikilla organisaatioilla on omaisuutta, joka auttaa yritystä menestymään liiketoiminnallisesti sekä tuottamaan tuloja. Tietoturvan tavoitteena on tunnistaa ja suojata nämä tiedot ja tällä tavalla varmentaa yrityksen toiminta. (Zinatullin 2016, 13.)

Nykyään verkkohuijarit eivät yritä murtautua palomuurin läpi vaan he kiertävät ketterästi palomuurit. Organisaatiot ovat investoineet runsaasti rahaa kehittääkseen moninaisia puolustuskeinoja verkkohuijareita vastaan. Tietojen suojaamiseen on kehitetty monenlaisia ratkaisuja, kuten virustorjunta, tunkeutumisen havainnointijärjestelmät, tunkeutumisen estojärjestelmät ja muut tekniset ratkaisut. Näiden kehittyneiden ratkaisujen ansiosta hyökkääjät ovat nyt siirtyneet kohdistetumpiin hyökkäyksiin, jotka keskittyvät huijaamaan itse käyttäjiä ja iskemään tätä kautta organisaation tietoihin. (Gardner & Thomas 2014, 23.)

Tietoturvatietoisuuden tärkeys kasvaa kovaa vauhtia teknologian kehittyessä sekä ympäristön muuttuessa jatkuvasti. Tietoturva-ajattelun siirtyessä teknologisesta ihmisläheisemmäksi pystytään panostamaan enemmän ennaltaehkäisevään toimintaan ja tietoturvatietämyksen kehittämiseen. (Tietototurva 2021.) Suurin osa tapahtuneista tietomurroista- ja vuodoista tapahtuu ihmisten tekemien inhimillisten virheiden myötä, jonka vuoksi henkilöstön tietoturvatietoisuudella on merkittävä vaikutus toimivaan tietoturvaan. Tietoturvan tulisi olla osa johtamista ja sitä tulisi tarkastella positiivisena ja merkittävä tekijänä liiketoiminnalle. (Limnéll 2021.)

Tietoturva on käsitteenä moninainen, mutta sen pääasiallisena tarkoituksena on kehittää toimia, ohjeita sekä teknisiä ratkaisuja, jotka suojaavat määriteltyä tietoa. (VAHTI 2/2004, 15–16.) Tietoturva yksi tietosuojan toteutumisen perusta, joka kattaa sekä hallinnolliset että tekniset toimenpiteet. Tavoitteena on varmistaa tarvittavalle kohteelle tai tiedolle eheä ja luottamuksellinen suojaus riskien minimoimiseksi. (Andreasson, Riikonen, Ylipartanen 2017, 21.) Tietoturvatietoisuudella taas tarkoitetaan henkilöstön tietoisuutta ja ymmärrystä omasta toiminnasta ja käytännöistä tietoturvaan liittyen. Esimerkiksi selkeät toimintatavat ja ymmärrys liittyen etätyöhön, salauskäytäntöihin, sekä Internetin käyttöön työtehtävissä ovat olennaisia tietoturvatietoisuuteen liittyviä tekijöitä organisaatiossa. (Gardner, & Thomas 2014,1.)

Organisaation tietoturvapolitiikka ohjaa tietoturvan toteutumista ja vaikuttaa tietoturvankäytäntöihin ja ymmärrykseen organisaatiossa. Tietoturvapolitiikalla tarkoitetaan sääntöjä ja ohjeita, jotka määrittävät, kuinka resursseja ja omaisuutta tulee käyttää, hallita ja suojata. Tietoturvapolitiikan avulla voidaan sitouttaa niin johto kuin yrityksen henkilöstö seuraamaan

laadittuja linjauksia tietoturvaan liittyen. (Laaksonen ym. 2006, 146) Tietoturvapolitiikasta laaditaan julkinen dokumentti, jossa kerrotaan yrityksen säännöt, toimet ja linjaukset koskien tietoturvaa. (Hakala ym. 2006, 7–9)

1.1 Opinnäytetyön tavoite ja rajaus

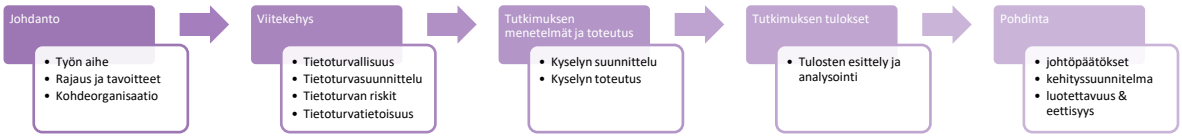
Tämän opinnäytetyön tavoitteena on tutkia kohdeorganisaation tietoturvatietoisuuden tasoa ja siihen vaikuttavia tekijöitä sekä esittää tutkimuksen pohjalta organisaatiolle kehittämisideoita tietoisuuden parantamiseksi. Tutkimuksen kohteena on selvittää miten työntekijät toimivat omissa rooleissaan tietoturvan näkökulmasta ja miten tietoisia he ovat omasta toiminnastaan. Opinnäytetyössä keskitytään niihin tietoturvan osa-alueisiin, jotka ovat kohdeorganisaation kannalta oleellisimpia ja joiden avulla voidaan selvittää tietoturvatietoisuuden yleistä tasoa yrityksessä.

Työ on rajattu tutkimaan kohdeorganisaation Suomen työntekijöiden tietoturvatietoisuutta. Tutkimus kohdistuu organisaation tietoturvaan liittyviään tietoisuuteen ja näin ollen muut turvallisuuden osa-alueet ovat jätetty pois tutkimuksesta. Tutkimuksessa tutkitaan yhdessä kaikkia kohderyhmässä työskenteleviä samalla kyselytutkimuksella. Työntekijöiden taustatiedot tai yksikkö ei vaikuta tutkimuksen sisältöön.

1.2 Opinnäytetyön rakenne

Opinnäytetyö on rakennettu alla olevan kuvion (kuvio 1) mukaisesti. Työ alkaa johdannolla, eli aiheen ja kohdeorganisaation esittelyllä. Seuraavaksi työn viitekehyksessä perehdytään tietoturvallisuuteen yleisellä tasolla, tietoturvan suunnitteluun ja sen yleisimpiin riskeihin sekä käsitellään tietoturvatietoisuuden mittaamista ja kehittämistä.

.



Kuvio 1: Opinnäytetyön rakenne

Tutkimusmenetelmäluvussa tarkastellaan opinnäytetyössä hyödynnettyä tutkimusmenetelmää ja perehdytään tutkimuksen suunnitteluun sekä toteutukseen. Seuraavassa osiossa käsitellään kyselytutkimuksen tuloksia ja analysoidaan niitä erilaisten kuvioiden sekä tunnuslukujen avulla. Työn viimeisessä osiossa tehdään johtopäätökset tietoturvatietoisuuden tilasta ja kehitys-

kohteista kohdeorganisaatiossa sekä laaditaan kehitysehdotus kohdeorganisaatiolle tietoturvatietoisuuden parantamiseksi. Tämän lisäksi viimeisessä luvussa käsitellään myös työn luotettavuutta, eettisyyttä sekä työn onnistumista kokonaisuudessaan

1.3 Kohdeorganisaation esittely

Tämän opinnäytetyön tutkimus tehdään anonyymisti kohdeorganisaation pyynnöstä. Tutkimuksen kannalta on oleellista tietää, että tutkimuksen kohteena olevan organisaation työntekijät toimivat pääosin asiantuntijatehtävissä ja työtehtävät tehdään toimistoympäristössä tai etätyönä työntekijän omasta kodista. Monet yrityksen työntekijät käsittelevät henkilötietoja tai asiakastietoja työssään päivittäin ja organisaatiossa käytetään myös monia eri tietoteknisiä järjestelmiä työn toteuttamiseen.

Kohdeorganisaatiolla on pääkonttorit Suomesta, Ruotsista sekä Iso-Britanniasta ja asiakkaita yritykseltä löytyy maailmanlaajuisesti. Työntekijöitä organisaatiossa on tällä hetkellä noin 150, joista 82 työskentelee Suomen organisaatiossa.

Opinnäytetyössä tutkitaan yrityksen Suomen henkilöstön tietoturvatietoisuutta, jota ei ole aikaisemmin kyseisessä yrityksessä tutkittu. Lähtötilanne tietoturvaan liittyvien dokumenttien ja koulutusten kannalta on myös olennainen. Kohde organisaatiosta löytyy turvallisuuspolitiikka sekä turvallisuusohjeistus, jossa käsitellään tietoturvallisuutta yleisellä tasolla. Organisaation perehdytys tai koulutusohjelmaan ei tällä hetkellä kuulu puhtaasti tietoturvaan liittyviä koulutuksia.

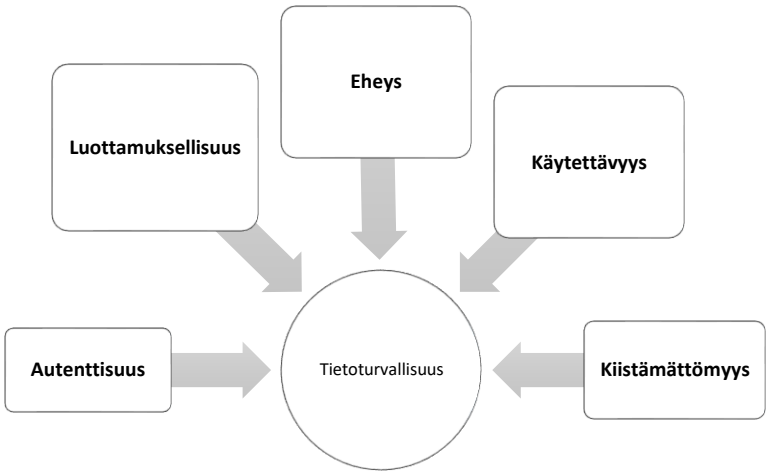
2 Tietoturvan perusteet

Tietoturvallisuus on käsitteenä moninainen ja se sisältää monia erilaisia toimia ja toimintoja toteutuakseen. Tietoturva ei tarkoita pelkästään teknisten ratkaisujen ja toimintojen kehittämistä turvalliseksi, vaan se sisältää myös henkilöstön toimintaan ja käyttäytymiseen liittyviä toimintoja. Tietoturvallisuus vaikuttaa koko organisaation toimintaan, kuten laatuun ja taloudellisuuteen. (VAHTI 2/2004, 15–16.) Tietoturvatoiminnan on tarkoitus varmistaa, että tarvittavat salassa pidettävät tiedot suojataan ja vain niihin oikeutetuilla henkilöillä on mahdollisuus päästä tietoihin ja järjestelmiin käsiksi. Osa tietoturvallisuuden toimintaa on myös varmentaa, että tiedot säilyvät tarvittavaan määräaikaan asti ja ovat saatavilla tarvittaessa. (VAHTI 4/2013, 17.)

Tietoturvallisuus voidaan nähdä sekä päämääränä että prosessina samalla tavalla kuin turvallisuus yleisenä käsitteenä. Tietoturva on ensisijaisesti suojelemista eli tiedon suojaamista erilaisilla toimilla, käytänteillä ja käytöksellä. Tietoturvan tarkoitus on varmistaa, että turvaavat toimet ovat asianmukaisesti implementoitu turvaamaan kohdetta mahdollisilta hyök-

käyksiltä ja tarjoamaan mahdollisimman korkean suojauksen. (Ciampa 2015, 11.) Tietoturvalla tarkoitetaan yhtä tietosuojan toteuttamisen tapaa, joka kattaa sekä hallinnolliset että tekniset toimenpiteet, jotka pyrkivät suojamaan edut, oikeudet ja yksityiselämän. Tavoite on siis taata tarvittaville ohjelmistoille ja toiminnoille keskeytymätön toiminta ja varmistaa, että kohde ei joudu tahattoman tai hallisen tiedon tuhoutumisen tai väärentymisen kohteeksi. (Andreasson ym. 2017, 21.)

Tietoturvallisuuden klassiseen määrittelyyn käytetään osatekijöitä, joista käsite koostuu. Nämä osatekijät ovat luottamuksellisuus, käytettävyys ja eheys (Hakala, Vainio, Vuorinen 2006, 4). Luottamuksellisuudella tarkoitetaan, että tiedot ovat saatavilla vain heille tarkoitetuilla henkilöillä, käytettävyys takaa sen, että tiedot ja mahdolliset tietojärjestelmät ovat käytettävissä ja helposti saatavilla tietojen käyttöön oikeutetuilla henkilöillä ja eheys varmistaa sen, että tietoja pystyy muokkaamaan vain siihen oikeutetut henkilöt. (Tietoturva, 2022.)



Kuvio 2: Tietoturvallisuuden osatekijät

Ruohosen (2002, 2–3) mukaan määritelmä tietoturvasta ja sen tavoitteista on taas jaettu viiteen osatekijään, jotka ovat luottamuksellisuus, autenttisuus, kiistämättömyys, eheys ja käytettävyys (Kuvio 2). Autenttisuus tietoturvan osatekijänä tarkoittaa todentamista eli käyttäjän tunnistamista luotettavasti ja kiistämättömyydellä pyritään osoittamaan kiistatta, kuka tietoa on käsitellyt tai siirtänyt. Tämän määrittelyn mukaan onnistuneen tietoturvan olisi huolehdittava jokaisesta näistä yllä mainituista viidestä osatekijästä ja niiden toteutumisesta.

2.1 Tietoturvallisuuden osa-alueet

Tietoturvallisuus kattaa monia eri osa-alueita, jotka valtiovarainministeriön VAHTI 2/2004 ohjeistuksen mukaan ovat jaettu kahdeksaan eri alueeseen. Nämä ryhmät ovat:

- Fyysinen turvallisuus

- Hallinnollinen tietoturvallisuus
- Henkilöstöturvallisuus
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Tietoliikenneturvallisuus
- Käyttöturvallisuus

Mainittu osa-alueiden jaottelu on karkea, sillä suurimmaksi osaksi kaikki alueet liittyvät toisiinsa ja niillä on yhteisiä vaikutustekijöitä. Jaottelun on tarkoitus helpottaa hahmottamaan organisaatioiden tietoruvallisuuden hallintaa ja suunnittelua. (Hakala ym. 2006, 10–12.)

Fyysisellä turvallisuudella tarkoitetaan fyysisten tilojen kuten rakennusten suojaaminen ulkopuolisilta fyysisiltä uhkatekijöiltä. Näitä voivat olla esimerkiksi ympäristön aiheuttamat uhat kuten vesivahingot, tai henkilöiden aiheuttamat uhat kuten esimerkiksi ilkivalta tai murtautuminen yrityksen toimitilaan. Fyysistä turvallisuutta ylläpidetään yhdessä kiinteistöhuollon ja tietohallinnon ammattilaisten kanssa. (Hakala ym. 2006, 10–12.) Fyysisen ympäristön riskit tulisi arvioida suunnitelmallisesti ja tasaisin väliajoin, jotta tilat voidaan luokitella tietoturvallisuuden kannalta kattavasti ja näin ylläpitää tietoturvallista toimintaympäristöä (Laaksonen, Nevasalo, Tomula 2006, 125).

Hallinnollinen turvallisuus varmistaa yrityksen tietoturvan johtamisen sekä kehitystoiminnan. Hallinnollisessa turvallisuudessa täytyy huomioida tietoturvallisuutta koskeva lainsäädäntö sekä mahdolliset lisenssi- ja palvelusopimukset ja niiden vaikutus yrityksen käytäntöihin koskien tietoturvaa. Hallinnollisen turvallisuuden vastuu on usein osa tietohallinnon työtehtäviä. (Hakala ym. 2006, 10–12.) Hallinnollisen turvallisuuden päämääränä on myös varmistaa jokaisen tietoturvan alueen riittävä kehittäminen ja nykyinen taso organisaatiossa (Ruohonen 2002, 5).

Henkilöstöturvallisuus on olennainen osa tietojen turvaamista ja se koskee kaikkia organisaation työntekijöitä. Tätä osa-aluetta voidaan kutsua ennalta ehkäiseväksi turvallisuuden toiminnaksi. (VAHTI 2/2008, 12.) Henkilöturvallisuus tarkoittaa tiedon käsittelijöiden tai järjestelmien käyttäjien oikeuksia tarkastella tietoja ja kykyä toimia turvallisesti suojattavaa tietoa käsiteltäessä. Henkilöturvallisuutta hallitaan esimerkiksi järjestelmäkoulutusten ja vastuiden sekä oikeuksien määrittelyn kautta. Henkilöturvallisuudesta vastaa henkilöstöhallinto yhteistyössä turvallisuusasiantuntijan tai yksikön kanssa. (Hakala ym. 2006, 10–12.)

Laitteistoturvallisuus koskee fyysisten laitteiden kuten tietokoneiden tai muiden tietojärjestelmään liittyvien laitteiden toimintaan, testaukseen, huoltoon tai varautumiseen liittyviä tehtäviä ja toimenpiteitä. Laitteistoturvallisuus kattaa myös laitteista aiheutuvien vaaratilanteiden ehkäisemisen ja ennakoimisen kuten mahdolliset sähköiskut tai laitteiden fyysiset

loukkaantumisvaarat. Tietohallinto vastaa useimmiten myös laitteistoturvallisuudesta. (Hakala ym. 2006, 10–1.2) Laitteistoturvallisuuden yhteys fyysiseen turvallisuuteen on merkittävä, sillä molemmat osa-alueet käsittelevät osittain laitteiden suojaamista ulkopuolisilta tekijöiltä (Ruohonen 2002, 5).

Ohjelmistoturvallisuus koskee ohjelmistoja ja niihin liittyviä tietoturvallisia tekijöitä. Tämä tarkoittaa esimerkiksi ohjelmistojen soveltuvuuden testausta tulevaan käyttötarkoitukseen, yhteensopivuuden suunnittelua muiden käytössä olevien ohjelmistojen kanssa, sekä ohjelmistojen toiminnan luotettavuutta sekä virheettömyyttä. Ohjelmistoturvallisuus kattaa myös linssien hallinnan sekä ohjelmistoverisoiden ylläpitämisen varmistamisen. (Hakala ym.2006, 10–12.)

Tietoaineistoturvallisuus tarkoittaa tietojen säilyttämiseen, palauttamiseen, tuhoamiseen sekä varmistamiseen liittyvää turvallisuustoimintaa. Tämä koskee niin manuaalisia tietojenkäsittelyä kuin automaattista sähköistä tietojen hallintaa. Tietoaineturvallisuus on usein tietohallinnon ja arkistoinnista vastaavan henkilön tai yksikön yhteisvastuulla. (Hakala ym. 2006, 10–12.) Tietoaineiston turvallisuutta vahvistetaan muun muassa viruksentorjuntaohjelmilla, varmuuskopioilla sekä valvomalla käyttöoikeuksia (Ruohonen 2002, 4).

Tietoliikenneturvallisuuden tehtävä on huolehtia esimerkiksi verkkoyhteyksien tai muiden vastaavien viestintään liittyvien tiedonsiirtokanavien turvallisuudesta. Organisaation tietohallinto vastaa pääosin laitteistoturvallisuudesta. (Hakala ym. 2006, 10–12.) Tietoliikenne turvallisuuden parantamiseen hyödynnetään esimerkiksi palomuureja ja VPN-verkkoja (Ruohonen 2002, 4).

Käyttöturvallisuudella tarkoitetaan organisaation laitteistojen käyttöön, saatavuuteen ja toimintaan liittyviä tekijöitä (VAHTI 2/4, 16). Käyttöturvallisuus sisältää myös käyttöympäristöön sekä tukeen ja ylläpitoon liittyvän turvallisuuden. Käyttöturvallisuutta arvioidessa on tärkeää muistaa myös huomioida ulkoistetut palvelut ja etätyöhön liittyvät riskit. (Tietoturvariskien arviointi 2021.)

2.2 Lainsäädäntö ja säännökset

Suomalainen sekä kansainvälinen lainsäädäntö esittää monenlaisia lakeja, jotka liittyvät jollain tapaa tietoturvaan ja tiedon asianmukaiseen suojaukseen. Organisaation on aina itse huolehdittava siitä, että tietoja käsitellään lain asettamien sääntöjen mukaisesti. (Tietoturvaopas henkilöstölle 2021, 16.) Lait voivat olla joko suoraan määrääviä tai asettaa epäsuoria velvoitteita tietoturvaa koskien. Onkin erittäin olennaista, että organisaatio selvittää itse yksittäiset säännökset ja lait, jotka ohjaavat sen tietotuvallista toimintaa. (Laaksonen, ym. 2006, 18.)

EU:n yleinen tietosuoja-asetus

EU:n asettama yleinen tietosuoja-asetus (2016/679) hyväksyttiin vuonna 2016 ja se ohjaa myös Suomessa tiedon suojaamiseen liittyvää toimintaa. Asetuksen tarkoituksena on yksilön oikeuksien vahvistaminen, globaali tietosuojan huomioiminen sekä tietosuojan toteutumisen tehostetumpi valvominen. Lisäksi tavoitteena on kehittää EU:lle kokonaisvaltainen ja vahva tietosuojakehys. Tietosuoja-asetus on kaikille jäsenmaille pakollinen ja kaikilta osin sitova kansallisen liikkumavaran huomioiden. Suomessa tietosuojan sääntely rakentuu EU:n yleisen tietosuoja-asetuksen sekä tietosuojalain mukaan.

Suomen perustuslaki 11.6.1999/731

Suomen perustuslain kohdassa 10 § määritellään oikeus jokaisen henkilön yksityisyyden suojaan. Lain tarkoitus on taata jokaiselle suojattu yksityiselämä, kotirauha sekä kunnia. Lain mukaan jokaisen kirjeen, puhelun tai muun luottamuksellisen viestin sisältö on koskematon. Lain sisältöä voidaan kuitenkin muokata, mikäli viestin sisältö on olennainen esimerkiksi rikollisen toiminnan selvittämiseksi.

Tietosuojalaki 1050/2018

Tietosuojalain (1050/2018) tarkoituksena on täydentää ja täsmentää henkilöiden suojelusta henkilötietoihin liittyvässä käsittelyssä. Tietosuojalaissa säädetään muun muassa henkilötunnuksen käsittelystä, tietosuojavaltuutetun tehtävistä ja henkilötietojen käsittelystä työsuhteen yhteydessä. Tietosuojalaki kumoaa vuonna 1999 käyttöönotetun henkilötietolain, joka koski henkilöiden tietojen käsittelyä ja rekisteröintiä.

Laki yksityisyyden suojasta työelämässä 759/2004

Lain yksityisyyden suojasta työelämässä (759/2001) tarkoituksena on suojata henkilön yksityisyyden suojaa ja muita perusoikeuksia työelämässä. Laissa säädetään muun muassa kameravalvonnasta, henkilö- ja soveltuvuusarvioinneista sekä henkilötietojen käsittelystä työpaikalla. Oleellista lainsäädännön kannalta on, että työantajalla on oikeus käsitellä vain työsuhteen puolesta välttämättömiä ja tarpeellisia henkilötietoja eikä tästä tarpeellisuusvaatimuksesta voida poiketa edes työntekijän suostumuksella.

Laki sähköisen viestinnän palveluista 917/2014

Laki sähköisen viestinnän palveluista (917/2014) säätää tavoitteet edistävät sähköisen viestinnän palveluiden tarjontaa sekä käyttöä ja lain avulla pyritään myös varmistamaan viestintäverkkojen ja palveluiden kohtuullinen saatavuus jokaiselle koko maassa. Lain tavoitteena on myös turvata viestintäverkkojen ja palveluiden tekninen kehittyneisyys, turvallisuus sekä laa-

dukkuus. Tavoitteena on myös yksityisyydensuojan realisoituminen ja sähköisen viestinnän validiteetti.

2.3 Tietoturvaan liittyvät standardit ja ohjeet

Tietoturvan suunnittelua varten on tuotettu kansainvälisiä ja kansallisia standardeja, jotka ohjaavat tietoturvasuunnittelua ja siinä käytettäviä menetelmiä. Standardien avulla voidaan jäsennetysti vertailla ja tutkia suunnitelmia ja niiden tuloksia. Tietoturvan suunnittelussa on tärkeää muistaa, että standardit antavat raamit suunnittelutyön sisällölle ja dokumentoinnille, mutta ne eivät itsessään takaa riittävää turvallisuutta. (Hakala ym. 2006, 46)

Merkittävimpiä käytössä olevia standardeja ovat laajasti hyödynnettävät kansainväliset ISO-standardit. Tietoturvaa ohjaa ISO/IEC 27000 sarjan standardit, jotka käsittelevät tietoturvan johtamisjärjestelmän perustamista organisaation toiminnan tasolla. Standardisarja antaa tukea tietoturvallisuuden johtamiseen ja siihen liittyvien riskien hallintaan. (Luottamuksen lähteillä 2019, 8–14)

Standardisarjasta löytyvä ISO/IEC 27001 standardi on laajalti tunnettu standardi, ja se sisältää vaatimukset organisaation tietoturvan hallintajärjestelmälle. Standardeissa esitettyjen ohjeiden avulla kaikenlaiset ja kaiken kokoiset organisaatiot voivat hallita omaisuuden turvallisuutta, kuten taloudellisia tietoja, immateriaaliomaisuutta, työntekijöiden tietoja tai muiden sidosryhmien tietoja. Kyseinen standardi pohjautuu alkuperäisesti Brittiläiseen standardiin BS 7799. (Hakala ym. 2006, 46.) ISO standardi antaa alusta loppuun asti prosessinomaiset raamit tietoturvanhallintajärjestelmän luomiseen. Se sisältää järjestelmän luomisen, käyttöönoton, hyödyntämisen, ylläpidon, valvonnan sekä kehittämisen peruselementit.

ISO 27001 standardin viitekehys muotoutuu seuraavan seitsemän pääkohdan ympärille:

- Toimintaympäristön määrittely
- Johtajuus
- Suunnittelu
- Tukitoiminnot
- Toiminta
- Suorituskyvyn arviointi
- Parantaminen

Standardin liitteessä A on myös esitetty obligatorinen hallintatavoitteiden ja -keinojen viiteluettelo. (SFS-EN ISO/IEC 27001:2017) Viiteluettelossa kuvaillut hallintatavoitteet on jaettu seuraavasti:

- A.5 Tietoturvapolitiikat

- A.6 Tietoturvallisuuden organisointi
- A.7 Henkilöstöturvallisuus
- A.8 Suojattavan omaisuuden hallinta
- A.9 Pääsynhallinta
- A.10 Salaus
- A. 11 Fyysinen turvallisuus
- A. 12 Käyttöturvallisuus
- A.13 Viestintäturvallisuus
- A.14 Järjestelmien hankkiminen
- A.15 Suhteet toimittajiin
- A. 16 Tietoturvahäiriöiden hallinta
- A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia
- A.18 Vaatimustenmukaisuus

ISO/IEC 27002 syventää 27001-standardia tarjoamalla syventäviä ja tarkentavia ohjeita tietoturvanhallintaan liittyen. Muut 27001 standardiperheen standardit antavat tukea 27001 standardin käyttöönotolle esittämällä ohjeita ja vertailuperusteita muun muassa tietoturvan hallinnan mittaamiseen ja auditointiin. (Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet 2017, 4)

Muita tietoturvanhallintaan liittyviä ohjeistuksia ovat esimerkiksi viranomaisille suunnittelu auditiointityökalu Katakri tai valtionvarainministeriössä kehitetyt VAHTI-ohjeet. (Luottamuksen lähteillä 2019, 5). Katakri on laadittu huomioiden Suomen lainsäädännön, ja suomea velvoittavat kansainväliset tietoturvallisuus toimet. Katakrin rakenne koostuu kolmesta eri osa-alueesta, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Jokaisessa osa-alueessa määritellään asetetut turvallisuusvaatimukset ja annetaan esimerkkejä vaatimusten toteuttamiseksi. Tätä työkalua voidaan hyödyntää organisaatioiden, viranmaisten tai yhteisöjen turvallisuustyön kehitykseen sekä arviointiin. (Katakri 2020, 5–6)

3 Tietoturvasuunnittelu

Tietoturvasuunnittelun olennaisimpana lähtökohtana on ymmärtää kokonaisturvallisuuden merkitys ja yhtenäisyys suunnitelman taustalla. Suunnitelmaa tehdessä tulisi olla ymmärrys koko organisaation turvallisuudesta ja siihen vaikuttavista toimista. (Hakala ym. 2006, 14.) Suunnitelman rakentamisen tavoitteena on, että kaikki tietojärjestelmien osat ovat suojattu tehokkaasti ja niihin kohdistuvat riskit ovat minimoitu (Ruohonen 2002, 6).

Hakalan ym. (2006, 14–15) mukaan kokonaisturvallisuus koostuu sekä fyysisestä turvallisuudesta että tietoturvallisuudesta. Fyysisen turvallisuuden suojaaminen tarkoittaa suojautumista esimerkiksi varkauksilta tai tulipaloilta ja tietoturvallisuuden tarkoitus on taas keskittyä nimenomaisesti tietopääoman ja tietoverkkojen turvaamiseen.

Ciampa (2017 13–14) taas tarkastelee toteutuneen tietoturvallisuuden prosessia kolmen kokonaisuuden kautta, jotka ovat tavarat, ihmiset sekä politiikka ja menettelytavat. Näiden kolmen kokonaisuuden avulla mahdollistetaan hahmottamaan, miten tietoa turvataan ja suojellaan.

3.1 Tietoturvan hallintajärjestelmä

Tietoturvan hallintajärjestelmä eli ISMS (Information Security Management System) voidaan nähdä jatkuvana prosessina, jota kehitetään kohdeorganisaation kehityksen myötä, jotta se vastaisi toiminnan ja ympäristön mukana tulleisiin muutostarpeisiin. (Hakala ym. 2006, 106.) Tietoturvan hallintajärjestelmän käyttöönotto vaatii strategista ajattelua sekä johdon vahvaa sitoutumista. Hallintajärjestelmän rakentamiseen ja suunnitteluun vaikuttavia asioita ovat muun muassa organisaation omat tavoitteet, toimialan vaatimukset, organisaatiorakenne sekä prosessit. Hallintajärjestelmä tulee liittää osaksi organisaation muita prosesseja sekä johtamisjärjestelmää. (Haarni 2019, 5–6.) Hallintajärjestelmän kehittäminen lähtee usein havaituista riskeistä, tietoturvaongelmista, sidosryhmien laatuvaatimuksista tai mahdollisista viranomaisten määräyksistä (VAHTI 6/2006, 21).

VAHTI 3/2007(40) ohjeen mukaan tietoturvan hallintajärjestelmän viitekehys koostuu seuraavista dokumenteista:

- tietoturvapolitiikka ja -strategia
- tietoturvakäytännöt ja -periaatteet, joka kuvaa käytössä olevat turvakäytännöt
- tietoturvallisuuden kehittämissuunnitelma
- tietoturvallisuuden perus- ja lisäohjeistus
- tietoturva-arkkitehtuurit (topologia ja ratkaisujen periaatekuvaukset)
- tietoturvaraportointi johdolle
- pelastus-, jatkuvuus- ja valmiussuunnitelmat
- toimintaan liittyvät tietoturvaprosessit
- auditointisuunnitelma

Prosessinomainen tietoturvallisuuden hallinnan kehitys perustuu PCDA-mallin mukaiseen toimintaan. (Hakala ym. 2005, 49) (Kuvio 3)

Kuvio 3: Tietoturvallisuuden hallintaprosessi PCDA-mallin mukaisesti, mukaillen Hakala (2006).

Suunnittelun vaiheen ideana on määrittää organisaation suojattavat kohteet. Tämän jälkeen siirrytään toteutukseen, eli otetaan hallintajärjestelmä organisaatiossa konkreettisesti käyttöön. Tätä seuraa järjestelmän toiminnan valvonta ja mahdollisten muutosten toteuttaminen ja käyttöönotto uudelleen. Näin prosessi pyörii jatkuvasti ja sen muuttaminen ja parantaminen on mahdollista ja ajantasaista. (Hakala ym. 2005, 49)

3.2 Toimintaympäristön ja suojattavien kohteiden määrittely

Toimintaympäristö määritellään, jotta voidaan tarkentaa riskienarvioinnin kohde sekä tunnistetaan riskienarvioinnille tärkeät riippuvuussuhteet. Toimintaympäristön määrittelyssä on tärkeää ottaa huomioon sisäisen ja ulkoisen toimintaympäristön rajaus, toimintaympäristö kokonaisuudessaan sekä riskien kriteerit eli riskien riskienhallinta ja sietokyky. Toimintaympäristön määrittelyn tuloksen avulla voidaan määrittää mitä riskejä sisällytetään riskienhallintaan, suhteuttaa riskien analysoinnissa riskien todennäköisyydet ja vaikutukset paremmin sekä tehdä valintoja ja toimenpiteitä riskien käsittely varten. (VM 22 2017/19–20.)

Organisaation tulee määritellä omalle toiminnalle oleelliset asiat, jotka huomioidaan määriteltäessä suojattavia kohteita. Kohteet luokitellaan ja määritellään arvon sekä tärkeyden perusteella. Suojattavia kohteita voi olla esimerkiksi fyysiset laitteet, ohjelmistot, tiedostot, tai tietokannat. Listaus toimii perustana omaisuuden suojaukselle ja tukena riskienhallinnalle. (Johansson 2003, 5.)

3.3 Riskienhallinta

Riskienhallintaprosessin ideana on tunnistaa riskejä ja uhkia, jotka voivat uhata yrityksen tavoitteita ja toimintaa. Prosessin arvioinnin avulla määritellään kullekin riskille soveltuva hallintakeino. ISO 31000 mukaisessa riskienhallintaprosessissa on selkeästi viisi erilaista päävaihetta. Itse riskien arviointiin kuuluu kolme vaiheitta, jotka ovat riskien tunnistaminen, riskianalyysi ja riskien merkityksen arviointi. Ennen riskienhallinnan pääprosessin alkua tulee kuitenkin määritellä toimintaympäristö, jonka avulla rajataan mitä riskien arviointiin sisällytetään ja mitä tekijöitä jätetään ulkopuolelle. Pääprosessin jälkeen, eli riskien merkityksen arvioinnin ollessa valmis, tulee myös käsitellä riskit, eli keskittyä siihen millaisia toimenpiteitä kullekin riskille tulisi tehdä. Riskienhallintaan liittyy myös oleellisesti riskien seuranta ja viestintä. Kokonaisuudessaan riskienhallintaprosessissa on oleellista seurata miten tehdyt toimenpiteet vaikuttavat, päästäänkö tavoitteisiin ja tehdään tarvittavaa viestintää liittyen riskeihin ja niiden hallintakeinoihin. (VM 22/2017, 7–13.)

Tietoturvariskit tunnistetaan ja analysoidaan riskianalyysin avulla, jotta voidaan varmistaa, että jokainen osa on huomioitu ja riskeihin valmistauduttu tarpeeksi tehokkaasti. Riskianalyysin pohjana käytetään tietoturvasuunnitelmaa, jossa tietoturvatoiminnalle on asetettu objektiin sopivat tavoitteet. Riskianalyysissä tulisi huomioida sisäiset uhat, ulkoiset uhat, tahattoman vahingot sekä mahdolliset ennakoimattomat tilanteet. (Ruohonen 2002, 6–7.)

3.4 Tietoturvapolitiikka ja tietoturvasuunnitelma

Riskianalyysin ja organisaation strategian avulla voidaan lähteä rakentamaan tietoturvapolitiikkaa. (VAHTI 3/2007, 25). Organisaation tietoturvapolitiikka antaa raamit tietoturvan kehittämiselle ja toteutukselle sekä muodostaa perustan tietoturvakoulutuksille ja henkilöstön ohjeistuksille. Tietoturvapolitiikka tarkoittaa tietoturvaan liittyen linjausten vetoa ja sen avulla myös johto osoittaa sitoutuneensa organisaation tietoturvan kehitykseen. (Laaksonen ym. 2006, 146.)

Tietoturvapolitiikasta tulee laatia kirjallinen dokumentti, josta käy ilmi politiikkaan sisällytetyt toimet ja linjaukset. Dokumentin tulee olla julkinen niin että kaikki organisaation työntekijät ovat oikeutettuja sen lukemiseen ja ymmärtämiseen. Lisäksi se voidaan osoittaa myös muille sidosryhmille luettavaksi osoituksesi esimerkiksi luotettavuudesta suhteessa tietoturvaan. (Hakala ym. 2006, 7–9.) Johdon tulee hyväksyä ja varmistaa tietoturvapolitiikka sekä siinä määritellyt vastuut ja toimenpiteet. Johdon tehtävä on myös huolehtia, että dokumenttia tarkistetaan ja tarvittaessa päivitetään säännöllisin väliajoin, vähintään kuitenkin 3 vuoden välein. (VAHTI 3/2007, 25.)

Tietoturvapolitiikka kertoo tietoturvaan liittyvät roolit ja vastuut eli se määrittää vastuualueet organisaation sisällä. Tietoruvapolitiikassa esitellään myös tavoitteet ja tietoturvan vaiku-

tus yrityksen toimintaan, sekä määritellään pääpiirteiset linjaukset jatkuvuudenhallinnasta ja toipumissuunnitelmasta. On tärkeää sisällyttää politiikkaan myös tietoturvakoulutukset ja niihin liittyvät odotukset ja vaatimukset, jotta henkilöstö tiedostaa organisaation tavoitteet ja pystyy sitoutumaan niiden saavuttamiseen. (Laaksonen ym. 2006, 147.)

Tietoturvasuunnitelmalla tarkoitetaan konkreettisempaa suunnitelmaa siitä, miten haluttuisiin tietoturvatavoitteisiin päästään. Suunnitelma sisältää kirjalliset, yksityiskohtaiset ja tekniset ratkaisut esimerkiksi ohjelmistojen tai laitteiden käyttöön liittyen. (Hakala ym. 2006 9–10.) Dokumentissa kuvataan muun muassa tietoturvatehtävät ja vastuut ja niiden toteutustapa, kuvaus mahdollisten tietojen suojaamisesta ja salassapitokäytänteistä, sekä määritellään organisaation raportointi käytänteet liittyen tietoturvatoimintaan. (VAHTI 3/2007, 47). Suunnitelma voi olla joko salainen tai luottamuksellinen, riippuen sen tarkasta sisällöstä. (Hakala ym. 2006 9–10).

4 Suurimmat tietoturvariskit

Nykypäivän organisaatioiden kohtaamat tietoturva uhat ovat erittäin moninaisia. Ulkopuolisten toteuttamista hyökkäyksistä organisaatioita vastaan on tullut hyvin yksinkertaista monien tekijöiden vuoksi, joita ovat esimerkiksi loppukäyttäjien toiminta, haittaohjelmien lisääntyminen, haavoittuvien ohjelmistojen ja käyttöjärjestelmien esiintyvyys sekä teknologisten henkilökohtaisten laitteiden lisääntyminen (Renfrow & Death 2017, 8.)

IBM:n tekemän tutkimuksen mukaan (2021, 2–3) kuluttajien välinpitämätön lähestymistapa turvallisuuteen liittyen yhdistettynä yritysten nopeaan digitaaliseen muutokseen, tarjoaa kyberhyökkääjille lisää mahdollisuuksia kiristysohjelmista tietovarkauksiin. Huonot henkilökohtaiset turvallisuustottumukset voivat siirtyä myös työpaikalle ja johtaa kalliisiin tietoturvatapahtumiin yrityksille. Tutkimuksen mukaan yksi tietoturvahyökkäysten päälähteistä vuonna 2020 koski vaarantuneita käyttäjätietoja.

Järvisen ja Rouskun (2017, 33–44) mukaan suurin ulkopuolinen uhka organisaation tieturvaan liittyen on tietoverkkorikollisuus. Tämän kaltaisilla rikollisilla voi olla erilaisia motiiveja taustalla ja osa heistä on ammattilaisia, osa harrastelijoita ja osa esimerkiksi kyberterroristeja. Kaikki nämä ryhmät kuitenkin tähtäävät samaan tavoitteeseen, eli pyrkivät jollain tapaa pääsemään käsiksi salassa pidettävään tietoon ja tämän jälkeen tarkoituksena on tuhota tieto, varastaa tieto tai levittää tietoa sopimattomille tahoille. Verkkorikollisten ensisijaisena tavoitteena voi olla myös rahan huijaaminen tai kiristäminen.

Traficom on listannut vuoden 2021 suurimmiksi tieturvauhkiksi organisaatoille seuraavat kolme tekijää:

- Tietojenkalastelu
- Haittaohjelmat
- Etätyön puutteellinen tietoturva (Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle, 2021.)

Myös Traficomin kyberturvallisuusoppaassa pienyrityksille (2020, 4–9) on korostettu pienyritysten suurimpina tietoturvauhkina tietojenkalastelua, haittaohjelmia sekä kiristyshaittaohjelmia. Pienemmissä organisaatioissa kyber- tai tietoturvauhka voi olla todella vaikuttava toteutuessaan ja sen merkitys voi jopa koitua yrityksen kohtaloksi. Haasteita hyökkäyksiltä suojautumiseen tuo kehittyneet hyökkäystavat, heikot ja viivästyneet tietoturvapäivitykset, helpot ja yksikertaiset hyökkäystyökalut sekä haavoittuvuuksien nopeampi havaitseminen (Ciampa 2017, 7).

4.1 Tietojenkalastelu

Tietojenkalastelu eli englanniksi Phishing perustuu salasanojen ja käyttäjätunnusten vakoilemiseen. Kalastelu tapahtuu usein tunnetuilla verkkosivuilla, kuten kansainvälisissä nettikaupoissa, jotka käyttäjän näkökulmasta voivat vaikuttaa turvallisilta. Tietojenkalastelu toteutetaan esimerkiksi väärennetyllä sähköpostilla, joka pyytää vastaanottajaa painamaan linkistä jonkin hyvän syyn tarkoituksena ja linkki ohjaa käyttäjän tunnetulle, mutta väärennetylle nettisivulle. Käyttäjän kirjoitettua omat tunnuksensa väärennetylle sivulle nettihuijari pääsee käyttämään tunnuksia ja aiheuttamaan tällä tavalla vahinkoa ja esimerkiksi tilaamaan tuotteita huijatun henkilön laskuun. (Järvinen ym. 2017, 85.)

Tietojenkalastelujen motiivit ovat yleensä melko tyypillisesti raha tai tieto. Usein kohteena ovat tavalliset ihmiset ja heitä lähestytään sähköpostilla jonkin mielenkiintoisen aiheen tiimoilta. Muita todennäköisiä kohteita ovat minkä tahansa yrityksen niin sanotut tavalliset työntekijät. Vaikka heillä ei itsellään ehkä ole paljoakaan huijarille relevanttia tietoa, kirjautumistietojen luovuttaminen voi saada hyökkääjälle mahdollisen pääsyn koko yrityksen verkkoon. (Hadnagy & Fincher 2015, 36.) Vahinkoja voidaan minimoida nopealla reagoinnilla, eli salasanan vaihtamisella heti kun huomaa joutuneensa tietojenkalastelun uhriksi. Näin salasanan varastanut henkilö ei pääse hyödyntämään anastettua salasanaa. Tietojenkalastelun ehkäisyksi on myös tärkeää opetella havaitsemaan mahdolliset kalasteluviestit joissa. (Järvinen & Rousku 2017, 85–87.)

4.2 Haittaohjelmat ja haavoittuvuudet

Haittaohjelmilla tarkoitetaan koneeseen päässeitä ohjelmia, jotka vaikuttavat negatiivisesti koneeseen tai järjestelmään. Haittaohjelmat löytävät tiensä koneeseen usein sähköpostin tiedostojen tai verkkosivujen kautta. Näitä voi torjua erilaisilla tiedostetuilla menetelmillä,

joita ovat esimerkiksi koneen suojaus, säännöllinen päivittäminen sekä puhtaana pito. (Järvinen ym. 2017, 90–91)

Suomen yleisimpiä haittaohjelmia vuonna 2021 lokakuussa ovat olleet muun muassa Mailto, Formbook ja Lokibook. Mailto on kiristyshaittaohjelma, joka leviää enimmäkseen sähköpostien kautta. Formbook taas toimii Windows-ohjelmiston kautta ja se kerää kohteiden salattavia tietoja monin eri tavoin. Myös Lokibook kerää tunnistetietoja mutta se toimii sekä Androidissa että Windowsissa. Tietojen keräys tässä haittaohjelmassa tapahtuu esimerkiksi sovelluksista sekä selaimista. (Kailio 2021.)

Haavoittuvuus mahdollistaa esimerkiksi juuri haittaohjelmien helpomman ja nopeamman leviämisen ja mahdollistaa konkreettisen vahingon realisoitumisen. Haavoittuvuudet kuvaavat siis kaikenlaisia heikkouksia, jotka helpottavat vahingon aiheutumista. Haavoittuvuuksia voidaan löytää muun muassa laitteista, ohjelmistoista tai tietojärjestelmistä ja sen voi aiheuttaa esimerkiksi laitteen päivittämättömyys, vanha käyttöön sopimaton teknologia tai ohjelmiston käyttötarkoituksen suunnittelemattomuus. (Haavoittuvuudet - miten niistä ilmoitetaan oikein 2020.) Jatkuva tietokoneen tai ohjelmiston päivitysten lykkääminen lisää laitteen haavoittuvuutta ja altistaa laitteen mahdollisille haittaohjelmille herkemmin. Vaikka laitteeseen asennettu automaattinen päivitys helpottaa päivitysten ajantasaisuutta tulisi laitteen käyttäjän muistaa tarkistaa päivitykset myös itse sillä aina automaattiset päivitykset eivät onnistu esimerkiksi vähäisen virran tai muistin vuoksi. (Digiturvan käytännön vinkit 2021, 3.)

4.3 Etätyön puutteellinen tietoturva

Etätyön puutteellinen tietoturva johtuu usein nopeista ratkaisuista ja ohjeiden vähäisyydestä etätyössä. Organisaatioilla toimistolla käytössä olevat tietoturvakontrollit eivät automaattisesti anna samanlaista turvaa etätyössä kuin toimistolla työskennellessä. (Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle, 2021.) Merkittäviä etätyön tietoturvaan liittyviä tekijöitä ovat suojatun verkon käyttäminen, työnantajan tarjoamien laitteiden käyttäminen työn tekoon sekä hyvän salauksen varmistaminen. Tietojen turvaamiseen vaikuttaa toki myös salassapitovelvollisuuden sekä annettujen ohjeiden noudattaminen. (Tee etätyöstä turvallista vinkkiemme avulla, 2020.)

Yleispätevä sääntö on, että työntekoon ei tulisi käyttää julkisia verkkoyhteyksiä niiden mahdollisen puutteellisen tietoturvan vuoksi. (Vinkkejä turvalliseen etätyöhön, 2020). Kotona käytettävien langattomien verkkoyhteyksien oletusalasanat tulisi vaihtaa aina verkon käyttöönoton yhteydessä. Etätyöskentelyssä voidaan käyttää myös esimerkiksi työpuhelimen WiFi-hotspot ominaisuutta, kunhan verkon salaukset ovat kunnossa. (Digiturvan käytännön vinkit 2021, 10.)

Omien henkilökohtaisten laitteiden, kuten puhelimen tai tietokoneen käyttöä työasioiden hoitamiseen tulisi välttää. Omien laitteiden suojaukset ja päivitykset eivät usein vastaa organisaation asettamia vaatimuksia, ja nämä puutteet luovat herkemmin haavoittuvuuksia ja luovat riskejä tietojen suojaukseen. (Tee etätyöstä turvallista vinkkiemme avulla, 2020.) Myöskään omaa henkilökohtaista sähköpostia tai muita henkilökohtaisia tilejä ei ole turvallista käyttää työhön liittyvien materiaalien toimittamiseen. (Vinkkejä tietoturvalliseen etätyöhön, 2020).

Työn tekoon käytettävien laitteiden ja tilien suojaus on yksi tärkeimmistä tietoturvan elementeistä. Salasanan turvaaminen työskentely-ympäristöstä huolimatta on erityisen tärkeää ja siihen on hyvä kiinnittää huomiota. (Järvinen & Rousku 2017, 57–58.) Hyviä salauksen elementtejä on uniikki salasana jokaiseen tiliin, jossa on vähintään 8 merkkiä. Salasanan olisi hyvä myös sisältää numeroita sekä erikoismerkkejä. Salauksen vahvistamiseksi kannattaa käyttää monivaiheista tunnistautumista, joka vaatii salasanan lisäksi myös esimerkiksi tunnistautumaan puhelimella tai tunnuslistalla. (Pidempi parempi - Näin teet hyvän salasanan, 2021)

5 Tietoturvatietoisuus

Vaikuttava ja tehokas tietoturvatietoisuus eli ISTA (Information Security Awareness) on välttämätöntä organisaation toiminnan suojelemiseksi. Organisaatiot käyttävät huomattavan määrän rahaa ja resursseja tietoturvan ylläpitoon. Tästä huolimatta suurin osa tieto- tai kyberturvaan liittyvistä vaaroista johtuvat työntekijöiden toiminnasta, eli työpaikan tietoturvapolitiikan laiminlyönnistä. (Alshaikh, Maynard, Ahmad & Chang 2018, 5085.)

Tietoturvatietoisuus tarkoittaa ymmärrystä käytännöistä ja toimintatavoista kuten muun muassa tietokoneen käyttökäytännöt, Internetin käyttökäytännöt, etätyökäytännöt ja muut käytännöt, joilla pyritään hallitsemaan ja suojaamaan organisaation salattavia tietoja. (Gardner, & Thomas 2014,1.) Tietoturvatietoisuuden määritelmällä on kaksi olennaista osatekijää. Ensimmäinen näistä elementeistä liittyy yksilön ymmärryksen tasoon organisaation tietoturvapolitiikasta. On huomioitava, että tässä yhteydessä on erityisen tärkeää, että työntekijät aidosti ymmärtävät tietoturvakäytännöt ja protokollat, jotta he voivat toimia tehokkaasti ja ohjeiden mukaan tietoturvan kontekstissa. Toinen osatekijä tietoturvallisuuden määrittelyssä on se, että missä määrin yksilö sitoutuu tietoturvan ydinperiaatteisiin organisaatiossaan ja omassa toiminnassaan. (Hadlington, Popovac, Janicke, Yevseyeva & Jones 2019, 41–48.)

Tietoturvatietoisuus on olennainen osa tehokasta tietoturvan hallintaa. Se vaatii keskittymistä ja panostusta organisaation useisiin rinnakkaisiin toimintoihin. Näitä ovat yrityspolitiikan ja standardien vahvistaminen, toimivan teknisen infrastruktuurin tarjoaminen, henkilöstön päte-

vyyden varmistaminen, sekä tehokkaan järjestelmien ja prosessien kehittämiseen toimivan ympäristön mahdollistaminen. (McIlwraith 2006, 21.) Tutkimukset osoittavat, että suurin tietoturvallisuuden uhka on käyttäjät itse, mikä tarkoittaa, että heikoin lenkki piilee organisaation työntekijöissä. Tärkeäksi tietoruvallisuuden kehityskohteeksi tulee siis ihmisen käyttäytyminen ja siihen liittyvät todelliset riskit. (Hadlington ym. 2019, 41–48.)

Tietoisuutta lisäävät koulutukset ohjaavat organisaation turvallisuuskulttuuria ja auttavat työntekijöitä tiedostamaan, että tietoturvan ymmärtäminen on yksi suurin edellytys turvallisuuden perustamiselle. Tietoturvatietoisuuden toteutuessa kokonaisvaltaisesti sen tulisi sisältää seuraavat kolme oleellista tasoa;

- **Havaitseminen:** työntekijä osaa havaita poikkeamia ympäristöstä
- **Ymmärtäminen**: Käyttäjä voi yhdistää eri lähteistä peräisin olevaa tietoa, ymmärtää lähteitä ja niistä saapunutta tietoa vähentääkseen mahdollisia ympärillä tapahtuvia riskejä
- **Ennustaminen**: Työntekijä pystyy ennustamaan mahdollisia tulevia hyökkäyksiä ja muuttaa omaa käyttäytymistään ja toimintaansa vähentääkseen tai poistaakseen riskin kokonaisuudessaan. (Vasileiou, & Furnell 2019, 45)

Jokaisen organisaatiossa työskentelevän tulisi saada tarpeellinen koulutus ja opastus tietoturvatietoisuuden kehittämiseksi, mikäli se on henkilön työnkuvan kannalta merkittävää ja välttämätöntä. Työntekijöiden osaamista tulee myös päivittää muutosten myötä. (ISO/IEC 27001:2017, 16.) Tietoturvatietoisuuden kehittämiseksi ja ylläpitämiseksi taritaan usein muutakin kuin pelkkiä koulutuksia. Muita mahdollisuuksia tietoisuuden lisäämiseksi ovat esimerkiksi henkilöstön itseopiskelu valmiin materiaalin avulla, teema viikko tai päivä tietoturvasta, viestintä sisäisissä palavereissa, tietoturvatesti sekä tietoturvamateriaalin lisääminen uuden työntekijän perehdytykseen. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 31.) Organisaation tulee tarjota työntekijöilleen koulutusta ja tietoisuuden vahvistamista varmistaakseen, että kaikki organisaation toimet ovat tietosuojakäytäntöjen sekä paikallisten lakien ja määräysten mukaisia. Työntekijöille tulee tulla selkeästi ilmi yrityksen velvoittamat tietosuojaodotukset sekä mahdollisten asiakkaiden tietosuojaperiaatteet. Henkilöstön tulee myös pystyä sisällyttää periaatteet päivittäisiin työtehtäviinsä ja heillä tulee olla ymmärrys turvallisuus- ja tietosuojakäytäntöjen laiminlyömisen sanktioista. (Herold 2010, 9–10.)

5.1 Tietoturvatietoisuuden kehittäminen

Tietoturvatietoisuutta voidaan kehittää turvallisuustietoisuusohjelman kautta. Turvallisuustietoisuusohjelma on organisaatioissa käytössä oleva muodollinen ohjelma, jonka tavoitteena on kouluttaa henkilöstöä organisaation tietoihin kohdistuvista mahdollisista uhista ja miten välttää tilanteet, jotka saattavat vaarantaa organisaation tiedot. Turvallisuustietoisuusohjelman

tavoitteena on minimoida riskejä, valtuuttaa käyttäjät ottamaan henkilökohtaista vastuuta organisaation tietojen suojaamisesta sekä valvomaan ja tarkastamaan organisaation käytäntöjä sekä toimintatapoja tietojen suojaamiseksi. (Gardner & Thomas 2014, 1.) Tietoturvatietoisuuden koulutusohjelman luominen ei ole yksinkertaista, mutta sen avulla voidaan varmistaa, että henkilöstö ymmärtää ja noudattaa vaatimuksia, jotka ovat liiketoiminnan kannalta elintärkeitä. Ymmärryksen tai taidon puute tietoturvaan liittyvissä asioissa voi pahimmassa tapauksessa johtaa yrityksen maineen menetykseen, liiketoiminnan kaatumiseen tai vaikuttaa negatiivisesti johonkin toiseen yrityksen sidosryhmään. (Herold 2010, 7–8.)

Heroldin (2010, 72–73) mukaan tehokkaan tietoturvatietoisuuden koulutusohjelman tulisi pitää seuraavat sisällään neljä kriittistä vaihetta.

1. **Ohjelman suunnittelu:** Organisaation tarpeiden arviointi, koulutuksen strategian suunnittelu ja hyväksyttäminen, kehityskohteiden ja tarvittavien toimien määrittely
2. **Materiaalien kehitys**: kohderyhmien tunnistaminen ja laajuuden asettaminen, sisällön ja koulutusmateriaalin kehittäminen
3. **Ohjelman implementointi**: ohjelmasta tiedottaminen ja sen toteuttaminen, materiaalin toimittaminen osallistujille (esimerkiksi videot tai nettisivut)
4. **Toteutuksen jälkeiset toimenpiteet:** Ohjelman ylläpito, tehokkuuden ja vaikutusten mittaus ja tarkkailu, palautteen kerääminen esimerkiksi kyselyllä tai ryhmäkeskusteluissa

Tietoturvatietoisuusohjelman toteuttaminen ei automaattisesti takaa sitä, että kaikki työntekijät ymmärtävät roolinsa tietoturvan toteuttamisessa. Jotta turvallisuustietoisuusohjelma voisi tuoda lisäarvoa organisaatiolle ja samalla edistää tietoturvan yleistä ymmärtämistä, on sen vaikutusta tutkittava systemaattisesti. (Kruger & Kearney 2006, 289-296.)

5.2 Tietoturvatietoisuuden mittaaminen

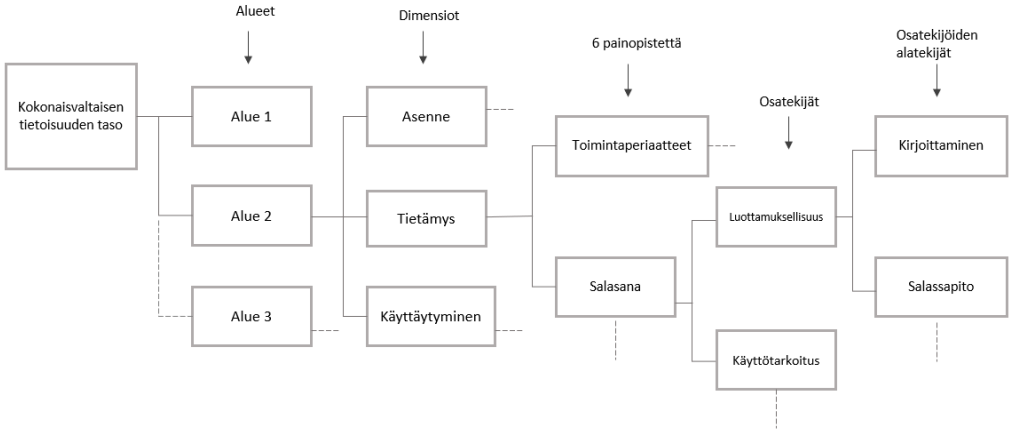
Tietoturvallisuuden mittaamisen lähtökohtana on saada informaatiota mitattavasta kohteesta, joka auttaa kehittämään tietoturvallisuuteen liittyvien toimien suunnittelua, johtamista sekä priorisointia. Laadukkaalla ja säännöllisellä mittaamisella tähdätään muun muassa tietoturvaan liittyvät kehityskohteiden selvittämiseen, kouluttamaan työntekijöitä oikeilla osa-alueilla, keräämään vertailuaineistoa sekä vakuuttamaan sidosryhmät. Mitattaessa tietoturvallisuutta täytyy ensin määrittää mitattava kohde ja sen vaikutus organisaation toimintaan sekä tuloksellisuuteen. (Laaksonen ym. 2006, 268–269.) Tietoturvallisuuden mittaaminen antaa organisaatiolle työkalun turvallisuuden kehittämiseen, johtamiseen ja parantamiseen. Ennen ulkoisen arvioinnin teettämistä on suositeltavaa, että organisaatio tekee itse sisäisesti

kohteeseen estimoinnin suurimmista kehityskohteista, joita voidaan korjata jo ennen mahdollista ulkoista arviointia. (VAHTI 2/2014, 14–15.)

ENISAN (2007, 1–2) tutkimuksen mukaan tietoturvatietoisuutta voidaan mitata monella eri tavalla ja organisaatiot käyttävät mittauksissa kirjavasti erilaisia lähestymistapoja. Tutkimuksessa esiin tulleita mittaamisen keinoja olivat auditointi (sisäinen tai ulkoinen), ihmisten aiheuttavien tietoturvallisuustapaturmien määrä sekä tietoturvallisuuteen liittyvä kysely henkilöstölle. Jokaisen organisaation on löydettävä itselleen sopiva vaihtoehto mittaamiseen, sillä kaikki lähestymistavat eivät sovi kaikille organisaatioille. Lähestymistavan pitäminen yksinkertaisena pitää sen yleensä myös kustannustehokkaana. Laaksonen ym. (2006, 278–279) painottaa, että työntekijöiden toimintaa tai käyttäytymistä mitatessa on hyvä muistaa positiivinen lähestymistapa, jotta mittaaminen ei tunnu syyllistävältä tai vaikuta kohderyhmän mielentilaan. Relevantteja henkilöstön toimintaan liittyviä mittauksen kohteita ovat muun muassa salasanakäytännöt, tietämyksen taso sekä tiedon käsittely ja luokittelu.

Yksi tietoturvatietoisuuden mittausmalleista on Krugerin ja Kearneyn (2006, 291–292) prototyyppinen KAB-malli (Knowledge, Attitude, Behaviour), joka pohjautuu sosiaalipsykologian alalta tulleisiin tekniikoihin. Tietoturvatietoisuuden arvioinnissa käytetään 3 ulottuvuutta, jotka ovat tieto, asenne ja käyttäytyminen. Tiedon mittaamisella tarkoitetaan käyttäjien tietämyksen mittausta liittyen tietoturvaan. Tietoturvaan liittyvä näkemys on ensimmäinen askel tietoturvatietoisuuden luomisessa. Asennetta mitatessa taas tarkastellaan, että miten käyttäjät tuntevat tai ajattelevat tunnetusta tietoturvariskistä. Käyttäytymisen mittauksella tarkoitetaan käyttäjien tietoturvaan liittyviä toimia tai toimintaa.

KAB-mallissa lähdetään liikkeelle painopistealuista ja niiden jälleen jakamisesta edelleen erityistekijöihin. Malli esitetään puurakenteen muodossa, joka on esitetty alla olevassa kuviossa 3. Puuhun valitaan mitattavat tekijät ja määritellään vaikuttavien tekijöiden tärkeys. Olennaista on huomioida, että alueilla ja painopisteillä voi olla erilaiset tärkeystasot ja niiden vaikutus tietoturvatietoisuuteen vaihtelee. Esimerkiksi johto voi määrittää mitattavien painopisteiden tai osatekijöiden tärkeyden. (Krugerin & Kearneyn 2006, 291–293.)



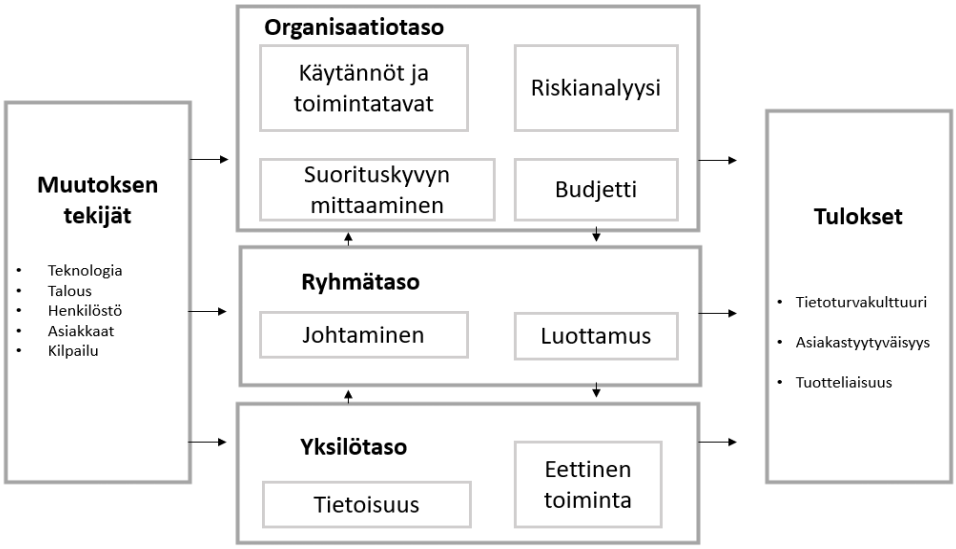
Kuvio 4: Ongelman puurakenne, mukaillen Kruger ja Keaney (2006)

Krugerin ja Kearney (2006, 292–293) tutkimusmenetelmä pohjautuu kyselylomakkeeseen, jossa 35 kysymystä oli suunniteltu testaamaan vastaajien tietämystä, asenteita ja käyttäytymistä. Osaan kysymyksistä vastataan kolmen vaihtoehdon asteikoilla- oikein, väärin, en osaa sanoa. Tutkimuksen tulokset mittaavat tietämyksen tason käyttäen apuna painotettua keskiarvoa. Tulokset kuvataan asteikolla 0–100 %. Kolmiportainen tulosasteikko on kuvattu alla olevassa taulukossa. (Taulukko 1).

Tietoisuus	**Mittaustulos**
Hyvä	80–100 %
Tyydyttävä	60–79 %
Huono	-59 %

Taulukko 1: Tietoisuuden tulokset, mukaillen Kruger & Kearney 2006

Toinen käytetty menetelmä mitata organisaation turvallisuustietoisuutta on Martinsin ja Eloffin (2002) tutkimuksessa käytetty strukturoitu menetelmä, joka pohjautuu turvallisuuskulttuurin tutkimiseen. Tässä menetelmässä organisaatio jaetaan kolmeen tasoon, jotka ovat; organisaatio, ryhmä ja yksilö. Kyselylomakkeella toteuttava arviointitapa kehitettiin tietoturvakulttuuriin arvioimiseksi sekä tietoturvan ymmärryksen kartoittamiseksi yksilö- ryhmä- ja organisaatiotasolla. Alla olevassa kuvassa on esitetty yhdeksän tekijää, jotka käsitellään kaikilla kolmella mitattavalla tasolla.



Kuvio 5: Kuvaus turvallisuuskulttuurin tutkimisesta, mukaillen Martins & Eloff 2002

Menetelmän kyselylomake rakennetaan kehittämällä neljäkymmentäviisi väitettä, jotka arvioivat työntekijöiden asenteita ja käsityksiä liittyen tietoturvaan. Martinsin ja Eloffin (2002) tutkimuksessa käytettiin erilaisia mittausasteikkoja arvioimaan työntekijöiden erilaisia käsityksiä. Hyödynnetyt asteikot olivat monivalintakysymykset, joissa vastaaja sai vastata yhden tai useamman vastausvaihtoehdon sekä Likertin asteikot, joissa vastaaja valitsi itselleen sopivimman vastauksen. Vastausvaihtoehdot olivat: täysin eri mieltä, eri mieltä, en osaa sanoa, samaa mieltä sekä täysin samaa mieltä.

Tietoturvallisuuden mittaamiseen liittyy myös haasteita, sillä mittaamisen kohteeseen vaikuttaa myös esimerkiksi käyttäytymiseen liittyvät tekijät sekä arvaamattomat aukot tietoturvassa. Tavallisimpia ongelmia mittaamisessa on kohteen rajaus, eli mitä mitataan ja mitä tekijöitä tulisi jättää mittauksen ulkopuolelle. Muita mahdollisia haasteita ovat esimerkiksi riskien mittaus lukuarvoina sekä kohdistusongelma eli toimien ja suojausten oikea kohdistaminen ja tunnistaminen. Mittauksessa on hyvä huomioida myös mittarin tärkeimmät tunnusmerkit. Näitä ovat muuan muassa helppolukuisuus, yksiselitteisyys, validius ja oikea-aikaisuus. Mittarin vaikutukset tutkimuksen tuloksiin on oltavat mahdollisimman vähäiset ja tulosten tulisi olla helppolukuisia ja helposti hyödynnettävissä. (Laaksonen ym. 2006, 270–271)

6 Tutkimuksen menetelmä

Empiirinen tutkimus tarkoittaa tutkimusta, jonka toteuttamiseksi kerätään reaalitietoa ja kerätty tieto pyritään hyödyntämään johdonmukaisesti. Tutkimusta varten kerättyä tietoa

kutsutaan tutkimus- tai havaintoaineistoksi. Tutkimukseen aineisto voidaan kerätä erilaisilla tiedonkeruun menetelmillä, jotka perustuvat joko määrälliseen tai laadulliseen tutkimusotteeseen. Tutkimuksen kohde ja aihealue usein ohjaavat valintaa menetelmän suhteen. Tutkimus voidaan myös toteuttaa yhdistelemällä erilaisia menetelmiä. (Heinonen, Keinänen, Paasonen 2013, 21–35.)

Kvalitatiivinen eli laadullinen tutkimus on suuntaus, jossa tarkoitus on ymmärtää esimerkiksi tutkittavan kohteen laatua tai ominaispiirteitä ja tällä tutkimussuuntauksella tutkitaan usein sellaisia aiheita, joita entuudestaan on tutkittu vähän ja niitä pyritään ymmärtämään paremmin. (Ojasalo, Moilanen & Ritalahti 2009, 93–94.) **Kvantitatiivinen eli määrällinen tutkimus** taas antaa vastauksia kysymyksiin ”kuinka paljon tai kuinka usein” ja kerättyä tietoa tutkitaan numeerisesti. Määrällisen tutkimuksen tunnuspiirteitä ovat muun muassa mittarit, suuri vastausjoukko, sekä tiedon esittäminen numeroiden avulla. (Vilkka 2007, 13–15.)

Tutkimuksen toteutus voidaan tehdä erilaisilla kohteelle sopivilla tiedonkeruumenetelmillä. Kyselylomake on hyvä keino toteuttaa tutkimus, jos tutkittavia on määrällisesti paljon ja halutaan selvittää vastaus useampiin kysymyksiin. (Vilkka 2007, 28). Kyselylomakkeen kysymykset pyrkivät selvittämään vastausta tutkimuksen metakysymykseen, eli tutkimusongelmaan. Kyselylomakkeen kysymykset ovat usein apukysymyksiä tutkimusongelman selvittämiseen, eli itse metakysymystä ei välttämättä esitetä kyselylomakkeessa. (Kananen 2012, 122.)

Kyselylomakkeen kysymysten laadinnassa tulee ottaa huomioon erilaisia tutkimukseen vaikuttavia tekijöitä. On olennaista suunnitella miten aineisto tullaan käsittelemään, miten tiedot lomakkeelle syötetään sekä miten tulokset raportoidaan. Tutkimuksen päämäärä ohjaa kysymysten asettelua ja vaikuttaa siihen kuinka tarkkoja vastausvaihtoehtoja kyselyyn laaditaan. (Heikkilä 2014, 45.)

Heikkilän (2014, 46) mukaan tutkimuksen kyselylomakkeen rakentamiseen kuuluu alla olevat vaiheet:

- nimetään tutkittavat asiat
- suunnitellaan lomakkeen rakenne
- muotoillaan kysymykset
- testataan lomake
- mahdollisten korjaustoimenpiteiden toteuttaminen
- lopullisen lomakkeen lähetys

Kyselylomake voidaan rakentaa hyödyntämällä erilaisia kysymystyyppejä. Vaihtoehtoja ovat esimerkiksi avoimet kysymykset, vaihtoehdolliset kysymykset sekä asteikkotyyppiset kysymyk-

set. (Kananen 2012, 125–131.) Kysymysten muotoiluun ja sisältöön on myös hyvä kiinnittää huomiota. Hyvän kysymykset tunnusmerkkejä ovat kysymyksen tarpeellisuus, kohteliaisuus, selkeys ja kielellisesti moitteeton ulkoasu. Kysymys ei saisi myöskään olla turhan johdatteleva tai monimutkainen (Heikkilä 2014, 54.)

Kyselytutkimukseen kuuluu myös saatekirje, joka lähetetään kohderyhmälle pyydettäessä vastamaan kyselyyn. Saatekirjeen tarkoitus on avata tutkimuksen taustaa ja herättää lukijan mielenkiinto vastaamaan kyseiseen kyselyyn. Hyvässä saatekirjeessä tiedotetaan tutkimuksen tavoite, toteuttaja, vastausten käyttö ja luottamuksellisuus sekä viimeinen mahdollinen vastauspäivä. Saatekirjeen tulisi olla mahdollisimman ytimekäs sekä kohtelias. (Heikkilä 2014, 59.) Muita kyselyn toteutuksessa tärkeitä huomioon otettavia asioita ovat kyselyn ajoitus ja mahdollisten muistutusviestien lähettäminen. Verkossa lähetettävän kyselyn ajankohta on tärkeää suunnitella tarkoin ja huomioida esimerkiksi vastausprosenttiin vaikuttavat sesongit tai vuodenajat. (Vilkka 2007, 28.)

Kyselytutkimuksen tuloksia voidaan analysoida monella eri tavalla. Tyypillisimpiä analysointi menetelmiä ovat selvittämiseen ja ymmärtämiseen pyrkivät lähestymistavat. Laadullisessa tutkimuksessa tulokset voidaan analysoida esimerkiksi teemoittelulla tai sisällönerittelyllä. (Hiltunen 2022, 9–10.) Määrällisen tutkimuksen yleisimpiä analysointimenetelmiä ovat tunnuslukuihin perustuvat analyysit, joilla kuvataan muuttujien välisiä suhteita. Näitä ovat esimerkiksi keskihajonta, mediaani, moodi sekä variaatiokerroin. (Vilkka 2007, 128–119.) Kyselyyn pohjautuvat tutkimustulokset voidaan analysoida myös havainnollistamisen avulla. Tulokset kootaan esimerkiksi graafeihin tai diagrammeihin tai niitä voidaan havainnoida myös esimerkiksi frekvenssitaulukoiden sekä tunnuslukutaulukoiden avulla. (Heikkilä 2014, 88.)

7 Tutkimuksen toteutus

Tutkimus toteutettiin kyselylomakkeella, jossa hyödynnettiin sekä laadullista että määrällistä tiedonkeruumenetelmää. Kyselylomakkeen kysymykset olivat monivalintakysymyksiä, väittämiä ja Likertin- asteikollisia kysymyksiä sekä kyselyyn kuului myös yksi avoin kysymys. Laadullisen tiedonkeruun avulla selvitettiin työntekijöiden ajatuksia, käyttäytymistä ja asenteita kohdeorganisaatiossa. Määrällisen menetelmän elementtejä tutkimukseen toi Likertin-asteikon hyödyntäminen sekä tietoturvatietoisuuden tason mittaus vastauksista numeerisesti. Näin ollen tulosten analysoinnissa tarkastellaan numeerista dataa sekä myös kategorisoitavaa ja tulkinnan varaista dataa.

Tutkimus kokonaisuudessaan koostuu aiheen kirjallisuuskatsauksesta, kohdeorganisaatiolle toteutetusta kyselystä sekä tulosten analysoinnista ja kehitysehdotusten esittelystä. Kysely tietoturvatietoisuudesta jaettiin kolmeen osaan, jotka olivat; taustatiedot, organisaation

ohjeet tietoturvasta, tietoturvaan liittyvät asenteet- ja käyttäytyminen sekä tietoturvatietoisuus.

Kysymysten sisältö rakennettiin vastaamaan opinnäytetyön tutkimuskysymykseen ja aseteltujen kysymysten avulla pyrittiin saamaan mahdollisimman todenmukainen kuva kohdeorganisaation henkilöstön tietoturvatietoisuudesta. Kysymykset kyselyn taustatiedoista valittiin sillä perustein, jotta voitaisiin tutkia, onko työntekijän työskentelyfunktiolla, iällä tai työskentely ajalla kohdeorganisaatiossa merkittäviä vaikutuksia tietoturvatietoisuuteen. Esimerkiksi perehdytyksen kehityksellä, funktiokohtaisilla koulutuksilla ja ohjeistuksilla sekä työntekijän iällä viitaten teknologiatietoisuuteen voidaan olettaa olevan oleellinen merkitys myös tietoturvaan liittyvän tietoisuuden osalta. Taustatietojen avulla pyrittiin myös varmistamaan, että vastaajaryhmä kuvastaa tarpeeksi laajasti tutkittavaa perusjoukkoa. Muut kyselyn osioiden kysymykset ovat suunniteltu niin, että saadaan mahdollisimman kattava kuva yleiselllä tasolla olevasta tietoturvatietoisuudesta organisaatiossa. Kysymysten rakentamisessa on käytetty apuna työn alussa esiteltyä kirjallisuuskatsausta sekä yrityksen tietoturvallisuuskäytäntöihin liittyvää ohjeistusta. Organisaation sisäinen ohjeistus käsittelee muun muassa sähköpostin, internetin, salasanojen sekä käyttäjävaltuuksiin liittyvää turvallista toimintaa. Kyselyssä pyrittiin myös huomioimaan mahdollisimman relevantit aihealueet henkilöstön päivittäisen työskentelyn kannalta.

Kysymysten asettelussa päädyttiin hyödyntämään erilaisia kysymystyyppejä, jotta kyselyn arvo ja kattavuus olisi mahdollisimman suuri kohdeorganisaatiolle. Asteikkotyyppisissä kysymyksissä hyödynnettiin Likertin asteikkoa (kysymykset 6–8). Likertin asteikko on yleinen mielipideväittämissä hyödynnetty asenneasteikko, jossa vastaaja valitsee parhaiten omaa mielipidettä edustavan vastauksen (Heikkilä 2014, 51). Taustatietojen selvittämisessä (kysymykset 1–3) sekä tietoturvatietämykseen liittyvissä kysymyksissä (kysymykset 19, 22–23, 29–32) käytettiin strukturoituja kysymyksiä, eli vastaajalle esitettiin valmiit vastausvaihtoehdot, joista hän valitsi omia tietojaan vastaavan vaihtoehdon. Muut kyselyn kysymykset esitettiin käyttämällä väittämiä (tosi/epätosi) sekä kyselyn viimeinen kysymys toteutettiin avoimen kysymyksen avulla, jossa vastaajalla oli vapaus kirjoittaa omia ajatuksia organisaation tietoturvaan liittyen.

Opinnäytetyön kysely tietoturvatietoisuudesta toteutettiin Microsoft Formsin avulla. Sähköinen kysely on helppokäyttöinen ja edullinen vaihtoehto, joka edesauttaa kyselyn tulosten helpompaa käsittelyä esimerkiksi Excelissä tai muissa tilasto-ohjelmissa. (Heikkilä 2014, 66–67). Sähköisen kyselylomakkeen toimivuus sekä saatekirjeen selkeys testattiin lähettämällä kyselylomake testaustaukseen organisaation HR:lle sekä kahdelle organisaation ulkopuoliselle henkilölle. Virallinen kysely lähetettiin sähköpostilla kohdeorganisaation Suomen henkilöstölle 13.12.2021. Viesti sisälsi linkin kyselyyn sekä saatekirjeen (Liite 1). Alkuperäinen kysely koh-

deorganisaatiolle on toteutettu englanniksi, mutta tässä opinnäytetyössä tulokset analysoidaan suomeksi.

Vastausaikaa kohderyhmälle annettiin 9 päivää. Ensimmäinen muistutusviesti kyselyyn vastaamisesta lähetettiin 72 tuntia ensimmäisen viestin jälkeen ja toinen muistutusviesti lähetettiin kaksi päivää ennen kyselyn sulkeutumista. Kyselyn vastaanotti yhteensä 82 kohdeorganisaation työntekijää, joista kyselyyn vastasi 39. Kyselyn vastausprosentiksi saatiin siis 48 prosenttia. Vehkalahden (2008, 44) mukaan tavanomainen vastausprosentti kyselytutkimuksissa yleisesti on alle 50 %.

Aineistonanalyysi tehtiin ryhmittelemällä tulokset Microsoft Excelin avulla ja tarkempana analysointi välineenä hyödynnettiin myös SPSS-ohjelmaa (Statistical Package for Social Sciences). Microsoft Excelin ja SPSS:n avulla aineiston monivalintakysymysten sekä väittämien vastauksia analysointiin frekvenssijakauman avulla sekä tunnuslukujen avulla. Kyselylomakkeen viimeisen avoimen kysymyksen tulokset analysointiin sisällönalyysillä, jossa vastaukset ryhmiteltiin niin että niistä pyrittiin löytämään eroja ja yhtäläisyyksiä aineistolähtöisesti.

8 Kyselyn tulokset

Tässä luvussa käsitellään yhteenveto tehdyn kyselyn tuloksista. Tulosten käsittely tehdään samassa järjestyksessä kuin kyselyn asettelu, eli ensin esitellään yleiset taustatiedot, jonka jälkeen siirrytään avaamaan kohdeorganisaation tietoturvapolitiikkaan ja ohjeisiin liittyviä kysymyksiä, tietoturvakäyttäytymistä ja asenteita, sekä viimeisenä tietoon perustuvaa tietämystä/osaamista. Lopuksi tuloksia tarkastellaan vastaajien taustatietoihin perustuen ja vertaillaan eli funktioiden ja ikäryhmien välisiä vastauksia.

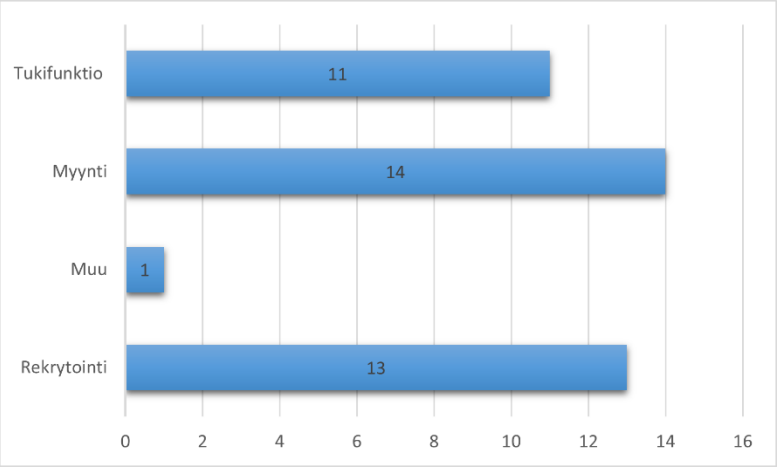
Taustatiedot sekä tietoturvapolitiikkaan ja ohjeisiin liittyvät esitellään pylväs- ja ympyräkaavioiden avulla hyödyntämällä vastausprosentteja sekä vastaaja määrää kappaleittain. Muut osiot, eli käyttäytymiseen, asenteisiin ja tietoon perustuvat vastaukset analysoidaan hyödyntämällä kaavioita sekä erilaisia tunnuslukuja kuten keskiarvoa sekä keskihajontaa. Keskiarvo on yksi käytetyimmistä tunnusluvuista, jonka avulla voidaan havainnoida numeerisesti mitattavia tasoja. Keskiarvo kertoo muuttujan keskimääräisen arvon ja keskihajonta puolestaan selittää keskimääräistä hajontaa vastauksissa. (Vehkalahti 2008, 54). Tulosten analysoinnin välineenä on käytetty Microsoft Exceliä sekä SPSS-ohjelmaa.

8.1 Taustatiedot

Kyselyssä selvitettiin ensimmäiseksi kyselyn vastaajien ikäjakaumaa. Suurin osa vastaajista eli 66,67 % sijoittui ikäryhmään 26–34 vuotta. 20,51 % vastaajista löytyi ikäryhmästä 18–25-vuotiaat sekä loput vastaajista eli 13 % ilmoitti kuuluvansa ikäryhmään 35–44-vuotiaat. Yli 45-

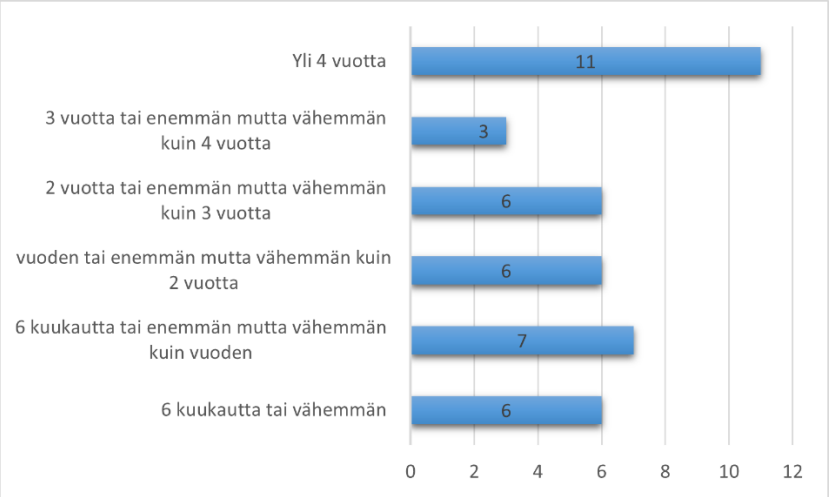
vuotiaiden ryhmästä ei kertynyt yhtään vastausta. Ikäjakauma selvitettiin, jotta tuloksia voidaan varmistaa, että vastaajajoukko kuvastaa mahdollisimman monipuolisesti kohdeorganisaatioita. Kohdeorganisaation työntekijöiden ikäjakauma vastaa suhteellisen hyvin myös kyselyn ikäjakaumaa, sillä työntekijöiden ikä keskiarvollisesti yrityksessä X on 31 vuotta.

Toisena taustatietona kysyttiin vastaajien työskentely funktiota. Kuten kuviosta 6 voidaan nähdä, funktiojakauma vastaajien kesken oli todella tasainen ja vastauksia saatiin hyvin jokaisesta kolmesta kohdeorganisaation pääfunktiosta. 36 % vastaajista ilmoitti työskentelevänsä myynnissä, 33 % rekrytoinnissa sekä 28 % tukifunktiossa. Yksi vastaus, eli 2,56 % oli luokiteltu kategoriaan ” Muut”. Työskentelyfunktiolla saattaa olla merkittävä vaikutus esimerkiksi perehdytykseen tai tietoturvaan liittyviin asenteisiin, jonka vuoksi haluttiin selvittää tämän taustatekijän mahdolliset vaikutukset tietoturvatietoisuuteen.



Kuvio 6: Jakauma työntekijöiden työskentely osastoista

Tällä hetkellä yrityksen X myynnissä työskentelee 39 henkilöä, rekrytoinnissa 21, tukifunktiossa 17 ja ”muut” ryhmään voidaan luokitella 5 työntekijää. Näin ollen eniten vastaajia suhteessa funktion kokoon saatiin eniten tukifunktiosta ja vähinten myynnin yksiköstä. Kokonaisuudessaan vastaaja joukon voidaan katsoa edustavan tyydyttävästi yrityksen kaikkia funktioita verratessa vastausten jakautumista yrityksen normaaliin jakaumaan funktioiden kesken.



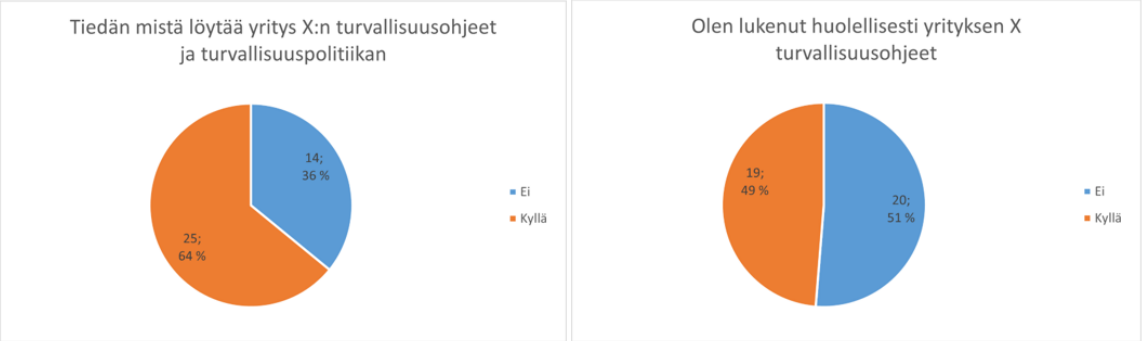
Kuvio 7: Vastaajan työvuodet yrityksessä X

Kyselytutkimuksessa kolmantena taustatietona tutkittiin työntekijän työskentely aikaa kohdeorganisaatiossa. Eniten vastauksia eli 28 % vastauksista saatiin yli 4 vuotta organisaatiossa työkennelleiltä henkilöiltä ja vähinten eli 8 % työntekijöiltä, jotka ovat olleet yrityksessä 3 vuotta tai enemmän, mutta vähemmän kuin 4 vuotta. Loput vastauksista jakautuivat suhteellisen tasaisesti muiden ryhmien kesken (Kuvio 7). Vastausten jakauma kuvaa suhteellisen realistisesti yrityksen X henkilöstöä, sillä tällä hetkellä keskiarvo työskentely vuosissa on 3,2 vuotta.

8.2 Ohjeistukset ja tietoturvapolitiikka

Kyselyn toinen osio koostuu kysymyksistä liittyen kohdeorganisaation tietoturvaohjeisiin ja tietoturvapolitiikkaan. Kysymysten perusteella oli tarkoitus selvittää kuinka hyvin työntekijät tietävät mistä yrityksen tietoturvaan liittyvä ohjeistus löytyy, onko sitä helppo noudattaa ja onko ohjeistukseen sekä tietoturvaan itsessään perehdytetty tarpeeksi työntekijöiden näkökulmasta.

Kyselytutkimuksen neljäs ja viides kyselyn kysymys käsitteli yrityksen X turvallisuuspolitiikka ja ohjeita. Kuviosta voimme nähdä, että 64 % vastaajista kertoi tietävänsä mistä yrityksen turvallisuusohjeistus ja turvallisuuspolitiikka löytyvät (Kuvio 8). Kuitenkin vain 49 % vastaajista kertoi lukeneensa kyseisen ohjeen huolellisesti. Näin ollen yli puolet vastaajista eivät ole perehtyneet tarpeen mukaisesti yrityksen laatimaan ohjeistukseen koskien muun muassa tietoturvallisuutta.



Kuvio 8: Turvallisuusohjeiden löytäminen & lukeminen

Kysymyksissä 6–8 hyödynnettiin Likertin-asteikkoa ja vastausvaihtoehtoja oli annettu viisi: täysin samaa mieltä, samaa mieltä, neutraali, eri mieltä sekä täysin eri mieltä. Kysymykset liittyivät yrityksen X tietoturvapolitiikan noudattamiseen, tietoturvakoulutuksiin sekä omaan osaamiseen tietoturvaan liittyen. Kysymykset ovat analysoitu alla olevaan taulukkoon (Taulukko 2) laskemalla kysymysten moodi, keskiarvo sekä keskihajonta. Taulukossa vastausvaihtoehdoille on annettu numerokoodit 1–5, jonka avulla kyseiset laskelmat ovat toteutettu.

	5 Täysin eri mieltä	4 Eri mieltä	3 Neutraali	2 Samaa mieltä	1 Täysin samaa mieltä	Moodi	Keskiarvo	Keskihajonta
Mielestäni yrityksen X turvallisuuspolitiikkaa on helppo noudattaa	0 kpl	7 kpl	16 kpl	14 kpl	2 kpl	3	2,71	0,826
Koen, että olen saanut riittävästi tietoturvakoulutusta yrityksessämme	0 kpl	18 kpl	12 kpl	8 kpl	1 kpl	4	3,20	0,864
Koen, että minulla riittävät tiedot tietoturvasta työtäni varten	0 kpl	10 kpl	5 kpl	23 kpl	1 kpl	2	2,61	0,907

Taulukko 2: Tietoturvapolitiikka, ohjeistus ja osaaminen

Taulukosta voimme nähdä, että kysymyksen 6 (Mielestäni yrityksen X tietoturvapolitiikkaa on helppo noudattaa) moodiksi on saatu numero kolme ja keskiarvoksi 2,71. Tämä tarkoittaa sitä, että kysymykseen on annettu eniten neutraaleja vastauksia (41 %) ja toiseksi eniten (36 %) ”samaa mieltä” vastauksia. Kysymyksen keskihajonta kuitenkin kertoo, että vastauksissa on ollut myös pientä hajanaisuutta.

Kysymyksessä seitsemän vastaajilta kysyttiin, että kokevatko he saaneensa riittävästi tietoturvakoulutusta yrityksessä X. Kysymyksen moodiksi saatiin numero neljä ja keskiarvoksi 3,20.

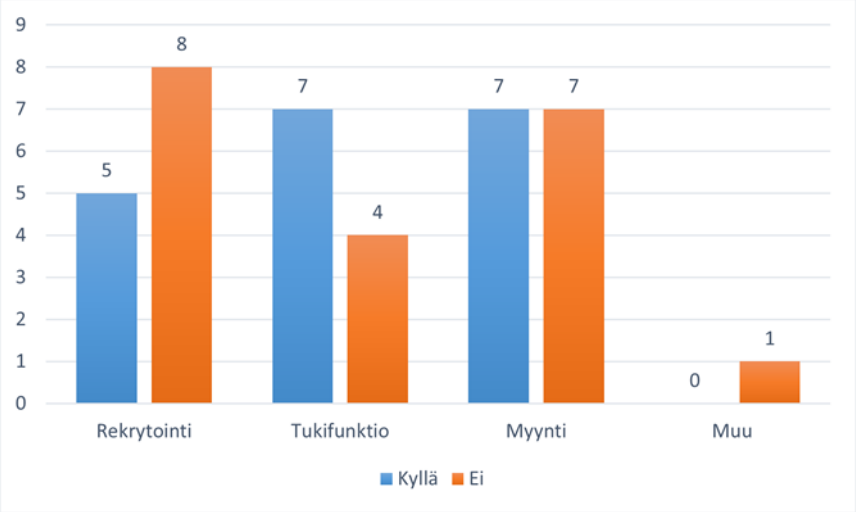
Numero neljä kuvastaa taulukossa vastausta ”Eri mieltä”, joten tämän perusteella voimme todeta, että suurin osa vastaajista kokee, että koulutus tietoturvasta yrityksessä X on puutteellinen. Yllä olevasta taulukosta voimme kuitenkin myös nähdä, että iso joukko vastaajista (12 kpl) jätti neutraalin vastauksen ja kahdeksan vastaajaa oli sitä mieltä, että yrityksen tietoturvakoulutus on ollut riittävä. Yksi vastaajista vastasi olevansa täysin erimieltä väittämän kanssa.

Kysymyksessä kahdeksan kyselyyn vastaajilta kysyttiin, että kokevatko he omaavansa riittävät tiedot/taidot tietoturvaan liittyen suhteessa omaan työhönsä. Kysymyksen moodiksi saatiin numero 2 ja keskiarvoksi 2,61. Moodi kertoo, että suurin osa vastaajista on ollut samaa mieltä väittämän kanssa, ja kokee omaavansa tarpeellisen tiedon tietoturvasta omaa työtä varten. Eri mieltä väittämän kanssa on ollut kuitenkin 10 vastaajista eli 26 prosenttia.

Taulukon 2 viimeiseen sarakkeeseen on myös laskettu vastausten keskihajonta, eli vastausten hajonta keskiarvosta. Taulukossa esitettyjen kysymysten keskihajonnat ovat suhteellisen samalla tasolla ja keskihajonnan voidaan todeta olevan suhteellisen matala. Hajontaa keskiarvojen ympärillä kuitenkin on, mikä kertoo vastaajien näkemyseroista kysyttyjen kysymysten suhteen. Suurin keskihajonta on taulukon viimeisessä kysymyksessä, eli kokevatko työntekijät, että heillä on riittävät tiedot tietoturvasta omaa työtänsä varten.

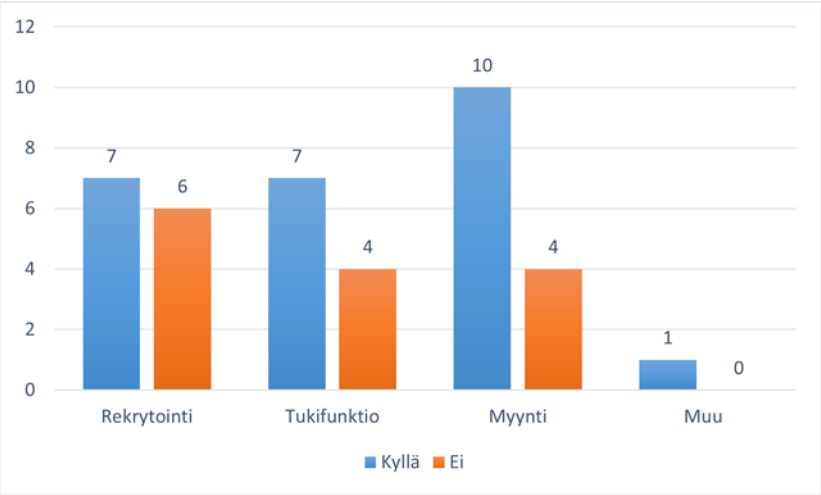
8.2.1 Tulokset funktioittain

Funktioiden merkitys liittyen yrityksen turvallisuusohjeistuksiin ja turvallisuuspolitikkaan sekä koulutuksiin voi olla suuri, jonka vuoksi näiden kyseisten osioiden tulokset ovat analysoitu myös funktioittain. Funktiokohtaiset erot voivat myös selittää yllä esitetyn taulukon (taulukko 2) keskihajontaa.



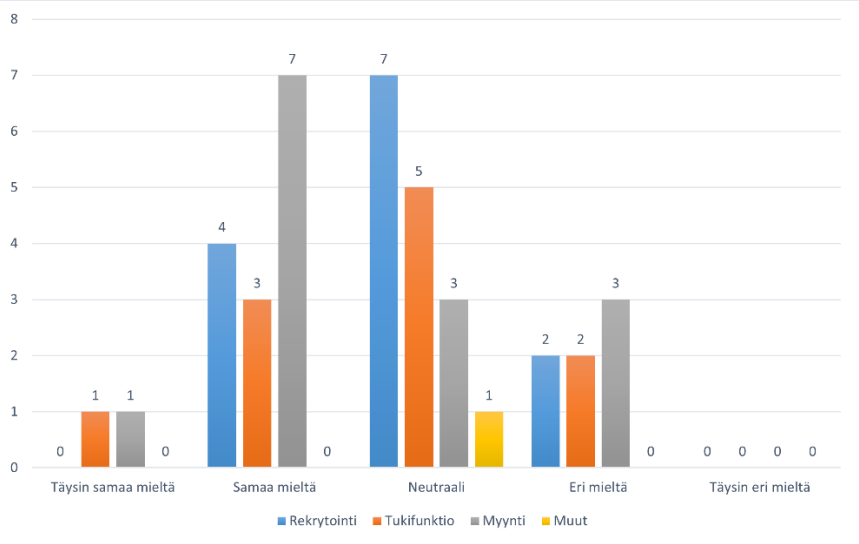
Kuvio 9: Tiedän mistä löytää yrityksen X turvallisuusohjeet ja turvallisuuspolitiikan

Kuviossa 9 nähdään jakauma siitä, kuinka hyvin kussakin funktiossa tiedetään mistä löytyy yrityksen X turvallisuusohjeet ja politiikka. Kuten kuviossa näkyy myynnin tulokset ovat jakautuneet hyvin tasaisesti, eli puolet vastaajista tietävät mistä ohjeet löytyvät ja puolet eivät tiedä. Huomioitavaa on, että rekrytoinnissa yli puolet kyselyyn vastanneista eivät tienneet mistä kyseisen dokumentin löytää. Tukifunktion tulokset ovat päinvastaiset verraten rekrytointiin ja yli puolet vastanneista tiesivät mistä turvallisuusohjeet ja turvallisuuspolitiikan voi löytää. Näistä tuloksista voimme pääteellä, että tieto turvallisuusohjeiden ja turvallisuuspolitiikan sijainnista vaihtelee huomattavasti eri yksiköiden välillä. Tähän tulokseen voi johtaa esimerkiksi funktioiden erilaiset ohjeistukset tai tiedottaminen turvallisuusasioihin liittyen työsuhteen alkaessa.



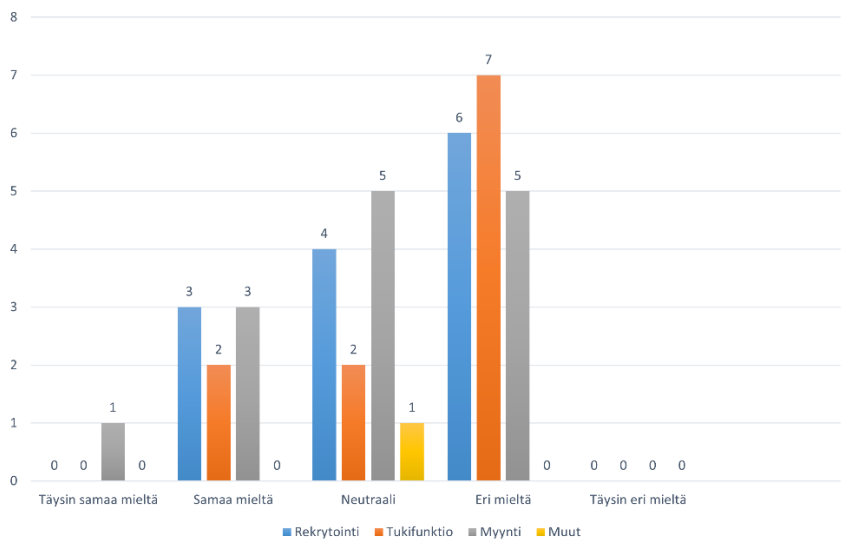
Kuvio 10: Olen lukenut yrityksen X turvallisuusohjeet huolellisesti

Yllä olevan kuvion (kuvio 10) perusteella voimme todeta, että funktioiden välillä löytyy myös hajontaa henkilöstön turvallisuusohjeiden lukemisesta. Suurin osa myynnissä työskentelevistä vastaajista eli 79 % kertoi lukeneensa turvallisuusohjeet huolellisesti, kun taas rekrytoinnin tulosten perusteella kuusi eli 46 % rekrytoinnin vastaajista ei ollut lukenut yrityksen turvallisuusohjeita ja politiikkaa. Myös tukifunktion vastauksista löytyi selkeää hajontaa ja seitsemän vastaajaa eli 64 % tästä funktiosta kertoi lukeneensa ohjeen ja neljä eli 36 % taas ei ollut lukenut ohjeistusta. Tuloksia tulkitessa voidaan todeta, että työskentely yksikkö voi vaikuttaa turvallisuusohjeistuksen lukemiseen. Tähän voi olla syynä taustalla esimerkiksi erilainen perehdytysohjelma tai esihenkilön antamat ohjeistukset tietoturvaan liittyen.



Kuvio 11: Mielestäni yrityksen X turvallisuuspolitiikkaa on helppo noudattaa

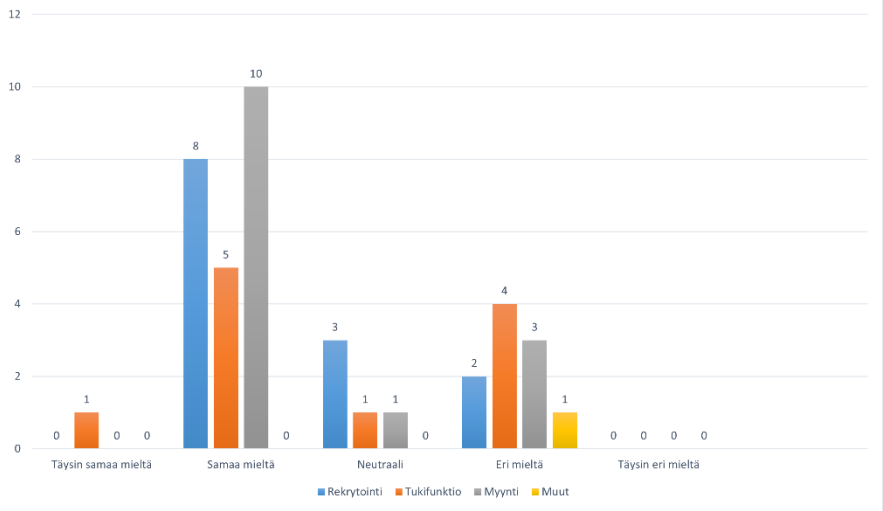
Kuviossa 11 on analysoitu kysymyksen: ”mielestäni yrityksen turvallisuuspolitiikkaa on helppo noudattaa” tulokset funktioiden jakaumat huomioiden. Tuloksista voimme nähdä, että etenkin myynnissä oltiin samaa mieltä esitetyn väittämän kanssa. Eniten neutraaleja kantaa ottamattomia vastauksia saatiin rekrytoinnista (7kpl) ja toiseksi eniten tukifunktiosta (5kpl). Funktioiden väliset erot vastausten jakaumissa ovat suhteellisen vähäisiä, mutta tuloksista on huomioitavissa, että myynnin henkilöstön mielestä turvallisuuspolitiikka on helpompi noudattaa suhteessa muihin vastaajaryhmiin.



Kuvio 12: Koen, että olen saanut riittävästi tietoturvakoulutusta yrityksessämme

Yllä olevasta kuviosta (kuvio 12) on nähtävissä, että suurin osa yrityksen X henkilöstöstä on sitä mieltä, että ei ole saanut riittävästi koulutusta tietoturvaan liittyen. Myynnissä 38 %,

rekrytoinnissa 46 % ja tukifunktiossa jopa 64 % vastasi, että ole mielestään saanut riittävää tietoturvakoulutusta yrityksessä. Myynnistä, rekrytoinnista ja tukifunktiosta löytyy kuitenkin myös vastaajia, jotka ovat samaa mieltä siitä, että ovat saaneet riittävästi koulutusta aiheeseen liittyen. Neutraaleja vastauksia on saatu jokaisesta funktiosta, mikä saattaa tarkoittaa, että osa henkilöstöstä ei esimerkiksi tunnista mikä koulutus luokitellaan tietoturvakoulutukseksi tai vastaajat eivät tiedä mikä määrä tietoturvakoulutusta olisi heille riittävä.



Kuvio 13: Koen, että minulla riittävät tiedot tietoturvasta työtäni varten

Kuvion 13 perusteella voidaan todeta, että suurin osa kyselyyn vastanneista kokee omaavansa riittävät tiedot tietoturvasta omaa työtänsä varten. Etenkin rekrytoinnissa ja myynnissä vastaajat olivat samaa mieltä asetetun kysymyksen kanssa. Tukifunktiosta kuitenkin neljä vastaajaa vastasi, että on eri meiltä väittämän kanssa, eli kokee että ei heillä ei ole riittäviä taitoja tietoturvasta omaa työtänsä varten. Muutoin jakauma vastausvaihtoehdoissa funktioiden kesken on suhteellisen tasainen. Tulosten perusteella voidaan todeta, että omalla työskentelyfunktiolla voi olla merkitys tietoturva taitojen/tietojen riittävyyteen. Tämä eroavaisuus voi johtua yksiköiden välisistä eroista työtehtävistä ja esimerkiksi tukifunktioiden työnkuvan vaatimukset tiedon käsittelyn suhteen voivat olla korkeammat.

8.3 Käyttäytyminen ja asenteet

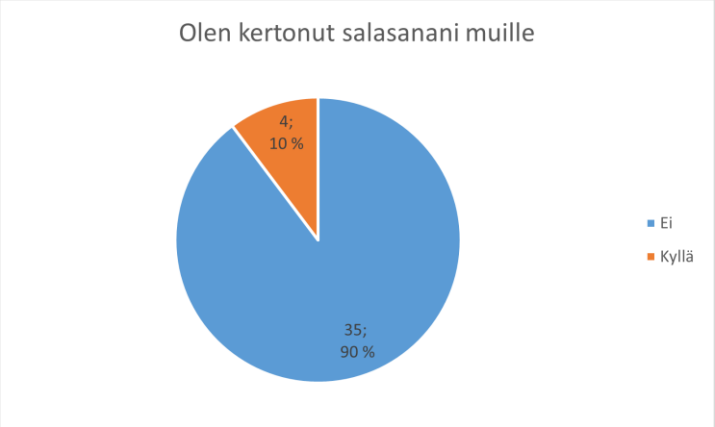
Tietoturvaan liittyvän käyttäytymisen ja asenteiden selvittämiseksi kohderyhmälle esitettiin muutamia erilaisia skenaariopohjaisia väittämiä sekä monivalintakysymyksiä. Kysymyksissä käsiteltiin salasanoihin liittyvää käyttämistä, suojattavan tiedon käsittelyä, tietokoneen päivityskäytäntöjä sekä monivaiheista tunnistautumista.

Ensimmäinen kysymys liittyen käyttäytymiseen ja asenteisiin käsitteli tietokoneen lukitsemiseen liittyvää toimintaa. Alla olevasta ympyräkaaviosta (Kuvio 14) voidaan nähdä, että vastaa-

jista 22 eli 56 prosenttia vastasi, että ei lukitse omaa tietokonettaan, vaikka poistuisi itse paikalta. Loput 44 prosenttia kertoi lukitsevansa tietokoneensa.

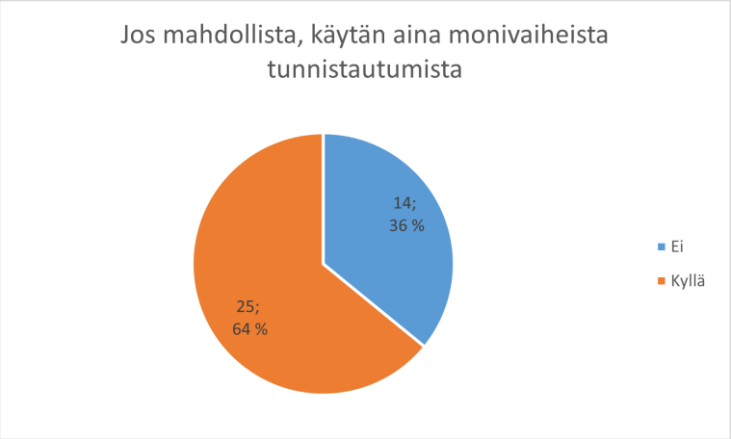
Kuvio 14: Tietokoneen lukitseminen

Toinen asenteita ja käyttäytymistä kuvaava kysymys liittyi työsalasanojen jakamiseen muiden kanssa. 90 % vastaajista vastasi ”Ei”, eli kertoi että ei ole jakanut salasanoja muiden kanssa. 10 % vastaajista eli 4 henkilöä vastasi kertoneensa salasanan/salasanoja muille henkilöille.



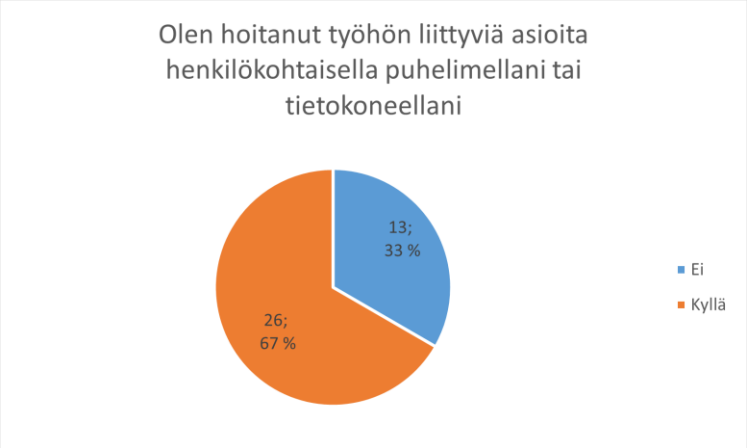
Kuvio 15: Salasanan jakaminen muille henkilöille

Kolmantena aiheena tässä osiossa kysyttiin monivaiheisen tunnistautumisen käyttöä. Kyselyyn vastaajilta kysyttiin käyttävätkö monivaiheista tunnistautumista kirjautumisessa aina kun on mahdollista. Yli puolet vastaajista, eli 64 % ilmoitti käyttävänsä monivaiheista tunnistautumista aina kun se on mahdollista. Loput 36 % vastasi kysymykseen ei, eli he eivät käytä monivaiheista tunnistautumista aina vaikka siihen olisikin mahdollisuus.



Kuvio 16: Monivaiheinen tunnistautuminen

Seuraavana kysymyksenä selvitettiin ovatko työntekijät käyttäneet omia laitteitaan, kuten tietokonetta ja puhelinta työasioiden hoitamiseen. Alla olevan kuvion (kuvio 17) perusteella voimme nähdä, että yli 33 % kyselyyn vastanneista on hoitanut työasioita omalla henkilökohtaisella laitteellaan. Vastaajista 26 eli 67 % vastasi kysymykseen kielteisesti, eli eivät ole hoitaneet työasioita omalla henkilökohtaisella tietokoneella tai puhelimella.



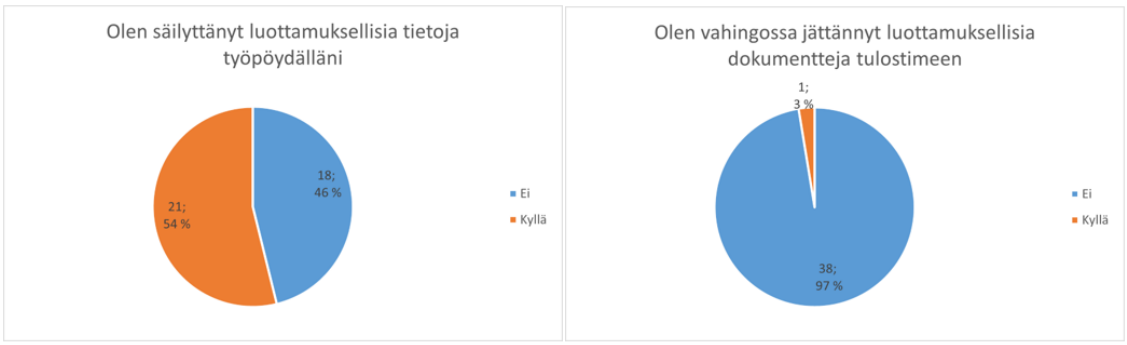
Kuvio 17: Henkilökohtaisten laitteiden käyttö työasioiden hoitamisessa

Alla olevassa kuviossa 18 tarkastellaan kysymysten 13 ja 14 tuloksia. Kysymyksessä 13 kysyttiin, että sisältääkö vastaajan työssä käyttämät salasanat vähintään 8 merkkiä pitäen sisällään isoja ja pieniä kirjaimia, erikoismerkkejä sekä numeroita. Vastaajista 33, eli 85 % vastasi kyllä, eli salasanat täyttävät kysymyksen kriteerit. Loput 15 % vastasi kysymykseen kielteisesti, eli ilmoitti että heidän käyttämänsä salasanat eivät täytä kysymyksessä esitettyjä kriteerejä. Kysymyksessä 14 selvitettiin, että käyttävätkö työntekijät usein samoja salasanoja niin työssä kuin henkilökohtaisessa elämässä. Vastaajista 24 eli 62 % prosenttia vastasi kysymykseen kielteisesti eli vastauksen perusteella kertoo käyttävänsä eri salasanoja töissä ja vapaa-ajalla. Loput vastaajista eli 38 % käyttää usein eri salasanoja työssä ja henkilökohteisessa elämässä.

Näiden tulosten perusteella voimme todeta, että salasanakäytännöt yrityksessä X ovat suhteellisen turvalliset ja työntekijät kiinnittävät huomioita salasanojen vaikuttavuuteen.

Kuvio 18: Salasanakäytännöt

Kuviossa 19 käsitellään kysymysten 15 ja 16 tuloksia, jotka liittyvät käyttäytymiseen koskien suojattavaa tietoa. Suojattava tiedon oikeanlainen käsittely ja tunnistaminen on olennaisessa osassa monessa yrityksen X työnkuvassa, joten aihetta on kyselyssä käsitelty useampaan otteeseen erilaisista näkökulmista. Kyselyssä kysyttiin ovatko työntekijät säilyttäneet työpöydällään luottamuksellisia tietoa sekä ovatko he jättäneet luottamuksellisia dokumentteja vahingossa tulostimeen. Kuten kuviosta näkyy (Kuvio 15) vastaajista yli puolet, eli 54 % on säilyttänyt luottamuksellisia tietoja omalla työpöydällään. Puolestaan luottamuksellisia tietoja tulostimeen vahingossa oli jättänyt vain yksi kyselyyn vastanneista eli 3 %. Näiden tulosten perusteella voimme päätellä, että luottamuksellisten tietojen säilyttämisessä olisi parantamisen varaa, vaikka kysymyksen 16 tulokset antavatkin positiivisen tuloksen.



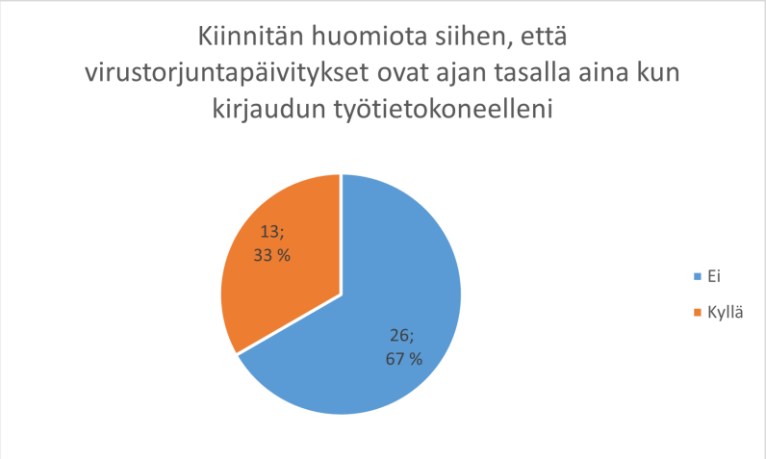
Kuvio 19: Luottamuksellisten tietojen säilytys

Kuviosta 20 voidaan tulkita työntekijöiden käyttäytymistä luottamuksellisten tietojen käsittelyn/toimituksen suhteen (kysymys 17). Yrityksessä X luottamuksellisten dokumenttien käsittely ja eteenpäin toimitus on lähes päivittäistä ja siksi haluttiin selvittää ovatko työntekijät lähettäneet kyseisiä dokumentteja tavallisen sähköpostin välityksellä. Yrityksessä ei ole käy-

tössä suojatun sähköpostin toimittamista, vaan luottamuksellisten tiedot lähetetään lähtökohtaisesti erillisen ohjelman kautta. Vastaajista 26 eli 67 % prosenttia vastasi kysymykseen 17 myöntävästi, eli kertoi lähettäneensä luottamuksellisia tietoja sähköpostin välityksellä. Loput 33 % vastasivat kysymykseen kielteisesti.

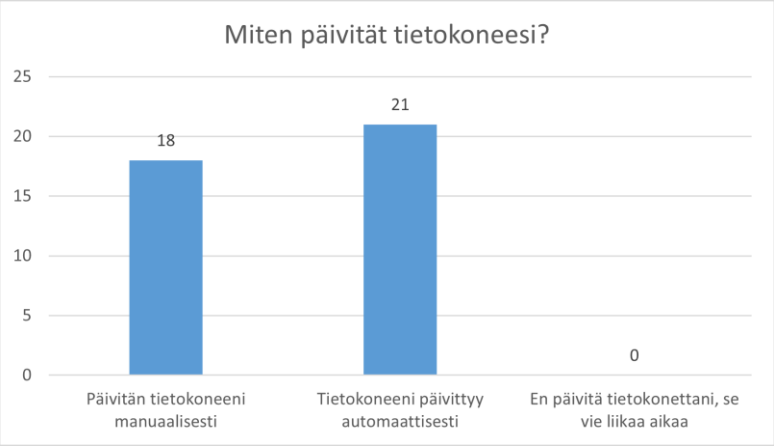
Kuvio 20: Luottamuksellisten tietojen lähettäminen sähköpostilla

Kysymyksessä 18 käsiteltiin virustorjuntapäivitysten huomioimista omalla työtietokoneella. Virustorjunnan päivitykset tietokoneilla ovat erittäin tärkeitä yrityksen kaikissa työtehtävissä, sillä tietokonetta käytetään päivittäin ja erilaisten ohjelmistojen ja luottamuksellisten tietojen käsittely on iso osa työtehtäviä. Alla olevasta kuviosta (kuvio 21) voimme nähdä, että yli puolet, 67 %, kyselyyn vastanneista vastasi kysymykseen kielteisesti, eli he eivät kiinnitä huomioita virustorjuntapäivityksiin kirjautuessaan työkoneelle. Loput 33 % vastasi kiinnittävänsä virustorjuntapäivityksiin huomiota.



Kuvio 21: Virustorjuntapäivitysten huomioiminen

Viimeinen kysymys (kysymys 19) käyttäytyminen/asenteet osiossa käsitteli tietokoneen päivittämistä yleisellä tasolla. Kysymyksessä vastaajilta kysyttiin, että miten he päivittävät tietokoneensa ja vastausvaihtoehdoksi annettiin kolme vaihtoehtoa. Vaihtoehdot olivat; ”päivitän tietokoneeni manuaalisesti”, ”tietokoneeni päivittyy automaattisesti” sekä ”en päivitä tietokonettani, se vie liikaa aikaa”. 46 % ilmoitti päivittävänsä tietokoneensa manuaalisesti ja 54 % kertoi tietokoneensa päivittyvän automaattisesti. Vastausten mukaan kukaan ei jätä tietokonettansa päivittämättä.



Kuvio 22: Tietokoneen päivittäminen

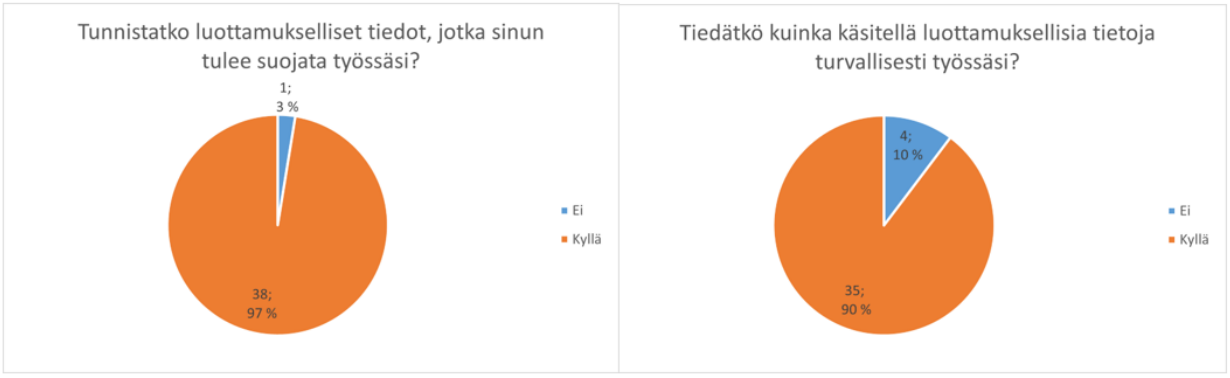
8.4 Tietous

Kyselyn kysymykset 20–35 käsittelivät vastaajan tietämystä tietoturvaan liittyen. Kysymyksissä esitettiin erilaisia väittämiä sekä monivalintakysymyksiä. Osion ensimmäiset kysymykset käsittelivät suojattavaa tietoa ja siihen liittyvää toimintaa. Nämä kysymykset ovat analysoitu sanallisesti ja osa tuloksista on esitelty hyödyntäen ympyrä- ja palkkikuvioita. Muut väittämät

sekä monivalinnat ovat analysoitu taulukoiden avulla käyttäen keskiarvomittausta väärien ja oikeiden vastausten avulla.

8.4.1 Luottamukselliset tiedot

Kuviossa 23 on esitelty kysymysten 20–21 vastausten jakauma. Kysymyksissä kysyttiin tunnistaako työntekijä luottamukselliset tiedot, jotka hänen tulee suojata työssään ja tietääkö työntekijä miten luottamuksellisia tietoja tulee käsitellä. 39 vastaajasta 38 kertoi tunnistavansa luottamukselliset suojattavat tiedot ja 35 vastaajista kertoi tietävänsä, kuinka luottamuksellista tietoa tulee käsitellä. Näin ollen voidaan todeta, että suurin osa, 90 % tai yli vastaajajoukosta kokee omaavansa hyvän käsityksen luottamuksellisista tiedoista ja niiden turvallisesta käsitellystä.



Kuvio 23: Suojattavan tiedon tunnistaminen ja käsittely

Kysymyksessä 22 vastaajilta kysyttiin monivalinnan avulla, että mitä tietoja käsitellessä tulisi erityisesti huomioida tietoturvallisuus. Vastausvaihtoehdot olivat: sopimukset, henkilötiedot, talouteen liittyvät asiakirjat, kaikki yllä mainitut sekä ei mikään yllä mainituista. Viidestä vastausvaihdosta yksi oli oikea, eli vastaus ”kaikkia yllä mainittuja”. Tähän kysymykseen kaikki 39 vastaajaa vastasi kysymykseen oikein, eli jokaisella vastaajalla oli käsitys suojattavista tiedoista. Vastausvaihtoehdoiksi oli valittu erityisesti yrityksessä päivittäin käsiteltäviä tietoja.

Seuraavassa monivalintakysymyksessä (kysymys 23) haluttiin selvittää tietävätkö työntekijät, että kuka yrityksessä X vastaa tietoturvan varmistamisesta/toteutumisesta. Tässäkin kysymyksessä vastausvaihtoehtoja oli annettu viisi, joista yksi oli oikea. Vastausvaihtoehdot olivat: työntekijät, johtoryhmä, henkilöstöhallinto, kaikki yllä mainitut sekä ei mikään yllä mainituista. 35 vastaajaa eli 90 % vastasi kysymykseen ”kaikki yllä mainitut” joka oli oikea vastausvaihtoehto. Loput neljä vastaaja eli 10 % vastasi kysymykseen vaihtoehdon ”työntekijät”. Muihin vaihtoehtoihin ei tullut vastauksia.

8.4.2 Tietoisuuteen liittyvät väittämät & monivalintakysymykset

Alla olevassa taulukossa (Taulukko 3) on kuvattu kysymysten eli väittämien 24–28 vastauksien paikkaansa pitävyys keskiarvon avulla. Taulukossa esitellyssä analyysissa numero yksi (1) kuvastaa eriomaista tietoisuutta ja numero nolla (0) epätietoisuutta. Vastaajalla on näin ollen kyseisissä väittämissä annettu vastausvaihtoehdot ”tosi” ja ”epätosi. Oikeata vastauksesta analyysissa on annettu numero yksi ja väärästä 0.

Kysymys= K	K24: Tietokoneellani ei ole arvoa hakkereille, he eivät kohdista iskujaan minuun	K25: Sähköpostin todennus on hyvä tapa suojautua tietojenkalasteluhyökkäyksiä vastaan	K26: Tietokoneelle tallennetut varmuuskopiotiedostot estävät tietojen katoamisen kiristysohjelmahyökkäyksen sattuessa	K27: Julkiset verkkoyhteydet ovat turvallisia käyttää luottamuksellisiin toimintoihin, jos niihin tarvitaan salasana	K28: Pikaviestit, ovat turvallisempia käyttää tavalliseen sähköpostiin verrattuna	Yhteensä
Validit vastaukset (kpl)	39	39	39	39	39	39
Puuttuvat (kpl)	0	0	0	0	0	0
Tietoisuuden taso (keskiarvo %)	0,95	0,62	0,74	0,95	0,85	0,82
Minimi=epätietoisuus	0	0	0	0	0	0
Maksimi=tietoisuus	1	1	1	1	1	1

Taulukko 3: Tietämykseen liittyvien väittämien analyysi

Jokaisessa väittämässä tietoisuuden arvo on yli 0,60 eli yli 60 % vastaajista on vastannut jokaiseen väittämään oikein. Kysymyksessä 24 ja 27 tietoisuuden arvo oli 0,95 eli vain kaksi 38 vastaajasta vastasi kysymykseen väärin. Alhaisin tietoisuuden arvo alla olevista väittämistä saatiin kysymyksessä 24, joka oli 0,74. Tässäkin kysymyksessä vain 10 vastaajista vastasi kysyttyyn väittämään väärin. Kokonaisuudessa tietämykseen liittyvien väittämien tulokset olivat kiitettäviä, sillä jokaiseen väittämään yli puolet kyselyyn vastanneista valitsi oikean vastausvaihtoehdon.

Taulukossa 4 on analysoitu kyselyn kysymykset 29–32 jotka koostuivat monivalintakysymyksistä liittyen tietoturvaosaamiseen. Monivalintakysymyksissä vastaajalle esitettiin kolme vastausvaihtoehtoa, joista yksi oli oikein. Taulukossa on esitelty kyseisten kysymysten vastauksien keskiarvo muodostamalla se vertailemalla oikeita ja vääriä vastauksia. Kyseinen keskiarvo tässä tutkimuksessa kuvastaa tietoisuuden tasoa. Kyselyn tarkat kysymykset ja niiden vastausvavaihtoehdot löytyvät liitteestä 2.

Kysymys=K	K29: Mitä pitäisi tehdä haittojen minimoimiseksi, jos joudut tietojenkalasteluhuijauksen uhriksi?	K30: Mitä sinun tulisi tehdä ensimmäisenä, jos epäilet haittaohjelmatartuntaa?	K31: Mikä seuraavista on paras tapa suojautua haittaohjelmilta tai kiristysohjelmilta?	K32: Mikä on yleisin tapa saada virustartunta tietokoneeseen?	**Yhteensä**
Validit (kpl)	39	39	39	39	39
Puuttuvat (kpl)	0	0	0	0	0
Tietoisuuden arvo (keskiarvo %)	0,92	0,41	0,62	0,36	0,58
Minimi=epätietoisuus	0	0	0	0	0
Maksimi=tietoisuus	1	1	1	1	1

Taulukko 4: Tietämykseen liittyvien monivalintakysymysten analyysi

Korkein tietoisuudentaso eli 0,92 saavutettiin kysymyksessä 29, jossa vastaajalta kysyttiin mitä tulisi tehdä haittojen minimoimiseksi, jos on joutunut tietojenkalatelun uhriksi. Vain kolme vastaajista vastasi kyseiseen monivalintakysymykseen väärin ja 36 vastaajista antoi kysymykseen oikean vastauksen. Kysymyksessä 30 vastaajilta kysyttiin, että mitä heidän tulisi tehdä ensimmäisenä, jos he epäilevät haittaohjelmatartuntaa. Kysymyksen tietoisuuden arvoksi saatiin 0,41, eli yli puolet vastaajista vastasi väittämään väärin. Seuraavassa kysymyksessä kysyttiin parasta tapaa suojautua haittaohjelmilta/kiristysohjelmilta ja tietoisuuden arvoksi saatiin 0,62. Näin ollen yli puolet kysymykseen vastanneista valitsi oikean vastausvaihtoehdon kysymykseen. Viimeisessä tietoisuutta mittaavassa monivalintakysymyksessä käsiteltiin yleisintä tapaa saada virustartunta tietokoneeseen. Tietoisuuden arvoksi saatiin 0,36, joka on alhaisin lukema, jota kyseisissä mittauksissa saatiin. 25 vastaajaa valitsi väärän vastauksen kyseisessä monivalintakysymyksessä.

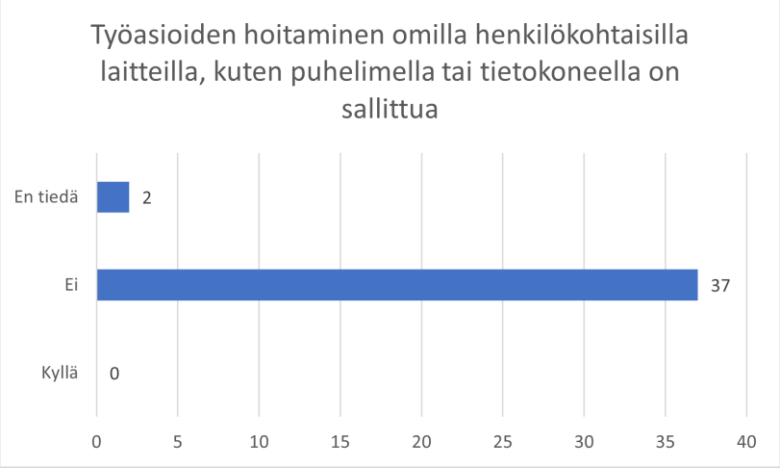
Alla olevaan taulukkoon on koottu tietoisuuden arvot kokonaisuudessaan kysymysten 24–32 osalta ja listattu tulokset funktio kohtaisesti. Tietoisuuden keskiarvo maksimissaan voi olla 1 ja minimissään 0. Kuten taulukon 5 tuloksista voimme havaita funktioiden tulokset ovat suhteellisen tasaisia ja tietoisuus kokonaisuudessaan sekä funktio tasolla että koko organisaatio tasolla on melko korkea. Jokaisessa funktiossa tietoisuuden taso on yli 0,60, mikä tarkoittaa sitä, että yli puolet vastauksista on mennyt keskiarvollisesti oikein. Korkein tietoisuuden keskiarvo, joka oli 0,75, saavutettiin tukifunktiossa sekä muut yksikössä. Vastauksista täytyy kuitenkin huomioida, että ”muut” yksikössä oli vain yksi vastaaja. Matalin tietoisuus vastausten perusteella on rekrytoinnissa, jonka tietoisuuden tasoksi tuli 0,68. Tulosten perusteella koko organisaation tietoisuuden taso kysymysten 24–32 perusteella on 0,72.

Yksikkö	Vastaukset (kpl)	Tietoisuuden taso (keskiarvo %)
Rekrytointi	13	0,68
Tukifunktio	11	0,75
Myynti	14	0,69
Muu	1	0,75
Total	39	0,72

Taulukko 5: Tietoisuus yksiköittäin ja kokonaisuudessaan

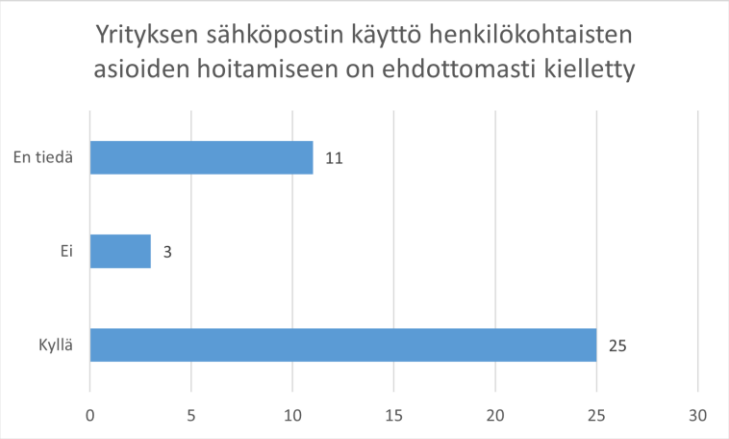
Viimeiset kolme kysymystä kyselyn tietoisuus osioissa olivat monivalintakysymyksiä liittyen yrityksen X tietoturvakäytäntöihin. Vastausvaihtoja oli kolme, jotka olivat: ”kyllä, ei, en tiedä”. Vastausvaihtoehdot ovat valittu niin, että vastausten perusteella voidaan analysoida, onko kyse tiedosta vai onko työntekijä tietämätön väitteen vastauksesta. Kyseisiin kysymyksiin liittyvät vastaukset löytyvät yrityksen turvallisuusohjeista, jotka ovat kaikkien työntekijöiden saatavilla.

Kysymyksessä 33 selvitettiin, onko omien henkilökohtaisten laitteiden käyttö työhön liittyvien luottamuksellisten tietojen lähettämiseen tai säilytykseen sallittua. Alla olevasta kuvioista voidaan nähdä, että suurin osa kyselyyn vastanneista, eli 95 % on vastannut, että omilla laitteilla ei saisi hoitaa kyseisiä työhön liittyviä asioita. Vain kaksi vastaajaa eli 5 % on valinnut vastausvaihtoehdoksi en tiedä, eli he eivät ole olleet tietoisia mikä on oikea tapa toimia kyseisen kysymyksen suhteen. Tuloksista voimme päätellä, että suurin osa yrityksen X henkilöstöstä on tietoinen työasioiden hoitamiseen liittyvistä käytännöistä ja ymmärtävät, että henkilökohtaisia laitteita ei tulisi hyödyntää työhön liittyvien luottamuksellisten tietojen säilytykseen tai lähettämiseen.



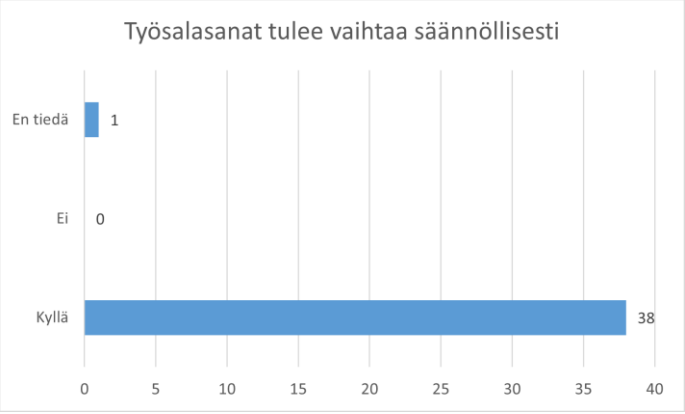
Kuvio 24: Henkilökohtaisten laitteiden käyttö työn hoitamiseen

Seuraavassa kysymyksessä (kuvio 27) selvitettiin, tietävätkö yrityksen X työntekijät onko yrityksen sähköpostin käyttö omien henkilökohtaisten asioiden hoitamiseen kielletty. Vastaajista 25 vastasi kyllä eli sähköpostin käyttö omien asioiden hoitoon on kielletty. 11 vastaajista vastasi ”en tiedä” eli he eivät olleet tietoisia mikä on yrityksen ohje kyseiseen toimintaan. Kolme vastaajista vastasi ”Ei” eli heidän mielestään työsähköpostin käyttö omien asioiden henkilökohtaisten hoitamiseen ei ole kiellettyä. Yrityksen X turvallisuusohjeistuksessa on kerrottu, että yrityksen sähköpostin käyttö omien henkilökohtaisten asioiden hoitamiseen on ehdottomasti kielletty.



Kuvio 25: yrityksen sähköpostin käyttäminen henkilökohtaisiin asioihin

Viimeisenä kysymyksenä tietoisuus osiossa kysyttiin, tuleeko työssä käytettävät salasanat vaihtaa säännöllisesti (kuvio 28).



Kuvio 26: Salasanan vaihtaminen säännöllisesti

38 vastaajaa valitsi vaihtoehdon ”kyllä, eli salasanat tulisi vaihtaa säännöllisesti. Yksi vastaaja valitsi vaihtoehdon ”en tiedä” eli vastaaja ei ollut varma yrityksen käytännöistä salasanojen vaihtamisen suhteen. Yrityksen X turvallisuusohjeistuksessa kerrotaan, että työssä käytettävät

salasanat tulisi vaihtaa säännöllisesti. Vastausten perusteella voimme siis todeta, että lähes kaikki (97 %) vastaajista ovat tietoisia yrityksen salasanojen vaihtoon liittyvistä käytännöistä.

8.5 Yleiset kysymykset

Kyselyn viimeinen osio koostui kolmesta yleisestä kysymyksestä, joista ensimmäisessä vastaajilta kysyttiin tietävätkö he keneen olla yhteydessä, jos vastaan tulee jotain epäilyttävää tietoturvaan liittyen. 30 vastaajista eli 77 % vastasi ”kyllä” eli kertoi tietävänsä kehen olla yhteydessä. Loput vastaajista eli 23 % eivät tienneet kehen ottaa yhteyttä kyseisessä tilanteessa.

Toisena yleisenä kysymyksenä kyselyyn vastaajilta kysyttiin haluavaisivatko he oppia lisää omaan työhönsä liittyvästä tietoturvasta. Vastaajista 35 eli 90 % vastasi ”kyllä” eli he olisivat halukkaita oppimaan lisää tietoturvasta. Loput 10 % vastasivat kysymykseen kielteisesti. Tuloksista voimme päätellä, että tietoturvakoulutusten toteuttaminen yrityksessä X olisi työntekijöiden mielestä tarpeellista.

8.5.1 Avoimet kommentit

Kyselyn viimeisessä kysymyksessä vastaajilla oli mahdollisuus jättää avoimia kommentteja liittyen yrityksen X tietoturvaan ja siihen liittyvään toimintaan. Avoimia kommentteja jätti kymmenen henkilöä, eli 26 % vastaajista. Toistuvia teemoja avoimen kysymyksen vastauksissa olivat epäselvyys/puutteellisuus tietoturvasta vastaavasta henkilöstä sekä tietoturvaohjeiden selventäminen. Jo aiemmin läpi käytyjen tulosten perusteella todettiin, että 36 % kyselyyn vastaajista ei tiennyt mistä yrityksen tietoturvaohjeistus löytyy ja 51 % prosenttia vastaajista ei ollut koskaan lukenut ohjetta. Yhdeksän kyselyyn vastanneista kertoi myös kysymyksessä 36, että ei tiedä keneen yrityksessä tulisi olla yhteydessä tietoturvaan liittyvissä kysymyksissä. Avoimet kommentit tukevat aiempia havaintoja, joita on tehty kyselyn muiden tulosten perusteella. Alla olevaan listaukseen on koottu kyseisten teemojen ympärille kertyneitä kommentteja.

- ”meiltä puuttuu oikea henkilö huolehtimaan turvallisuusasioista”
- ” Ei ole selvää linjausta, kuka näistä asioista on vastuussa, ja se on erittäin huolestuttavaa”.
- ” Kuka on yhteyshenkilömme tietoturvaan liittyen ja kuka vastaa tietosuojaohjelmistoista ja niiden käytöstä?
- ” Tietoturvapolitiikasta ja -ohjeista tulisi tiedottaa selkeämmin ja meillä pitäisi olla jonkinlaista turvallisuuteen liittyvää koulutusta”
- ”Tietoturvaohjeet tulee selventää työntekijöille”

- ”mistä voin lukea yrityksemme virallisen tietosuojaohjeistuksen?”

Muita aiheita, joita avoimissa kommenteissa nousi ilmi, oli tietämättömyys yrityksen tietoturvaohjelmistoista ja omista velvollisuuksista tietoturvaan liittyen. Alla kootusti muita avoimia kommentteja.

- ”En tiedä onko tietokoneessani virustorjuntaohjelmistoa, päivittyykö se automaattisesti, päivittääkö yritys sen automaattisesti kaikille jne. Tiedän, että koneellani on olemassa erittäin ärsyttävä McAfee-ohjelma, joka mainostaa joka tilauksen uusintaa. (se on tullut kannettavan tietokoneen mukana, mutta ymmärtääkseni emme käytä sitä?). Pidän kyberuhkaa erittäin merkittävänä, erityisesti sen vuoksi, mitä se voi vaikuttaa yrityksen maineeseen.”
- ” Mielestäni meidän työpaikallamme on varsin hyvä tietoturva, sitä voisi toki optimoida hankkimalla yritykselle kyberturvaohjelmiston ehkä F-Securen tai vastaavan.”
- ”Täyttäessäni tätä kyselyä ymmärsin, kuinka vähän minulla on tietoa tästä aiheesta”

9 Johtopäätökset

Tämän opinnäytetyön tavoitteena oli kartoittaa kohdeorganisaation, eli yrityksen X tietoturvatietoisuudentasoa ja siihen liittyviä tekijöitä sekä esittää tutkimuksen perusteella kehitysideoita tietoturvatietoisuuden kehittämiseksi ja ylläpitämiseksi. Vastaus tutkimuskysymykseen selvitettiin kyselylomakkeen avulla, joka lähetettiin kohdennetusti koko yrityksen X Suomen henkilöstölle. Kyselyssä tutkittiin tietoturvatietoisuuden tasoa ja siihen vaikuttavia osa-alueita, joita ovat tietoisuus, käyttäytyminen, ja asenteet.

9.1 Johtopäätökset kyselyn tuloksista

Tutkimuksessa analysoitavia alueita olivat tietous, asenteet ja käyttäytyminen sekä yrityksen tietoturvaohjeistuksiin ja politikkaan liittyvät tekijät. Osa-alueita tutkittiin kokonaisuutena kaikkien vastaajien vastauksia hyödyntäen sekä joitakin osa-alueita analysointiin taustatietojen perusteella jaetuissa ryhmissä.

Opinnäytetyön tutkimuksen perusteella voidaan todeta, että tietoturvatietoisuuteen ei vaikuta pelkkä tietämys tietoturvallisesta toiminnasta, vaan myös vahvasti käyttäjien omat asenteet ja käyttäytyminen tietoturvaan liittyen. Tulosten perusteella yrityksessä X tietoisuuden taso on suhteellisen korkea eli työntekijät tietävät melko hyvin, miten tulisi toimia tiedon kannalta turvallisesti. Asenteisiin ja käyttäytymiseen liittyvässä toiminnassa on kyselyn mu-

kaan kuitenkin puutteita ja tämä voi alentaa kohdeyrityksen tietoturvallisuutta. Tietoturva ei tarkoita pelkästään teknisten ratkaisujen ja toimintojen turvallisuutta, vaan turvallisuuden toteutumiseen vaikuttaa suuresti myös henkilöstön toiminta ja käyttäytyminen suhteessa työn tekoon. (VAHTI 2/2004, 15–16).

Eniten tietoturvallisuuteen liittyviä puutteita havaittiin henkilöstön päivittäisessä käyttäytymisessä ja tavoissa toimia turvallisesti. Tämän työn tutkimuksen mukaan 44 % kyselyyn vastanneista jättää tietokoneensa lukitsematta vaikka poistuisi itse paikalta, 36 % jättää käyttämättä monivaiheista tunnistautumista ohjelmistoihin kirjautuessa, vaikka se olisi mahdollista, sekä 67 % on hoitanut työasioita omalla henkilökohtaisella puhelimella tai tietokoneella. Myös 38 % vastaajista kertoi käyttävänsä samoja salasanoja niin töissä kuin vapaa-ajallakin. Näiden vastausten perusteella voimme todeta, että työntekijöiden toimet arjessa saattavat alentaa työpaikan tietoturvallisuutta ja lisätä riskiä tietojen joutumisesta väärien henkilön käsiin. Suurin heikkous yrityksen tietoturvassa piileekin tavanomaisesti työntekijöissä ja heidän käyttäytymisessään itsessään. (Hadlington ym. 2019, 41–48.) Luottamuksellisuus on yksi tietoturvan osatekijöistä, joka tarkoittaa, että suojattavat tiedot tulisi olla saatavilla vain niihin oikeutetuilla henkilöillä (Ruohonen 2002, 2–3). Tietomurroilta voidaan suojautua esimerkiksi monivaiheisen tunnistautumisen, tietokoneen säännöllisen päivittämisen sekä vahvojen ja uniikkien salasanojen avulla. (Traficom 2021). Nämä tiedot vahvistavat havaintoa, että turvallisilla toimintatavoilla ja käyttäytymisellä on vaikutusta tietoturvan toteutumiseen ja tietoisuuden merkitykseen yrityksessä X.

Myös yrityksen tietoturvaohjeistukseen ja politiikkaan perehtyminen sekä oma relevantti tietoturva osaaminen koettiin tutkimuksen tulosten perusteella puutteellisiksi. Kyselyn vastaajista 64 % tiesi mistä yrityksen tietoturvaohjeistus ja politiikka löytyy, mutta kuitenkin jopa 51 % ilmoitti, että ei ole lukenut kyseistä dokumenttia. Tämä tulos tukee päätelmää, jonka mukaan käyttäytyminen ja asenteet voivat mahdollistaa negatiivisen vaikutuksen tietoturvan toteutumiseen. IBM:n tuottaman tutkimuksen tulosten mukaan (2021, 2–3) erityisesti loppukäyttäjien välinpitämättömyys yhdistettynä digitaaliseen kehitykseen edistää tietovarkauksien ja kiristyshaittaohjelmien toteutumista niin yksityiselämässä kuin työpaikallakin. Tietoturvatietoisuuden yksi tärkeimmistä osatekijöistä on organisaation tietoturvapolitiikan ja käytänteiden ymmärtäminen, jotta voidaan toimia turvallisesti ja asetettujen ohjeiden mukaisesti. Näin työntekijän on myöskin mahdollista sitoutua periaatteisiin ja toteuttaa ohjeita omassa päivittäisessä toiminnassaan (Hadlington ym. 2019, 41–48.) Myös Gardnerin ja Thomaksen mukaan (2014,1) tietoturvatietoisuus tarkoittaa ymmärrystä käytännöistä ja toimintatavoista organisaatiossa kuten muun muassa tietokoneen käyttökäytännöt, internetin käyttökäytännöt sekä sähköpostiin ja salasanoihin liittyvät käytännöt, joiden avulla pyritään suojaamaan organisaation salattavia ja arkaluontoisia tietoja.

Heroldin (2010, 9–10) mukaan yrityksen tulisi tarjota työntekijöilleen koulutusta ja tietoisuuden vahvistamista edistäviä toimia varmistaakseen, että kaikki organisaation toimet ovat tietosuojakäytäntöjen sekä paikallisten lakien ja määräysten mukaisia. Henkilöstön tulee myös pystyä sisällyttämään periaatteet päivittäisiin työtehtäviinsä. 46 % kyselyyn vastanneista työntekijöistä olivat eri mieltä siitä, että he olisivat saaneet tarpeeksi kattavan tietoturvakoulutuksen työtänsä varten. Kyselyn tulosten mukaan myös 90 % vastaajista olisivat halukkaita oppimaan lisää työhön liittyvästä relevantista tietoturvasta. Näiden kyseisten tulosten perusteella voimme todeta, että tietoturvaan liittyvien asioiden kouluttaminen on tärkeää työntekijöille, ja kohdeorganisaation työntekijät olisivat halukkaita kehittämään osaamistaan tietoturvan saralla. Huolimatta siitä, että melkein puolet kyselylyyn vastanneista koki tietoturvakoulutuksen puutteelliseksi, jopa 59 % kyselyyn vastanneista on kuitenkin sitä mieltä, että omaa riittävät taidot tietoturvasta omaa työtänsä varten. Nämä tulokset voivat kertoa siitä, että työntekijöillä on relevanttia tietoa aiheesta omien opintojen, aikaisempien työkokemusten tai muun kokemuksen kautta tai voidaan myös otaksua, että työntekijöillä ei ole tarkkaa tietoa mikä on heille tarpeellinen ja riittävä tietoturvakoulutus.

Tietoisuus osiossa suurimmat kehityskohteet kyselyn perusteella löydettiin tietoisuudesta virusten ja haittaohjelmien leviäimiseen ja ennaltaehkäisyyn liittyen sekä mahdollisiin toimiin haittaohjelman iskiessä. Haittaohjelmat ja tietojenkalastelu ovat yleisimpiä tietoturvaan liittyviä riskejä organisaatioille ja näin ollen kyseisten aihealueiden perusymmärrys ja mahdollisten vaikutuksen käsittäminen olisi erittäin oleellista organisaation X tietoturvatietoisuuden kannalta. Toisaalta näitä vastaustuloksia voi selittää mahdolliset puutteet yrityksen tietoturvakoulutuksissa.

Suurimmaksi vahvuudeksi osoittautui kyselyn tietoisuus osio, jossa kysymykset perustuivat tietoon liittyviin tekijöihin. Kokonaisuudessa tulosten perusteella kohdeorganisaation tietoisuuden tasoksi saatiin 0,72 kun tuloksia käsiteltiin numeerisesti niin, että luku nolla edusti epätietoisuutta eli väärää vastausta ja luku 1 tietoisuutta eli oikeaa vastausta. Hyvä keskiarvollinen tietoisuuden taso viestii työntekijöiden ymmärryksestä tietoturvaan liittyen. Tulosten perusteella suurimmaksi vahvuudeksi nousi suojattavien tietojen tunnistaminen sekä käsitys siitä, miten suojattavaa tietoa tulisi käsitellä. Tietojen suojaamista sekä suojattavan tiedon käsittelyä säätää EU:n asettama yleinen tietosuoja-asetus (2016/679) sekä tietosuojalaki (1050/2018) joka täsmentää henkilötietojen käsittelyyn liittyvää toimintaa. Laaksosen, ym. (2006, 18.) mukaan onkin erittäin olennaista, että organisaatiossa kaikki ovat tietoisia noudatettavista laeista ja niiden täyttämisestä käytännön työssä.

Tämän havaitun korkean tietoisuuden vaikutusta tietoturvan toteutumiseen saattaa kuitenkin alentaa aiheeseen liittyvä käyttäytyminen ja asenteet suojattavaa tietoa kohtaan. Vaikka 95 % vastaajista kertoi tunnistavansa suojattavat tiedot ja 90 % vastaajista ilmaisi tietävänsä miten suojattavaa tietoa tulee käsitellä työskenneltäessä, silti suuri osa vastaajista on toimi-

nut omassa työssä päin vastaisesti. Esimerkiksi 54 % kertoi säilyttäneensä arkaluontoista salattavaa tietoa omalla työpöydällään ja 67 % vastaajista kertoi lähettäneensä arkaluontoista työ liitännäistä tietoa sähköpostin välityksellä.

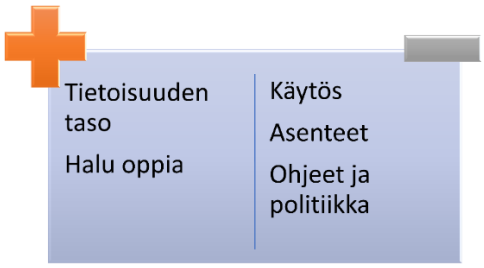
Funktio kohtaiset tulokset tutkimuksesta osoittavat, että työntekijän työskentelyfunktio saattaa vaikuttaa merkittävästi esimerkiksi työntekijän tietouteen yrityksen tietoturvaohjeista ja politiikasta sekä näiden ohjeiden perehtymiseen ja lukemiseen. Esimerkiksi tulosten mukaan vain 21 % myynnissä työskentelevistä ei ollut lukenut yrityksen tietoturvaohjeita ja tietoturvapolitiikkaa, kun taas rekrytoinnissa tämä luku oli jopa 46 % ja tukifunktiossa 36 %. Nämä tulokset osoittavat, että funktioiden välillä voi ilmetä eroavaisuuksia perehdytyksissä tai esimerkiksi tiimien sisällä valitsevissa asenteissa tietoturva-asioita kohtaan. Tietoturvatietoisuuden taso keskiarvollisesti oli suhteellisen korkea kaikissa funktioissa (taulukko 5), mutta pientä eroa funktioiden välillä kuitenkin voidaan havaita. Rekrytoinnissa keskiarvo oli kaikista alhaisin eli 0,68 ja tukifunktioissa sekä ”muu” funktioissa korkein, eli 0,75. Tästä voimme myös päätellä, että tietoturvaan liittyvä perehdytys ja tietoturvaohjeisiin ja politiikkaan perehtyminen saattaa vaihdella funktio tai tiimi kohtaisesti. Myös tiimeissä vallitseva tietokulttuuri voi olla yksi vaikuttava osatekijä tiimien välisiin eroihin käyttäytymisen sekä asenteiden osalta.

Huolimatta siitä, että tutkimuksen mukaan kokonaisuudessaan tietoisuuden taso yrityksessä on suhteellisen korkea, suurin osa yrityksen työntekijöistä vastasi kyselyssä, että ei ole saanut yritykseltä riittävää koulutusta tietoturvaan liittyen. Funktioiden väliset erot näkyvät myös näissä tuloksissa. Myynnissä 38 %, rekrytoinnissa 46 % ja tukifunktiossa 64 % vastasi, että ole mielestään saanut riittävää tietoturvakoulutusta yrityksessä. Näihin tuloksiin voi vaikuttaa funktiokohtaiset erot koulutusten tarpeellisuudesta sekä mahdollinen perehdytys ja koulutusohjelman eroavaisuus funktioiden kesken. Myös työtehtävien eriäväisyydet ja tietoturvaaliittyvien tietojen taitojen ja tietojen käyttö päivittäisessä työelämässä voi olla hyvinkin erilaista. Jokaisella työntekijällä tulee olla mahdollisuus oman työnkuvan kannalta merkittävään ja välttämättömään tietoturvakoulutukseen. Työn kuvan tai ympäristön muuttumisen myötä on myös erityisen tärkeää muistaa osaamisen ja tietoisuuden kehittäminen. (ISO/IEC 27001.)

9.2 Yhteenveto johtopäätöksistä

Yhteenvetona tulosten johtopäätöksistä voidaan todeta, että yrityksen X tietoturvatietoisuus tämän kyselyn perusteella on tyydyttävällä tasolla. Kyselyn perusteella työntekijöiltä löytyy ymmärrystä ja tietoa tietoturvan osa-alueisiin liittyvistä aiheista, mutta tietoturvan tasoa yrityksessä selkeästi alentaa työntekijöiden toiminta ja mahdolliset asenteet oman käytöksen takana. Käyttäytymisen ja asenteiden kannalta oleellisimmat puutteet olivat tiedon suojaamiseen liittyvät käytännöt sekä turvallisuusohjeisiin ja politikkaan perehtyminen.

Alla olevaan kuvioon (kuvio 31) on tiivistetty yrityksen X tietoturvatietoisuuden positiiviset tekijät sekä negatiivisesti vaikuttavat tekijät tämän tutkimuksen perusteella. Yrityksessä positiivisesti tietoturvatietoisuuteen vaikuttavia ominaisuuksia tulosten perusteella oli tietoturvaan liittyvän tietämyksen taso sekä halu oppia lisää kyseisestä aihealueesta. Suurimmat kehityskohteet olivat taas tietoturvaan liittyvät asenteet ja käyttäytyminen.



Kuvio 27: Yhteenveto tietoturvatietoisuudesta yrityksessä X

Koulutusten ja oman relevantin tietoturva osaamisen nähdään tulosten perusteella olevan puutteellista mikä voi vaikuttaa kokonaisuudessaan yrityksessä vallitsevaan tietoturvakulttuuriin. Myös henkilöstön asenteet ja käyttäytyminen nostaa huomattavasti tietoturvaan liittyvä riskejä, ja henkilöstö ei välttämättä itse ymmärrä tai tiedosta oman toiminnan vaikutuksia tietoturvaan ilman relevantteja koulutuksia ja perehdytyksiä. Henkilöstön kiinnostus tietoturvaan liittyen sekä vallitsevan tietoturvakulttuurin tuomat asenteet ovat asioita joihin yrityksen tulisi tulevaisuudessa kiinnittää huomioita tietoturvatietoisuuden parantamiseksi entisestään.

9.3 Kehitysideat

Tämän opinnäytetyön tutkimusten tulosten perusteella voidaan esittää konkreettisia kehitysideoita kohdeorganisaatiolle X tietoturvatietoisuuden kehittämiseksi ja ylläpitämiseksi sekä selkeyttää nykyinen tietoturvatietoisuuden taso ja siihen liittyvät pääasialliset tekijät.

Yrityksen X tietoturvatietoisuuden kehittämiseksi ja ylläpitämiseksi tehtiin kirjallinen dokumentti taulukko muodossa. Dokumentti sisältää toimenpiteet, kuvauksen, aikataulun, sekä mahdolliset vastuujaot. Dokumentti on tarkoitettu hyödynnettäväksi vuosittaisella tasolla ja tarkemmat vastuut ja toimenpiteiden päivittäminen tulisi tehdä jokaisen vuoden päättyessä, sekä mahdollisen muiden muuttujien vaikutuksesta ohjeen toteutumiseen ja toimintaan. Pääasiallisina toimenpiteinä dokumentissa on esitelty yrityksen X tietoturvatietoisuuden tason nostamiseksi ja ylläpitämiseksi kuusi toimenpidettä, joiden avulla tietoturvatietoisuutta voidaan kehittää. Kehityskohteet ovat, tietoturvapolitiikka sekä ohjeistus, tietoturvatietoisuus intranetissä, henkilöstön kouluttaminen, uuden työntekijän perehdyttäminen, tietoturvalli-

suuden kartoittaminen sekä jatkuva kehittäminen. Toimenpiteiden jatkuvuus ja prosessinomainen toiminta on tärkeä osa kehittämistä ja se toimii myös tämän työn kehityssuunnitelman pohjana.

Ensimmäisenä toimenpiteenä kohdeorganisaation tulisi päivittää yrityksen tietoturvapolitiikka sekä tietoturvaohjeistus ja varmistaa että kyseiset dokumentit ovat ajan tasalla ja tarpeeksi kattavat. Näiden dokumenttien tulisi antaa työntekijöille selkeät s raamit ja ohjeet omalle toiminnalleen liittyen tietoturvalliseen työskentelyyn. Ohjeiden ja politiikan päivityksessä olisi hyvä keskittyä etenkin salauskäytäntöihin, luottamuksellisten tietojen säilyttämiseen ja välittämiseen sekä tietoturvaan etätyössä. Dokumentin tulisi sisältää selkeästi myös vastuunjaot sekä roolit tietoturvaan liittyen. Politiikan taustalla ja tukemassa yrityksen omaa ohjeistusta olisi hyvä huomioida yleiset lait, ohjeet ja standardit. Yrityksen X tulisi siis ennen kaikkea myös perehtyä oman organisaation tietoturvaan liittyvien ohjeiden ja politiikan suunnitteluun. Suunnittelun apuna yritys voisi hyödyntää esimerkiksi työssä aikaisemmin mainittua ISO/IEC 27000 sarjan standardia 27001 joka sisältää vaatimuksen tietoturvan hallintajärjestelmälle kaiken kokoisissa organisaatioissa. Uuden työntekijän perehdytykseen tulisi kuulua systemaattinen turvallisuusohjeistuksen -ja politiikan läpikäynti sekä yleisellä tasolla oleva tietoturvakoulutus. Tietoturvapolitiikan sekä tietoturvaohjeistuksen perehdyttäminen toki vaatii näiden dokumenttien ja ohjeiden systemaattista ylläpitoa ja päivittämistä työnantajalta. Tarkemmat yksikkö kohtaiset koulutukset voitaisiin toteuttaa tarpeen mukaan.

Tietoturvatietoisuutta voidaan lisätä merkittävästi aiheeseen liittyvillä koulutuksilla sekä uusien työntekijöiden perehdytyksellä. Yrityksen X tulisi lisätä tietoturvakoulutukset vuosittaiseen koulutussuunnitelmaansa ja ylläpitää tietoturvaan liittyvien koulutusten toistuvuutta ja monipuolisuutta, sekä huomioida koulutusten sisällössä muuttuva toimintaympäristö sekä teknologinen kehitys. Koulutusten suunnittelu tulisi toteuttaa yhteistyössä HR:n kanssa sekä osallistaa suunnitteluun esihenkilöitä. Koulutusten suunnitellussa tulisi erityisesti huomioida tiimikohtaiset/funktiokohtaiset tarpeet sekä esihenkilöiden rooli tietoturvallisen ympäristön tukemisessa. Työnkuvien erilaisuus liittyen ohjelmistojen käyttöön sekä muuhun tietotekniseen työskentelyyn asettaa erilaisia vaatimuksia eri henkilöille, joka on erityisen tärkeää ottaa huomioon osaamisen kehittämisessä ja kouluttamisessa. Koulutusten pohjana ja sisällön suunnittelussa on hyvä muistuttaa toimintaa ohjaavasta lainsäädännöstä, kuten EU:n yleisestä tietosuoja säännöksestä sekä Suomen tietosuojalaki (1050/2018). Lait vaikuttavat yritystoimintaan vahvasti ja voivat joko asettaa epäsuoria tai suoria velvoitteita koskien tietoturvaa. Tämän vuoksi yleinen tietämys tietosuojaan liittyvistä laeista on erittäin olennaista. (Laaksonen, ym. 2006, 18.)

Vaikuttava tietoturvatietoisuutta lisäävä tekijä on aiheen esille tuonti, tiedottaminen ja vaivaton tiedon hankinta tietoturvaan liittyen. Tämän vuoksi erittäin tärkeänä lisänä yritys X:n tulisi perustaa omaan intranettiin sivusto koskien tietoturvaa. Intranetin tietoturvasivuston

tarkoitus olisi auttaa henkilöstöä löytämään aiheeseen liittyviä ohjeita ja materiaalia sekä tiedottaa tarpeellisista tietoturvaa koskevista ajankohtaisista aiheista. Intranet sivusto sisältäisi koulutusmateriaalit, hälytykset mahdollisista ajankohtaisista tietoturvauhkista sekä tietoturvasta vastaavan ja yhteydenottolomakkeen tietoturvaan liittyvissä kysymyksissä. Kehittäessä ja ylläpitäessä tietoturvatietoisuutta on hyvä panostaa muuhunkin kuin pelkkään henkilöstön kouluttamiseen. Muita hyviä tietoisuuden kehittämisen keinoja on muun muassa itseopiskelu valmiin materiaalin avulla, teema viikko liittyen tietoturvaan tai tietoturvamateriaalin lisääminen uuden työntekijän perehdytykseen. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 31.)

Viidentenä erittäin merkittävänä tietoturvatietoisuuden kehittämisen alueena toimii aiheen mittaaminen, sekä siihen liittyvät relevantit kyselyt ja kartoitukset. Tietoturvatietoisuutta sekä tietoturvallisuutta voidaan mitata monella eri tavalla ja mittauksissa voidaan käyttää vaihtelevasti erilaisia lähestymistapoja. (ENISA 2007, 1–2.) Kyselyiden ja kartoitusten toteuttamisen tulisi olla jatkuvaa ja tulosten avulla voitaisiin keskittyä yritykselle olennaisiin kehityskohteisiin. Henkilöstön vaihtuvuuden sekä muuttuvan teknologisen ympäristön vuoksi kysely tulisi toteuttaa vähintään kerran vuodessa. Kyselyn sisältö voisi olla esimerkiksi tietoturvallisuuden tasoa mittavaa internet kysely, jossa tutkittaisiin asenteita, osaamista ja käyttäytymistä. Olennaisia henkilöstön toimintaan liittyviä mittauksen kohteita ovat muun muassa salasanakäytännöt, tietämyksen taso sekä tiedon käsittely ja luokittelu. (Laaksonen ym.2006, 278–279.)

Aikataulullisesti yllä esitettyjen kehitystoimenpiteiden toteuttaminen tulisi toteuttaa vuosittain, jatkuvan prosessin omaisesti. Osa toimenpiteistä vaatii mahdollisimman nopeaa reagointia kohdeorganisaatiolta, kuten tietoturvapolitiikan -ja ohjeiden päivittäminen sekä mahdollisen yleisen tietoturvakoulutuksen suunnittelu. Jokaiselle kehitystoimenpiteelle on määritelty oma aikataulu, joka on määritelty tarkemmin liitteessä kolme. Olennaista on huomioida, että myös kehityssuunnitelmaa tulee päivittää vuosittaisella tasolla ja tehdä mahdollisia muutoksia suunnitelman toimenpiteisiin, että aikatauluihin mikäli se nähdään tarpeelliseksi.

Näiden toimenpiteiden ja kehityssuunnitelman avulla kohdeorganisaatio voi systemaattisesti kehittää oman henkilöstön tietoturvatietoisuutta sekä ymmärtää toiminnan mahdolliset heikkoudet, vahvuudet sekä kehityskohteet. Tietoisuuden kehittäminen on myös suuri osa yleistä tietoturvaosaamista, jonka parantaminen on hyödyksi organisaation riskienhallinnalle.

9.4 Validiteetti ja reliabiliteetti

Tutkimustyön luotettavuutta voidaan arvioida reliabiliteetilla sekä validiteetilla. Validiteetti tarkoittaa tutkimuksen menetelmän pätevyyttä eli sen kykyä mitata alkuperäistä tutkimus-

kohdetta. (Heinonen ym. 2013, 91–92). Oikealla tavalla valittu tiedonkeruu, kattava perusjoukon määrittely sekä mahdollisimman korkea vastausprosentti vahvistavat validin opinnäytetyön tutkimuksen onnistumista. (Heikkilä 2014, 27.)

Reliabiliteetti kuvastaa tutkimuksen tulosten totuudellisuutta ja tarkkuutta. Näin ollen mittauksen tulosten tulisi olla toistettavia sekä riippumattomia, eli esimerkiksi kahden saman aiheen tutkijan saman kaltaiset tulokset vahvistavat tutkimuksen reliabiliteetin toteamista. (Heinonen ym. 2013, 93). Heikkilän (2014, 28) mukaan on tärkeää varmistaa tutkimuksen reliabiliteettia tarkastelemalla otoskokoa ja mahdollisia vinoumia tutkittavassa perusjoukossa. Tutkittavan otoksen tulisi edustaa kaikkia tutkimuksen perusjoukkoon sidoksissa olevia ryhmiä.

Tämän opinnäytetyön vastausprosentti, joka on 48 % sekä jakauma vastaajien kesken osastoissa (kuvio 7) ja työskentelyvuosissa (kuvio 8) lisäävät tutkimuksen reliabiliteettia. Tutkimukseen kokonaisuudessaan vastasi 39 henkilöä 82 henkilön populaatiosta. Vilkan (2007, 151–152) mukaan tutkimuksen luotettavuutta lisää se, miten otos kuvaa tutkimuksen perusjoukkoa. Pieni hajonta vastaajien ikäryhmissä vahvistaa tutkimuksen luotettavuutta. Tutkittava joukko edustaa realistisesti kohdeyrityksen tutkimuksen kohteena olevaa perusryhmää eli koko Suomen organisaatioita, ja näin ollen voidaan todeta, että vastaukset ovat puolueettomia ja antavat kuvan tietoturvatietoisuudesta organisaation jokaisella tasolla.

Tutkimuksen tulokset ovat myös hyvin loogisia, kun tarkastellaan yrityksen lähtötilannetta ja toimenpiteitä turvallisuuteen liittyen. Moni vastaajista koki epätietoisuutta liittyen yrityksen turvallisuusohjeisiin ja käytäntöihin sekä toivoi lisää koulutusta tietoturvaan liittyen. Nämä vastaukset heijastuvat siitä, että yrityksestä puuttuu puhtaasti tietoturvallisuuteen liittyvät koulutukset ja perehdytykset ja tietoturvaohjeiden -ja politiikan lukeminen on työntekijän omalla vastuulla. Loogiset tulokset lisäävät tämän tutkimuksen reliabiliteettia.

Tutkimustyön menetelmänä käytetty kyselylomake toimi hyvin tutkimaan kyseistä aihealuetta ja tutkimuksesta saadut vastaukset olivat tarkoituksenmukaisia. Kyselyn avoimen kysymyksen vastaukset vahvistivat myös monivalintakysymysten sekä väittämien tuloksia. Validiteettia tutkimuksessa vahvistettiin myös kyselylomakkeen huolellisella testauksella sekä kohdeorganisaatiossa että sen ulkopuolella. Testauksen avulla pyrittiin selvittämään, että kyselyn kysymykset ovat helposti ymmärrettävissä ja vastaus kysymyksiin on vaivatonta. Työn ulkopuolisten, kuten kollegoiden tai ohjaajien kommentit ovat relevantteja, jos halutaan nostaa tutkimuksen luotettavuutta ja minimoida mahdolliset virheet. (Vilkka 2007, 153).

Työn tulosten esittelyssä on hyödynnetty suoria lainauksia avoimen kysymyksen vastausten osalta, jotka vahvistavat muita työssä saatuja tuloksia. Kohdeyrityksessä ei ole aikaisemmin tehty samankaltaista tutkimusta, joten tuloksia ei voida arvioida suhteessa aikaisempiin tuloksiin. Opinnäytetyön tutkimus on tehty työelämälähtöisesti ja tutkimuksessa on vahvasti

huomioitu kohdeorganisaation lähtötilanne, tausta tietoturvasta sekä kyselyn kysymyksiin vaikuttavat tekijät työntekijöiden päivittäisissä työtehtävissä. Näin ollen tutkimuksen tulokset sekä johtopäätökset antavat ajankohtaista ja relevanttia tietoa yrityksen tietoturvatietoisuudesta, joka vahvistaa tulosten ja kehityssuunnitelman käyttökelpoisuutta kohdeorganisaatioissa.

9.5 Työn eettisyys

Tämän opinnäytetyön tutkimus toteutettiin noudattamalla eettistä työskentelytapaa ja periaatteita. Tutkimus toteutettiin anonyymisti ja kaikilla vastaajilla oli mahdollisuus itse päättää tutkimukseen osallistumisesta. Tutkimuksen saatekirjeessä tuotiin ilmi osallistumisen vapaaehtoisuus sekä tutkimuksen tavoite ja tarkoitus. Tutkimukseen osallistuvilta kerättiin vain tarpeellisia taustatietoja tutkimuksen onnistumisen kannalta ja tutkimuksen tulokset esitettiin kunnioittavasti ja neutraalisti. Tutkimuksen eettisyyttä vahvistaa luottamuksellisuus ja tutkimukseen osallistuneille luvattu anonyymiys. (Vilkka 2007, 164).

Tutkimuksen eettisyyteen kuuluu tutkimuksen rehellisyys ja tarkkuus ainestoa käsiteltäessä. Myös suunnitelmallisuus, toteutus ja raportointi tulee tehdä tieteellistä näkökulmaa kunnioittaen. (Tutkimuseettinen neuvottelukunta 2012, 6.) Tutkimuksen tulokset ovat esitetty rehellisesti ja niiden analysointi on tehty tarkasti. Kyselytutkimuksen tuloksena kerättyä aineistoa käsiteltiin huolellisesti ja tutkimuksen tuloksia esittäessä on pidetty huoli tutkimukseen osallistuneiden tunnistautumattomuudesta.

Opinnäytetyön lähdeviitteet on tehty asiallisesti sekä mahdollisimman tarkasti ja viitemerkinnöissä on ilmoitettu riittävät lähdetiedot. Vilkan (2007, 165) mukaan hyvään tieteelliseen tapaan toimia kuuluu pätevien lähteiden käyttö, lähdeviitteiden tarkka merkitseminen sekä lähteiden kunnioittaminen.

9.6 Työn arviointi

Opinnäytetyön tekeminen oli erittäin mielenkiintoinen mutta haastava prosessi. Työn aihe oli tarpeellinen kohdeorganisaatiolle ja tietoturvatietoisuus yleisesti on erittäin tärkeä ja pinnalla oleva aihe nykypäivänä. Työ eteni lähes suunnitellusti prosessimaista etenemistä noudattaen, vaikka aikataulu muuttuikin työn edetessä. Opinnäytetyön tavoitteet täyttyivät sekä esitettyyn tutkimuskysymykseen saatiin kattava vastaus. Tutkimuksen tekemisestä mieleistä teki aiheen tärkeys sekä mahdollisuus hyödyntää tutkimustuloksia kohdeorganisaation tietoturvan ja siihen liittyvän tietoisuuden kehityksessä.

Työn viitekehyksen rakentaminen oli prosessin työläin osuus ja se vaatii syvällistä aiheen kirjallisuuteen perehtymistä ja työn kannalta relevantin tiedon etsimistä. Työssä pyrittiin hyödyntämään mahdollisimman tasokasta sekä kansainvälistä lähdeainestoa monipuolisia kanavia

hyödyntäen. Viitekehykseen valittiin aineistoa, joka antaisi lukijalleen mahdollisimman kattavan kuvan tietoturvasta kokonaisuudessa sekä tietoturvatietoisuudesta ja sen mittaamisesta sekä kehittämisestä. Viitekehyksen avulla tutkimusta voidaan hyödyntää myös muissa organisaatioissa.

Työn tutkimuksessa käytetty sähköinen kysely oli onnistunut ja vastauksia kyselyn avulla saatiin kiitettävästi. Positiivista oli, että kyselyssä saatiin avoimia kommentteja ja vastaajilla vaikutti olevan mielenkiintoa aihetta kohtaan. Kyselystä suullisesti saatu palaute oli myönteistä ja kysely herätti keskustelua työn aiheesta kohdeorganisaatiossa.

Opinnäytetyön tulokset analysoitiin selkeästi kyselyn osioita hyödyntäen ja analysoinnissa hyödynnettiin työssä esiteltyä viitekehystä. Analysoinnissa käytettiin apuna erilaisia tunnuslukuja, taulukoita sekä kaavioita, joiden avulla lukijan on helpompi hahmottaa kyselyn tuloksia ja siitä syntyneitä johtopäätöksiä. Työn avulla syntyneet johtopäätökset sekä kehitysideat olivat selkeitä sekä realistisia ja näiden kehitysideoiden avulla kohdeorganisaation on helpompi lähteä kehittämään yrityksen tietoturvallista toimintaa. Tutkimuksen avulla kohdeorganisaation on myös helpompi tutkia jatkossa tietoturvatietoisuuden kehitystä ja asettaa tavoitteita kyseisen aihealueen tiimoilta koko organisaatiolle. Kaiken kaikkiaan työ oli selkeästi ja tavoitteiden mukaisesti toteutettu ja prosessi oli onnistunut. Työn voidaan sanoa täyttäneen sekä työn tekijän, että kohdeorganisaation odotukset.

Opinnäytetyön tuloksia voidaan hyödyntää kohdeorganisaation tietoturvasuunnittelussa sekä työn kyselylomaketta ja tutkimustapaa myös muissa samalla toimialalla toimivissa tai samankaltaisissa organisaatioissa. Työn tutkimusmenetelmä pohjautuu kattavaan tietoturvan viitekehykseen joka mahdollistaa tutkimusmenetelmän hyödynnettävyyden muissa organisaatioissa tietoturvatietoisuuden tason selvittämiseksi. Tutkimuksen tulosten peruusteella rakennettua kehityssuunnitelmaa voidaan käyttää myös muissa organisaatioissa, mikäli halutaan keskittyä samoihin teemoihin vahvistaakseen yrityksen tietoiturvatietoisuutta ja sen ylläpitämistä.

Lähteet

Painetut

Andreasson, A. Riikonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma.

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

Ciampa, M. 2015. Security Awareness: Applying practical security in your world. Cengage Learning.

Hakala, M. Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Heikkilä, T. 2014. Tilastollinen tutkimus. 9. painos. Porvoo: Bookwell.

Heinonen, J. Keinänen, K. & Paasonen, J. 2013. Turvallisuustutkimuksen tekeminen. Helsinki: Tietosanoma Oy.

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas: Tunnista uhat, hallitse riskit. Helsinki: Alma Talent.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja: Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOY-pro

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo.

Vilkka, H. 2007. Tutki ja mittaa: määrällisen tutkimuksen perusteet. Helsinki: Tammi.

Sähköiset

Alshaikh, M., Maynard, S. Ahmad, A., & Chang, S. 2018. An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations. 51st HI International-Conference on System Sciences, HICSS, pp. 5085-5094.

Chopra, A, & Chaudhary, M. 2019. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. E-kirja. Berkeley: Apress L. P.

Digiturvallisuuden käytännön vinkit. 2021. Viitattu 3.5.2022. https://dvv.fi/documents/16079645/0/VHK_Digiturvallisuuden_k%C3%A4yt%C3%A4nn%C3%B6n_vinkit_0112_2021.pdf/0e475a77-0f54-4c54-df4e-5cda8b621ffb/VHK_Digiturvallisuuden_k%C3%A4yt%C3%A4nn%C3%B6n_vinkit_0112_2021.pdf?t=1645524044106

ENISA 2007. Information security awareness initiatives: Current practice and the measurement of success. Viitattu 3.5.2022. https://ifap.ru/library/book206.pdf

EN ISO/IEC 27001. 2017. Viittaaminen sähköisiin dokumentteihin tai niiden osiin. Helsinki: Suomen Standardoimisliitto.

Fowler, K 2016, Data Breach Preparation and Response: Breaches Are Certain, Impact Is Not. E-kirja. Rockland, MA: Elsevier Science & Technology Books.

Gardner, B, & Thomas, V. 2014. Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats. E-kirja. Rockland, MA: Elsevier Science & Technology Books.

Haarni, T. 2019. Tietoturvallisuuden hallintajärjestelmä. Viitattu 3.5.2022. https://www.slideshare.net/SuomenStandardisoimisliitto/tietoturvallisuuden-hallintajrjestelm-tuukka-haarni.

Hadnagy, C, & Fincher, M .2015. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. E-kirja. Somerset: John Wiley & Sons.

Hadlington, L., Popovac, M., Janicke, H. & Yevseyeva, I & Jones, K. 2019. Exploring the role of work identity and work locus of control in information security awareness, Computers & Security. Volume 81,2019, 41–48. Viitattu 3.5.2021. https://doi.org/10.1016/j.cose.2018.10.006

Herold, R. 2010. Managing an Information Security and Privacy Awareness and Training Program. E-kirja. Baton Rouge: Taylor & Francis Group.

Renfrow, H, & Death, D. 2017. Information Security Handbook: Develop a threat model and incident response strategy to build a strong information security framework. E-kirja. Birmingham: Packt Publishing.

Johansson, M. 2003. BS 7799, Tietoturvan hallinta. Viitattu 3.5.2022. https://www.cs.helsinki.fi/group/turvasem/papers/johansson_bs7799.pdf

Katakri 2020. Kansallinen turvallisuusviranomainen. Viitattu 17.5.2022. https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Laki sähköisen viestinnän palveluista 917/2004. Viitattu 3.5.2022. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Laki yksityisyyden suojasta työelämässä 759/2004. Viitattu 3.5.2022. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759?search%5Btype%5D=pika&search%5Bpika%5D=Laki%20yksityisyyden%20suojasta%20ty%C3%B6el%C3%A4m%C3%A4ss%C3%A4

Limnéll, J. 2021. Tietoturva on mahdollistaja. Viitattu 3.5.2022. https://www.aidon.com/fi/tietoturva-on-mahdollistaja/

Luottamuksen lähteillä 2019. Traficom. Viitattu 17.5.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

McIlwraith, A. 2006. Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness. E-kirja. Abingdon: Taylor & Francis Group.

Hiltunen, L. 2022. Metodina kyselytutkimus. Viitattu 20.5.2022. http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/kyselytutkimus2.pdf

Bernik, I. & Prislan, K. 2016. Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. Viitattu 3.5.2022. https://doi.org/10.1371/journal.pone.0163050

Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. 2003. Valtiovarainministeriö. Viitattu 3.5.2022. https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_11_2006.pdf

Pidempi parempi - Näin teet hyvän salasanan. 2021. Viitattu 3.5.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Pienyritysten kyberturvallisuusopas. 2020. Viitattu 8.5.2022. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

SFS 2021. Viitattu 8.5.2022. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

Suomen perustuslaki 731/1999. Viitattu 3.5.2022. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731?search%5Btype%5D=pika&search%5Bpika%5D=perustuslaki

Tietoturvaopas henkilöstölle. Viitattu 8.5.2022. https://www.turku.fi/sites/default/files/atoms/files//henkiloston20tietoturvaopas_hyto.pdf

Tietosuojalaki 1050/2018. Viitattu 3.5.2022. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050?search%5Btype%5D=pika&search%5Bpika%5D=Tietosuojalaki

Tietoturvariskien arviointi. 2021. Viitattu 3.5.2022. https://www.tietoturvariskienarviointi.fi/

Tietoturva 2021. Viitattu 3.5.2022. https://www.tietoturva.org/tietoturvatietoisuuden-merkitys-kasvaa/

Traficom 2021. Viitattu 3.5.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Tietoturva 2021: 3 uhkaa ja 3 ratkaisua jokaiselle. 2021. Viitattu 7.12.2021. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Tee etätyöstä turvallista vinkkiemme avulla. 2020. Viitattu 3.5.2022. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tee-etatyosta-turvallista-vinkkiemme-avulla

Tutkimuseettinen neuvottelukunta. 2012. Hyvä tieteellinen käytäntö ja sen loukkausten käsitteleminen. Viitattu 7.6.2022. https://www.tenk.fi/sites/tenk.fi/files/htk_ohje_verkko14112012.pdf

Vinkkejä tietoturvalliseen etätyöhön. 2020. Viitattu 3.5.2022. https://valtori.fi/-/vinkkeja-tietoturvalliseen-etatyohon

Vasileiou, I, & Furnell, S. 2019. Cybersecurity Education for Awareness and Compliance. E-kirja. Hershey: IGI Global.

VM 22/2017 Ohje riskienhallintaan- Riskiarviointityökalu-käyttö-ja täyttöohje. Viitattu 12.11.2021. https://vm.fi/documents/10623/1898625/Riskiarviointi+ohje/fe847307-0fc9-4389-bc0c-f003a98c150f.

Wheeler, E. 2011. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. E-kirja. Saint Louis: Elsevier Science & Technology Books.

Zinatullin, L. 2016. The Psychology of Information Security: Resolving Conflicts Between Security Compliance and Human Behaviour. E-kirja. Ely: IT Governance Ltd.

Kuviot

Taulukot

Liitteet

Liite 1: Kyselylomakkeen saatekirje

Dear colleagues,

I am studying Master's degree in Safety, Security and Risk Management at Laurea and am currently working on my thesis. My thesis project aims to understand the level of information security awareness of our company.

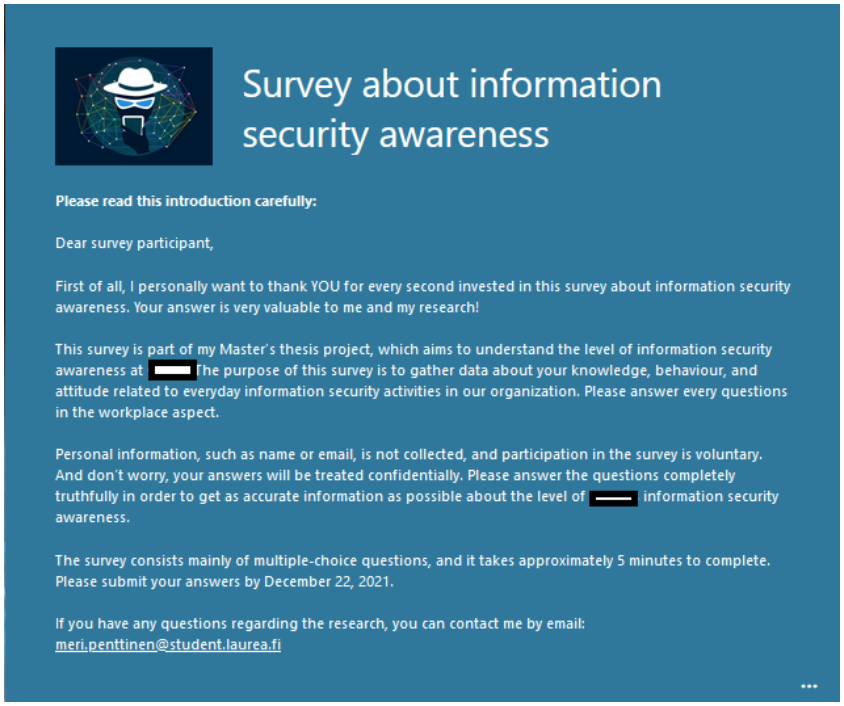
I would be really grateful if you could answer this survey regarding information security awareness - it only takes approximately 5 minutes. Please submit your answers by December 22, 2021.

You can access the survey through this link: https://forms.office.com/r/1zPQCZ9HzJ

Have a great week! 😊

Best Regards,
Meri

Liite 2: Kysely



Survey about information security awareness

Please read this introduction carefully:

Dear survey participant,

First of all, I personally want to thank YOU for every second invested in this survey about information security awareness. Your answer is very valuable to me and my research!

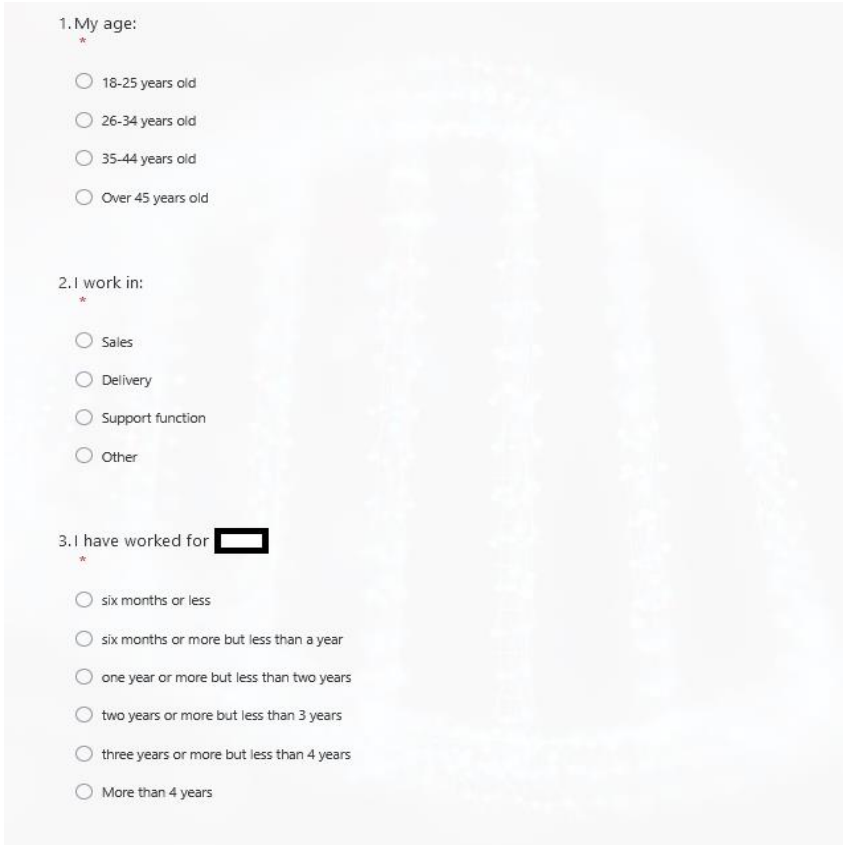
This survey is part of my Master's thesis project, which aims to understand the level of information security awareness at [redacted]. The purpose of this survey is to gather data about your knowledge, behaviour, and attitude related to everyday information security activities in our organization. Please answer every questions in the workplace aspect.

Personal information, such as name or email, is not collected, and participation in the survey is voluntary. And don't worry, your answers will be treated confidentially. Please answer the questions completely truthfully in order to get as accurate information as possible about the level of [redacted] information security awareness.

The survey consists mainly of multiple-choice questions, and it takes approximately 5 minutes to complete. Please submit your answers by December 22, 2021.

If you have any questions regarding the research, you can contact me by email:
meri.penttinen@student.laurea.fi

...



1. My age: *

- ○ 18-25 years old
- ○ 26-34 years old
- ○ 35-44 years old
- ○ Over 45 years old

2. I work in: *

- ○ Sales
- ○ Delivery
- ○ Support function
- ○ Other

3. I have worked for [redacted] *

- ○ six months or less
- ○ six months or more but less than a year
- ○ one year or more but less than two years
- ○ two years or more but less than 3 years
- ○ three years or more but less than 4 years
- ○ More than 4 years

Guidelines and policies

4. I know where to find [redacted] security guidelines and security policy *

- ○ Yes
- ○ No

5. I have carefully read the company's security guidelines and policy *

- ○ Yes
- ○ No

6. I feel that our company's security policies are easy to follow *

- ○ Strongly agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly disagree

7. I feel that I have been sufficiently trained in information security at our company *

- ○ Strongly agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly disagree

8. I feel that I have adequate knowledge about information security for my job *

- ○ Strongly agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly disagree

Behaviour & Attitude

9. I always lock my computer when I am not around *

- ○ Yes
- ○ No

10. I have shared my password with others *

- ○ Yes
- ○ No

11. If possible I always use Multi-Factor authentication *

- ○ Yes
- ○ No

12. I have taken care of work related matters on my personal phone or computer *

- ○ Yes
- ○ No

13. All my work related passwords include at least 8 characters, upper and lower case letters, symbols, and numbers *

- ○ Yes
- ○ No

14. I often use the same password for my personal accounts and for my work accounts *

- ○ Yes
- ○ No

15. I have stored confidential information on desktop *

- ○ Yes
- ○ No

16. I have accidentally forgot confidential papers on printer *

- ○ Yes
- ○ No

17. I have sent work-related sensitive/confidential information via email *

- ○ Yes
- ○ No

18. I pay attention that anti-virus updates are up to date every time I login to my computer at work *

- ○ Yes
- ○ No

19. How do you update your computer? *

- ○ It is automatically updated
- ○ I update it manually
- ○ I don't update my compter, it takes too long

Knowledge

20. Do you recognize the confidential information you should secure in your work? *

- ○ Yes
- ○ No

21. Do you know how to safely handle confidential information in your work? *

- ○ Yes
- ○ No

22. Which type of information should be handled securely? *

- ○ Contracts
- ○ Personal data
- ○ Financial records
- ○ All of the above
- ○ None of the above

23. Who in our organization is responsible for ensuring information security? *

- ○ Employees
- ○ Members of the board
- ○ Human Resources
- ○ All of the above
- ○ None of the above

24. My computer has no value to hackers, they do not target me *

- ○ True
- ○ False

25. Email authentication is a good way to protect against phishing attacks *

- ○ True
- ○ False

26. The backup files saved on computer prevent data loss in case of ransomware attack *

- ○ True
- ○ False

27. Public networks (such as restaurant or library Wi-Fi) are safe to use for confidential activities if it requires a password to access *

- ○ True
- ○ False

28. Instant messaging, for example Teams or WhatsApp, is safer to use compared regular email *

- ○ True
- ○ False

29. If you fall for a phisihing scam, what should be done to limit the harm? *

- ○ Delete the phishing email as soon as possible
- ○ Unplug the computer to get rid of any possible malwares
- ○ Change any compromised passwords immediately

30. What should you do in the first place if you suspect a malware infection? *

- ○ Turn off the computer
- ○ Turn off the computer and the internet connection
- ○ Turn off the internet connection

31. Which of the following is the best way to protect from malware or ransomware? *

- ○ Keep softwares up to date
- ○ Avoid sending emails outside the organization
- ○ Change the passwords every other week

32. What is the most common delivery for viruses? *

- Email
- Instant messaging
- Internet download

33. Is it allowed to use own personal devices, such as mobile phone, to store or transfer confidential company information? *

- Yes
- No
- I don't know

34. Any personal use of the company email is strictly prohibited *

- Yes
- No
- I don't know

35. Work passwords should be changed periodically *

- Yes
- No
- I don't know

36. Do you know who should you contact in our organization if you notice anything suspicious regarding information security? *

- Yes
- No

37. I would like to learn more about information security related to my work *

- Yes
- No

38. Do you have any other concerns or questions regarding [redacted] infomation security?

Kirjoita vastaus

Liite 3: Tietoturvatietoisuuden kehitys- ja ylläpitosuunnitelma

Actions	Description	Schedule	person in charge/responsibility
Policy and guidance	• developing a comprehensive and holistic information security policy and data protection guidelines	• Urgent need for updating • Must be updated regularly, at least every 3 years	Company management, security manager or other person in charge
Information security awareness at Intranet	• the place for security policies, principles, and guidelines • The intranet site would contain training materials, alerts about possible current security threats, as well as contact information for the person in charge of security	• Should be built as soon as possible • need for constant updating and maintenance	Security manager or other person in charge, HR
Training	• Regular training in the organization's security policies, compulsory training for all staff • Special training for specific areas of information security expertise	Annually, more often if necessary	Security manager or other person in charge, supervisor
Onboarding	• Introduction in the company's security policies • review of security policies and security guidance	At the beginning of the employment, not later than 2 weeks within starting	Supervisor, security manager or other person in charge
Information security awareness testing/survey	• Surveys for staff related to information security and information security awareness • implemented for all staff to develop the level information security awareness	Annually, more often if necessary	HR, Security manager or other person in charge
Improvement and development	• continuous monitoring and development related to information security • implementation of possible changes and development methods based on the results of surveys	• continuous monitoring • The content of all measures should be checked once a year	HR, Security manager or other person in charge

Author: Meri Penttinen