Sunnarborg Fanny

TYÖNTEKIJÖIDEN TIETOTURVAKÄYTTÄYTYMISEEN VAIKUTTAVAT TEKIJÄT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Sunnarborg, Fanny
Työntekijöiden tietoturvakäyttäytymiseen vaikuttavat tekijät
Jyväskylä: Jyväskylän yliopisto, 2024, 55 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Halttunen, Veikko

Tämä pro gradu tutkielma keskittyy tarkastelemaan työntekijöiden tietoturvakäyttäytymistä. Tutkielmassa pyritään antamaan kuva tietoturvan tärkeydestä sekä siitä, mitkä tekijät vaikuttavat työntekijöiden tietoturvakäyttäytymiseen. Tarkastelun kohteena on yleisesti työntekijät, sillä tutkimus pyrkii antamaan yleispätevän kuvan työntekijöiden tietoturvakäyttäytymisestä keskittymättä tiettyyn toimialaan. Tutkielma muodostuu kirjallisuuskatsauksesta sekä empiirisestä osuudesta. Kirjallisuuskatsaus pyrkii luomaan käsityksen siitä, mitä tietoturvallisen työskentelyn olisi yleisesti hyvä pitää sisällään. Tietoturvatietoisuus esitetään keinona parantaa työntekijöiden tietoturvatasoa. Kirjallisuuskatsauksessa pyritään myös antamaan käsitys työntekijän roolin tärkeydestä tietoturvakokonaisuudessa yrityksen näkökulmasta. Empiirisessä osuudessa puolestaan tarkastellaan työntekijöiden asenteita ja näkemyksiä tietoturvaa kohtaan laadullisen teemahaastattelun kautta. Haastattelun kautta pyritään selvittämään, mitkä tekijät vaikuttavat työntekijän tietoturvakäyttäytymiseen. Haastatteluista syntyneistä aineistoista kootaan työntekijöiden kokemat teemat liittyen tietoturvan koettuun kontrolliin, yleiseen asenteeseen sekä koettuun normiin. Haastattelut osoittavat, että tietoturvaan koetaan tärkeänä asiana, josta kaikkien on yrityksessä kannettava vastuuta. Kuitenkaan halukkuus tietoturvan itseopiskeluun tai muiden henkilöiden tietoturvakäyttäytymisen neuvomiseen ei ollut korkealla. Tutkimuksen tuloksia voidaan hyödyntää mahdollisissa aiheen syvemmissä tutkimuksissa.

Asiasanat: Tietoturva, tietoturvatietoisuus, tietoturvakäyttäytyminen

ABSTRACT

Sunnarborg, Fanny
Factors affecting employees' information security behavior
Jyväskylä: University of Jyväskylä, 2024, 55 pp.
Information Systems, Master's Thesis
Supervisor: Halttunen, Veikko

This thesis focuses on employees' information security behaviors. The thesis aims to give a picture of the importance of information security and discusses the factors that influence the information security behavior of employees. The focus is on employees in general, as the thesis aims to provide a general picture of employee security behavior without focusing on a specific field. The thesis consists of a literature review and an empirical study. The literature review aims to provide an insight into what should be included in working in an information secure way in general and information security awareness is presented as a way to improve the employees' level of information security. The literature review also aims to give an insight into the importance of the role of the employee in the information security context from the company's point of view. In the empirical part of the study, the attitudes and perceptions of employees towards information security are examined through a qualitative thematic interview. Through interviews, the aim is to find out what factors influence the information security behavior of employees. From the interview data, themes experienced by the employees were gathered in themes related to their perceived control, general attitude and perceived norm of information security. The interviews showed that information security is seen as an important subject that is everyone's responsibility. However, the motivation to study information security or to advise others was not high. The results of the study can be used in possible further research on the topic.

Keywords: Information Security, Information Security Awareness, Information security behavior

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tässä luvussa käydään läpi tutkimuksen johdanto. Luku jakautuu neljään alaotsikkoon. Aluksi käydään läpi tutkimuksen taustaa ja tavoitteita. Lopuksi esitetään tutkimuskysymykset sekä avataan niiden suhdetta, jonka jälkeen käydään tutkielman rakenne läpi.

1.1 Tutkimuksen tausta

Nykyisissä organisaatioissa tietojärjestelmät ovat kaiken keskiössä ja niitä kehitetään jatkuvasti. Näihin nykyaikaisiin järjestelmiin liittyy uhkia, kuten järjestelmähaavoittuvuuksia, jotka vaarantavat tiedon luottamuksellisuuden, eheyden ja saatavuuden (Kyberturvallisuuskeskus, 2023). Yritykset pyrkivät kehittämään järjestelmien tietoturvaa jatkuvasti, mutta tietojärjestelmät eivät nojaudu pelkästään teknisiin ratkaisuihin vaan myös inhimillisiin tekijöihin eli ihmisten toimintatapoihin. Hyökkääjät ovat tunnistaneet inhimillisten virheiden olemassaolon ja käyttävät tätä hyödykseen. Työntekijöihin kohdistuu laajasti erilaisia tietoturvauhkia, jotka vaarantavat organisaatioiden tietoturvallisuutta. Monissa tutkimuksissa nousee esille, että organisaatioissa henkilöstö on merkittävin yksittäinen riskitekijä tietoturvan näkökulmasta, sillä ihmisiä on haastava hallita sekä heidän toimiaan arvata (Alotaibi & Alfehaid, 2018). Toisaalta samalla valpas ja osaava henkilöstö on keino parantaa organisaation tietoturvaa, jos he osaavat ilmoittaa mahdollisista poikkeamista ja luoda näin puolustuslinjaa uhkia vastaan (The Institute of Internal Auditors, 2020). Yksi keino työntekijöiden toimintatavoista lähtöisin oleviin tietoturvarikkeiden vähentämiseen voi olla työntekijöiden tietoturvakäyttäytymisen syvempi tutkiminen. Sen kautta voidaan saada tunnistettua mahdolliset tekijät, jotka vaikuttavat työntekijöiden tietoturvakäyttäytymiseen. Kun näitä tekijöitä on tunnistettu, organisaatiot voivat kiinnittää kyseisiin tekijöihin huomioita ja tätä kautta parantaa tietoturvan tasoa.

Yleisesti suositeltavaa on, että työntekijät kehittävät ja syventävät osaamistaan erilaisissa tietoturvallisuuteen liittyvissä koulutuksissa ja harjoituksissa, jotta heillä on tietämystä muuttuvista tietoturvauhkista. Tutkimukset ovat

nostaneet työntekijöiden tietoturvatietoisuuden tärkeäksi tietoturvaloukkauksiin liittyvien riskien vähentämisessä. Itse tietämyksen ja asenteiden välillä on havaittu vahvoja suhteita, mutta samalla on kuitenkin huomattu, että työntekijät eivät välttämättä muuta käyttäytymistään, vaikka heillä olisi riittävästi tietämystä. On myös muita tekijöitä, jotka vaikuttavat työntekijöiden käyttäytymiseen, kuten sosiaalinen paine tai ympäristö. (Ajzen & Fishbein, 2009).

Tietoturvatutkimukset ovat rajautuneet pitkälti tietoturvan teknisiin ratkaisuihin, mutta viime vuosina tutkimukset liittyen tietoturvan inhimillisiin tekijöihin ovat myös lisääntyneet ja työntekijöiden käyttäytymisen tutkimista on lisätty (Khando, Gao, Islman & Salam, 2021; Parsons ym., 2017). Tämä on positiivista, sillä kehittämällä tekniikoita, joilla voidaan parantaa työntekijöiden tietoturvakäyttäytymistä, voidaan vähentää heidän alttiuttaan tehdä päätöksiä, jotka altistavat organisaation hyökkäyksille (Caldwell, 2016).

Koska organisaatioiden riippuvuus tietojärjestelmistä ja tietotekniikasta vain kasvaa, jatkuvasti muuttuvan tietoturvallisuuden ymmärtäminen on tärkeää sekä varsinkin ymmärrys siitä, miten ja mistä työntekijöiden tietoturvakäyttäytyminen muodostuu. Kun pystytään ymmärtämään tekijöitä, joista käyttäytyminen muodostuu, niihin voidaan vaikuttaa ja tämän tiedon kautta tietoturvaketjun heikoimmasta lenkistä, eli työntekijöistä, voi tulla sen vahvimpia puolustajia.

1.2 Tutkimuksen tavoitteet

Ihmisten käyttäytymiseen vaikuttavat monet taustatekijät, jotka puolestaan muodostavat uskomuksia, mitkä vaikuttavat henkilön kokemukseen ja asenteeseen käyttäytymisen kohdetta kohtaan (Ajzen & Fishbein, 2009). Tässä tutkimuksessa oletetaan, että sama ilmiö tapahtuu myös henkilön suhteessa tietoturvaan. Tutkimuksessa käsitellään, mitä työntekijöiden olisi hyvä tietää tietoturvasta sekä pyritään avaamaan sitä, miksi tietoturva on asia, minkä eteen kaikkien olisi tärkeää tehdä toimia. Tutkimusta konkretisoi esimerkit tietomurroista, jotka ovat olleet seurausta työntekijöiden toimista. Tutkimus painottuu tunnistamaan tekijöitä, jotka vaikuttavat tietoturvallisen käyttäytymisen muodostumiseen, sekä haastateltavien henkilöiden tietoturvaan liittyvien käsitysten analysoimiseen, ryhmittelyyn sekä näiden kuvaamiseen.

Tutkimuksen kohderyhmäksi on valittu kokonaisvaltaisesti työntekijät ilman, että keskityttäisiin vain johonkin tiettyyn toimialaan, ikäryhmään tai muuten tiettyyn joukkoon. Tähän on päädytty, koska tutkimuksella halutaan tuottaa yleispätevä katsaus tietoturvaan kohdistuvista asenteista ja käyttäytymisestä, jota voidaan myöhemmin laajentaa ja jatkotutkia, jos se koetaan hyödylliseksi.

Työntekijöillä tässä tutkimuksessa tarkoitetaan henkilöitä, jotka ovat tällä hetkellä vakituisessa tai pitkäaikaisessa työsuhteessa. Työn ohessa tapahtuva opiskelu ei ole este tähän ryhmään kuulumiselle, mutta täysipäiväiset opiskelijat sekä myös vain pätkätyötä tekevät henkilöt poissuljetaan tästä otannasta. Keskittymällä työntekijöihin pyritään saamaan kuvaa siitä, millaisten tietoturvaan liittyvien käyttäytymisten kanssa yritykset voivat olla vastassa sekä tätä kautta

luodaan mahdollisuus siihen, että näiden tunnistettujen käyttäytymisen muovaamista pystyttäisiin tulevaisuudessa tutkimaan.

Tutkimuksessa on käyttäytymisen lisäksi myös tavoitteena tutkia tekijöitä, jotka luovat tietoturvallista työskentelyä. Tähän pyritään löytämään vastaus tarkastelemalla tämän hetken kirjallisuutta sekä suositeltuja parhaita käytänteitä.

1.3 Tutkimuskysymykset

Tämä tutkimus pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

1. Mistä tekijöistä tietoturvallinen työskentely koostuu?
2. Mitkä tekijät vaikuttavat työntekijöiden tietoturvakäyttäytymiseen?

Ensimmäisen tutkimuskysymyksen kautta pyritään luomaan kuvaa siitä, mitä tietoturvallinen työskentely on sekä samalla havainnollistetaan työntekijöiden tietoturvan tärkeyttä. Tässä yhteydessä myös määritellään, mitä tietoturva tarkoittaa, sillä työntekijöiden tietoturvallinen käyttäytyminen nojaa tietoturvaan.

Työntekijöiden omat asenteet ja uskomukset vaikuttavat käyttäytymiseen, joten tätä kautta ne vaikuttavat myös heidän tietoturvakäyttämiseensä. Tästä johtuen tutkimuksen toinen kysymys keskittyy tutkimaan käyttäytymistä ja siihen vaikuttavia tekijöitä tietoturvan yhteydessä.

Yhdessä näiden kahden tutkimuskysymyksen tarkoituksena on luoda käsitys siitä, mitä tietoturvallisen työskentelyn olisi toivottavaa pitää sisällään, sekä miten työntekijät kokevat tietoturvan. Tutkimuksessa keskitytään teemoihin, joita kaikkien työntekijöiden olisi suositeltavaa harjoittaa työssään. Jotkin tietyt työtehtävät, kuten esimerkiksi puolustusvoimilla työskentely, vaatii ehdotonta turvallisuutta monella tasolla, mutta tässä tutkimuksessa ei keskitytä pelkästään tiettyihin erityistä huolellisuutta vaativiin työrooleihin vaan tarjotaan yleiskuvaa, josta kaikille on hyötyä. Samalla perehdytään myös tietoturvakäyttäytymiseen, jotta saadaan tunnistettua tekijöitä, jotka vaikuttavat taustalla työntekijöiden toimiin. Ensimmäiseen kysymykseen pyritään löytämään vastaus tutkimuksen kirjallisuuskatsausosiossa ja toiseen kysymykseen pyritään löytämään vastaus tutkimuksen empiirisen osuuden kautta, jossa tarkastellaan työntekijöiden asenteita ja näkemyksiä tietoturvaa kohtaan laadullisen teemahaastattelun kautta.

1.4 Tutkielman rakenne

Tutkielma koostuu kahdesta pääosasta, jotka ovat tutkimuksen kirjallisuuskatsausosuus sekä tutkimuksen empiirinen osuus. Kirjallisuuskatsaukseen on koottu tämän hetken kirjallisuutta liittyen tietoturvaan sekä osuudessa esitetään myös käyttäytymiseen liittyvä malli, jonka avulla empiirisen osuuden havaintoja peilataan sekä jonka pohjalta tutkimuksen haastattelun teemat eritellään. Johdannon jälkeen tutkimuksessa siirrytään tietoturvakäyttäytymiseen, jossa

käsitellään lyhyesti tietoturva, työntekijän tietoturvaa ja sen tärkeyttä sekä yleisempiä tietoturvahyökkäyksiä, joita työntekijöihin kohdistuu sekä yleisempiä rikkeitä. Tämän lisäksi käsitellään myös työntekijöiden vapaa-ajan internet käyttäytymisen suhdetta yrityksen tietoturvaan. Kirjallisuuskatsaus sisältää myös käsitteen tietoturvatietoisuus käsittelyn sekä käy läpi työntekijän tietoturvakäyttäytymiseen vaikuttavia tekijöitä. Tämän yhteydessä esitetään myös Ajzenin ja Fishbeinin (2009) perustellun toiminnan viitekehys.

Kirjallisuuskatsauksen jälkeen siirrytään tutkimuksen toteutuksen läpikäyntiin, jossa huomioidaan tutkimuksen menetelmä sekä aineiston keruu ja analysointi. Tämän jälkeen läpikäydään tutkimuksen tuloksia haastattelussa hyödynnettyjen teemojen pohjalta. Lopuksi vielä läpikäydään tutkimuksen johtopäätökset, luotettavuus ja jatkotutkimusaiheet.

2 TIETOTURVAKÄYTTÄYTYMINEN

Tässä luvussa ensin pohjustetaan työntekijän tietoturvaa, jonka jälkeen käsitellään lyhyesti tietoturva ja määritellään mitä se pitää sisällään. Tämän jälkeen siirrytään pohtimaan työntekijöiden tietoturvan tärkeyttä, yleisimpiä tietoturvahyökkäyksiä, joita työntekijöihin kohdistuu sekä käydään läpi tietoturva rikkeitä, joita työntekijät voivat tiedostamatta tehdä.

2.1 Työntekijän tietoturva

Elämme yhteiskunnassa, joka on laajasti digitalisoitunut ja pääosa tiedoista on jatkuvasti saatavilla sähköisessä muodossa, mikä vaatii organisaatiolta toimia tietojensa suojaamiseksi (Haeussinger & Kranz, 2017). Työntekijöiden rooli tietoturvassa on tunnetusti merkittävä (Khando ym. 2021; Fisher, Prord & Peterson, 2021), sillä muun muassa tietojärjestelmät ovat sosioteknisiä kokonaisuuksia, jossa teknologian lisäksi ihmisen rooli on keskeisessä osassa. Työntekijät ovat järjestelmien käyttäjiä ja siten kiinnostava ja merkittävä kohde tietoturvahyökkäyksille, sekä usein myös syynä tietoturvahyökkäysten onnistumiselle. Samalla työntekijöiden kautta hyökkäykset on mahdollista pystyä estämään tai tarvittavat toimenpiteet käynnistettyä ajoissa, jos työntekijöillä on tarvittava tietämys aiheesta. Tietoturva koskee kaikkia organisaation henkilöitä johtajista lähtien, minkä takia sen tärkeyttä ei voi sivuuttaa (Esteves, Ramalho & De Haro, 2017).

Organisaatiot tekevät monia tietoturvaa edistäviä toimia, kuten suojaavat laitteitaan sekä kouluttavat työntekijöitään. Tietoturvan oikeanlainen harjoittaminen, tai sen puute, on huolenaihe kaikenkokoisille organisaatioille toimialasta riippumatta. Tietoturvan tärkeys kuitenkin korostuu varsinkin, kun yrityksessä käsitellään sensitiivistä tietoa, kuten henkilötietoja, jotka voi yhdistää tiettyyn henkilöön. Tällöin yritykseltä vaaditaan usein myös vaatimustenmukaisuutta (compliance), joka tarkoittaa organisaation prosessien ja ohjelmien mukauttamista ulkoisiin sääntöihin ja standardeihin. (Haney & Lutters, 2017.)

Tietoturva on kokonaisuudessaan monitahoinen ja vaativa kokonaisuus, jonka hallintaan on olemassa tietoturvastandardeja ja parhaita käytäntöjä, joiden

tärkeys korostuu, kun organisaatiolta vaaditaan toimialan puitteissa tiettyä tasoa (McIlwraith, 2021). Tällaisia aloja ovat mm. terveydenhuolto, julkishallinto ja rahoituspalvelut (Haney & Lutters, 2017). Tiettyjen tietoturvastandardien tavoitteena on varmistaa hallinnan ajantasaisuus, kattavuus sekä sen parantamistavoitteet.

Vaikka monissa organisaatioissa luotetaan kehittyneisiin teknologioihin ja erikoistuneisiin tietoturvaominaisuuksiin järjestelmien suojaamiseksi, työntekijöiden roolia turvallisen ympäristön ylläpitämisessä ei pidä sivuttaa. Khando ym. (2021) nostavat tutkimuksessaan esille, kuinka merkittävä osa organisaatioiden tietoturvaongelmista johtuu joko suoraan tai välillisesti inhimillisistä tekijöistä eli ihmisten toimista, minkä takia työntekijöihin on oleellista myös keskittyä tietoturvassa.

Esteves, Ramalho ja De Haro (2017) esittävät, että yritysten on tärkeää kouluttaa ja lisätä työntekijöiden tietoisuutta tietoturvaan liittyen, jos työntekijät pääsevät edes jonkin tason luottamukselliseen tietoon käsiksi. Vaikka organisaatio on keskeisessä asemassa ja heillä on vastuu varmistaa, että työntekijät saavat tarvittavan tietoisuuden tietoturvan tärkeydestä, on työntekijän hyvä tietää henkilökohtaisesti edes perusteet tietoturvasta. Kyberturvallisuuskeskus (2020) luettelee muun muassa seuraavat kohdat osaamiseksi, joita kaikilla työntekijöillä olisi vähimmäisvaatimuksena hyvä olla, niin työpaikan, kuin myös osittain henkilökohtaisen tietoturvan kannalta:

- Riittävän pitkien uniikkien salasanojen käyttö.
- Monivaiheisen tunnistuksen hyödyntäminen.
- Oma aktiivisuus perehtyä yrityksen tietoturvakäytänteisiin sekä noudattaa niitä.
- Päivitysten tekeminen, kun ne tulevat saataville.

Edellä mainitut kohdat auttavat suojamaan organisaation tietoja, sillä kyseisten toimien kautta varmistetaan, että luvattomat henkilöt eivät pääse työntekijän käyttäjätilille. Työntekijän oma aktiivisuus tutusta työnantajaorganisaation tietoturvakäytänteiseen luo valmiutta tunnistaa riskejä ja antaa taitoja toimia oikeaoppisesti tilanteissa, jossa tietoturva on mahdollisesti vaarantunut. Päivitykset on myös nostettu listalle, sillä ne sisältävät usein tietoturvakorjauksia, joilla korjataan haavoittuvuuksia järjestelmässä.

2.2 Tietoturva lyhyesti

Tietoturva ja kyberturva voidaan helposti arkisessa keskustelussa sekoittaa keskenään, mutta tässä tutkielmassa keskitytään tietoturvallisuuteen eli tietoturvaan. Tietoturva kattaa laajasti tiedon turvaamisen, johon kuuluu esimerkiksi tietoon pääsyyn rajoittaminen sekä siihen kuuluu keskeisenä tekijänä myös riskienhallinta. Tietoturva ei rajoitu pelkästään tietojärjestelmiin, joten sen voidaan katsoa olevan osa organisaation kokonaisturvallisuutta. Kyberturvallisuus painottuu tiedon, tietojärjestelmien ja laitteiden turvallisuuden takaamiseen

verkkoympäristössä sekä eri hyökkäysten estämiseen. Von Solms ja Von Solms (2018) toteavat, että tietoturva ja kyberturvallisuus voivat mennä käsitteinä osittain päällekkäin, mutta kyberturvallisuus, on osa tietoturvaa ei välttämättä toisin päin. Kyberturvallisuutta voidaan näin pitää tietoturvan yhtenä osa-alueena.

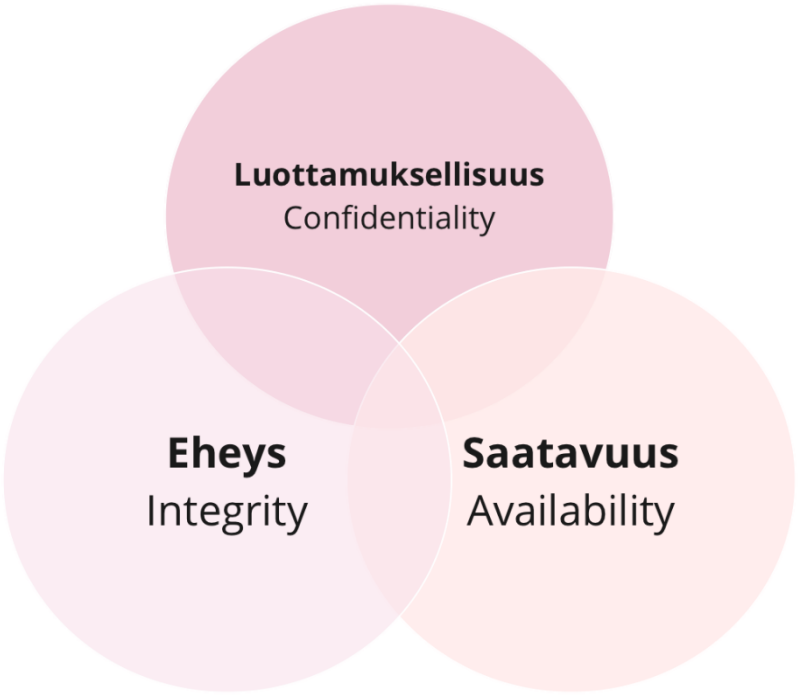
Tietoturvallisuus on jatkuva prosessi, johon kuuluu muun muassa suojaussovellusten ja -laitteiden hyödyntäminen, kuten haittaohjelmien torjuntaohjelmat tai palomuurit. Näiden teknisten ratkaisujen lisäksi, siihen vaikuttavat myös jokaisen oma toiminta sekä oikeaoppisten käytänteiden implementointi, kuten vaatimalla käyttäjiltä käyttäjän todentamista monivaiheista tunnistautumista hyödyntäen sekä ohjelmistojen pitämistä ajan tasalla. Tietoturvassa ei ole kysymys pelkästään tekniikasta, vaan ihmisten työskentelytavat ja oikeaoppinen toiminta ovat merkittävässä asemassa teknisten ratkaisuiden rinnalla.

Tietoturvallisuudessa tietoa käsitellään sekä tietojärjestelmien turvallisuudesta huolehditaan koko niiden elinkaaren ajan turvallisesti. Tietoturvaa pohtiessa on myös huomattava, että tieto ei aina välttämättä ole sähköisessä muodossa vaan myös paperilla oleva tieto on suojattava sekä puhuttaessa tapahtuva tiedonvaihto on tehtävä turvallisesti ja luottamuksellisesti. Kyberturvallisuuskeskus (2024) määrittelee tietoturvalle seuraavat keskeiset piirteet:

- Luottamuksellisuus eli se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla.
- Eheys eli se, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut, jolloin varmistutaan tietojen ristiriidattomuudesta.
- Saatavuus eli se, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

Luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability) muodostavat vahvan kulmakiven tietoturvan keskeiselle ominaisuudelle eli tiedon suojaamiselle, jotka edelleen luovat perustan yrityksen turvallisuus infrastruktuurille. Tästä kolmijaosta käytetään myös nimeä tietoturvan kolme pilaria (CIA-triad) (Smaonas & Coss, 2014). Näiden kolmen kohdan huomioon ottaminen antaa pohjan yrityksen tietoturvakäytäntöjen kehittämiselle sekä esimerkiksi tilanteisiin, kun arvioidaan uusien teknologioiden käyttöönottoa (Chai, 2023).

CIA-kolmiota (kuvio 1) voidaan pitää tietoturvan klassisena määrittelynä, sillä se juontaa juurensa pitkälle. Kyseinen jako on saanut kritiikkiä sen kapeasta teknisestä suuntautumisesta sekä sen rajallisesta hyödyllisyydestä hetkinä, kun on otettava huomioon turvallisuuden laajemmat organisatoriset ja sosiaaliset näkökohdat. Tästä syytä tätä klassista määritelmää on täydennetty uusilla osa-alueilla vuosien saatossa, kuten vastuullisuudella ja henkilöiden aitoudella, joita yritykset voivat soveltaa tarpeidensa mukaan. (Smaonas & Coss, 2014).



KUVIO 1 Tietoturvan kolme pilaria eli CIA-kolmio

CIA-kolmion perusmalli, joka edustaa yllä mainittua kolmea keskeistä periaatetta, on kuitenkin edelleen kulmakivi, jota organisaatiot hyödyntävät. Yhteenvetona voidaan todeta, että tietoturvalla tarkoitetaan käytäntöjä, jossa tietoa suojataan luvattomalta pääsyltä, käytöltä tai luvattomalta muokkaamiselta tai tuhoamiselta. Tietoturva käsittää erilaisia toimenpiteitä, joiden tarkoituksena on suojata niin tiedot, järjestelmät, verkot sekä muut organisaatioiden digitaaliset varat mahdollisilta uhilta ja haavoittuvuuksilta. Tehokkaisiin tietoturvakäytäntöihin kuuluu teknologian, toimintatapojen, menettelyjen ja työntekijöiden tietämyksen hyödyntäminen riskien vähentämiseksi ja tiedon suojaamiseksi.

2.3 Työntekijöiden tietoturvan tärkeys

The Institute of Internal Auditors (2020) määrittelee mallissaan riskienhallinnalle työntekijät osaksi ensimmäistä puolustuslinjaa, sillä he ovat osa jokapäiväisiä operatiivisia toimia. Tätä voi tietoturvamielessä ajatella niin, että työntekijöillä on oltava asianmukainen tietämys tietoturvasta ja heihin kohdistuvista uhkista, jotta yrityksen tietoturvastrategia onnistuu.

Monesti ihmiset, jotka eivät tee töitä tietoturvan parissa voivat mahdollisesti väheksyä omaa rooliaan yrityksen tietoturvassa. Ashenden (2018) tutkimuksessaan sai selville, että osa työntekijöistä ajattelee tietoturvan olevan työnantajan vastuulla sekä olevan asia, johon työntekijöiden ei tarvitsisi puuttua. Ashendenin (2018) tutkimuksessa tuli esille, että tietoturvan voidaan nähdä olevan etäinen asia, joka omalta osalta hoituu noudattamalla yrityksen tekemiä

pakollisia sääntöjä, ja muuten sen katsotaan olevan yrityksen vastuulla. Mikkola (2021) puolestaan pohtii kirjoituksessaan, kuinka tietoturvan on usein ajateltu ei niin ihmislähtöisenä asiana, vaan enemmän järjestelmiin keskittyneenä teknisempänä kokonaisuutena.

Vaikka monesti tietoturvan ajatellaan olevan pelkkä tietojärjestelmiin liittyvä asia, on tiedostettava sen olevan kokonaisuus. Pelkät tekniset ratkaisut eivät yksin suojaa yritystä, sillä kaikkia järjestelmiä käyttävät loppukädessä yrityksen työntekijät (Kyberturvallisuuskeskus, 2023). Myös Khando ym. (2021) nostavat esille, että pelkkä keskittyminen tietoturvan teknisiin näkökohtiin ei riitä, sillä tietoturva on luonteeltaan moniulotteista ja ihmisten toimilla on siinä suuri merkitys.

McIlwraith (2021) toteaa, että yksinkertainen tosiasia on, että suurin osa tietoturvarikkomuksista on peräisin yrityksen sisältä olevan tahon toiminnasta tai toimimattomuudesta, joka voi johtua joko tietämättömyydestä tai puhtaasta virheestä. Työntekijöiden on ymmärrettävä sääntöjen vastaisen toiminnan eli tietoturvarikkomusten seuraukset, joita voivat yritykselle olla pahimmassa tapauksessa imagon menetys sekä taloudelliset tappiot (Hänsch & Benenson, 2014). On erittäin oleellista tiedostaa, että tietoturva ei ole yhden henkilön tai tietyn tietojärjestelmän vastuulla, vaan se on koko organisaation yhteinen asia (Kyberturvallisuuskeskus, 2023). Tästä syystä työntekijöiden oikeaoppisen tietoturvakäyttäytymisen levittäminen on yksi tärkein tekijä, jolla pystytään suojautumaan epätoivotuilta tietoturvakäyttäytymiseltä (Alotaibi, 2019).

Kun työntekijätasolla tunnistetaan tietoturvan tärkeys, siitä voidaan luoda yhteinen prioriteetti, jolloin koko organisaation tietoturvan taso paranee. Näin tietoturvahyökkäyksiä on haastavampaa saada menestyksekkäästi toteutettua kuten myös työntekijöiden omat tiedostamatta haitalliset toimet vähenevät. (Pattinson ym., 2016).

Heiskanen (2020) esittää kirjoituksessaan, kuinka henkilöstön osaamista ja tietoisuutta kasvattamalla yritykselle voidaan rakentaa niin sanottu "vahva palomuuri", joka koostuu turvattujen järjestelmien ja laitteiden lisäksi myös valppaana olevasta henkilöstöstä. On oleellista huomioida, että vaikka henkilöstön osaamiseen panostetaan, inhimilliset virheet ovat aina mahdollisia ja niitä voi sattua. Henkilöstöstä ei voi täysin poissulkea riskiä virheille, mutta tietoturvatietoisuuteen on silti tärkeää panostaa, sillä kun henkilöstöllä on tiedossa oikeat toimintamallit, yritys voi tätä kautta minimoida vahingot, kun työntekijät osaavat tunnistaa virheitä ja tietävät oikeat toimet niiden sattuessa (Kyberturvallisuuskeskus, 2023).

2.4 Yleisimmät työntekijöihin kohdistuvat tietoturvahyökkäykset

Kuten aikaisemmin tässä tutkimuksessa todettiin, kyberturvallisuus kuuluu osaksi tietoturvaa, niinpä tietoturvahyökkäyksistä voidaan puhua myös kyberhyökkäyksinä. Kyberhyökkäykset voivat kohdistuvat tietokoneisiin, tietoverkkoihin ja infrastruktuureihin. Hyökkäyksen takana voi olla yksi henkilö tai

isompi taho (esimerkiksi valtio). Hyökkäykset voivat kohdistua organisaatioiden lisäksi myös yksityishenkilöihin. Traficom (2024) uutisoi, että organisaatioihin kohdistuneet tietoturvahyökkäykset ovat viime vuosina kasvaneet paljon. Yksi suurin tietoturvahyökkäysten tyyppi on kalasteluhyökkäykset, jotka kohdistuvat varsinkin yritysten työntekijöihin (Traficom, 2024; Thomas, 2018).

Fisher, Porod ja Peterson (2021) määrittelevät tutkimuksessaan, että turvallisuus muodostuu kolmesta komponentista, jotka ovat ihmiset, prosessit ja teknologiat. He toteavat, että nykypäivänä kaikkein kriittisempänä komponenttina voidaan katsoa ihmistä, sillä ihmiset ovat teknologian käyttäjiä sekä prosessit ovat juuri niin toimivia kuin miten ihmiset ovat ne käyttöönottaneet. Työntekijät ovat kaiken keskiössä tietoturvahyökkäyksissä, sillä työntekijät voivat huolimattomuudellaan tai tietämättömyydellään mahdollistaa hyökkääjille pääsyn yrityksen tietoihin, jolloin tietojen luottamuksellisuus, eheys ja saatavuus voi vaurioitua tai se voidaan menettää kokonaan. Pahimmissa tapauksessa, hyökkäyksen seurauksena koko yritys voi lamaantua ja/tai henkilötietoja varastetaan (Borkovich & Skovira, 2019). Hyökkääjät tiedostavat ihmisten olevan tietoturvan heikoin kohta, jonka takia hyökkääjät usein kohdentavat iskuja juuri työntekijöihin ja käyttävät aikaa huolellisten hyökkäysten tekemiseen.

Työntekijöihin kohdistuvissa hyökkäyksissä on monesti kyse käyttäjän manipuloinnista. Hyökkääjät käyttävät hyväksi käyttäjien tunteita ja pyrkivät herättämään käyttäjässä esimerkiksi kiireen, stressin tai uteliaisuuden tunteita, mikä edistää käyttäjän puolella harkitsemattomampaa toimintaa ja luo mahdollisuuden virheiden tekemiselle. Seuraavaksi käydään läpi yleisimpiä työntekijöihin kohdistuvia tietoturvahyökkäyksiä.

Haittaohjelma

Haittaohjelma (malware) on käsite, jonka alle kuuluu kyberrikollisten kehittämät pahantahtoiset ohjelmistot, virukset, madot ja muita ohjelmia lataavat haittaohjelmat kuten vakoiluohjelmat (Kyberturvallisuuskeskus, 2024). Haittaohjelmien motiivina on varastaa tietoja sekä vahingoittaa tai tuhota tietojärjestelmiä. Ne leviävät muun muassa sähköpostien liitteinä tai verkosta ladatun ohjelmiston mukana. Haittaohjelmat voivat tarttua kaikkiin fyysisiin verkossa oleviin laitteisiin eli tietokoneiden lisäksi myös mm. mobiililaitteisiin.

Väliintulohyökkäys

Väliintulohyökkäyksessä (Man-in-the-middle attack) kolmas osapuoli eli hyökkääjä tunkeutuu huomaamatta kahden osapuolen väliseen viestintään ja pystyy tätä kautta saamaan itselleen sensitiivistä dataa (Fisher, Porod & Peterson, 2021). Väliintulohyökkäyksen uhriksi voi johtua, jos käyttää esimerkiksi tuntemattomia julkisia Wi-Fi verkkoja, jolloin hyökkääjä pystyy seuraamaan kohteen liikkeitä Wi-Fin välityksellä.

Tietojenkalastelu

Tietojenkalastelu on erittäin suosittu hyökkäystapa tällä hetkellä, ja kalastelu hyökkäykset ovat lisääntyneet (Traficom, 2024; Thomas, 2018). Tietojenkalastellussa pahantahtoiset tahot pyrkivät samaan pääsääntöisesti erinäköisiä huijausviestejä hyödyntäen käsiinsä esimerkiksi käyttäjätunnuksia, salasanoja tai muita

tietoja. Tietojenkalastelu voi olla kohdennettua, jolloin se keskittyy esimerkiksi yrityksessä tiettyyn käyttäjään tai käyttäjäryhmään. Tämän tyyppiset tarkat hyökkäykset ovat tyypillisiä yritysmaailmassa, kun hyökkääjät tunnistavat mielenkiintoiset kohteet. Yleensä hyökkääjät tutkivat kohdeyritystä niin, että he pystyvät luomaan henkilökohtaisen ja aidon tuntuisen viestin, jota kautta he pyrkivät vaikuttamaan ja huijaamaan kohdettaan (Thomas, 2018).

Kohdennettuja viestejä voi olla erittäin haastava tunnistaa varsinkin, kun viestienvaihto sähköpostilla voi olla nopeatempoista, jolloin luotetaan aidolta tuntuvaan viestiin eikä pysähdytä tutkimaan viestin sisältöä tai ulkonäköä sen enempään. Tietojenkalasteluviestit sisältävät yleensä vaarallisia piilotettuja latauslinkkejä tai linkkejä, jotka vievät väärennetyille sivustoille. Tietojenkalastelu voi tapahtua myös puhelimitse, jolloin hyökkääjä esiintyy esimerkiksi yrityksen IT-tukena ja pyrkii saamaan käsiinsä tietoa tai työntekijän lataamaan etähallintaohjelman tietokoneellensa.

Haavoittuvuuksien hyväksikäyttö
Jos laitteita ei päivitetä ja pidetä ajan tasalla se on altis hyökkäyksille. Usein yritykset hallitsevat työasemiaan keskitettyjen hallintaohjelmien kautta, kuten Intune tai SCCM, ja tätä kautta pakotetusti puskevat päivitykset käyttäjien työasemiin, mutta esimerkiksi puhelimissa ohjelmistopäivitykset jäävät usein käyttäjän vastuulle, sillä niihin vaaditaan usein tietty määrä akkua tai WiFi-yhteys. Hyökkääjät voivat hyödyntää haavoittuvuuksia esimerkiksi haittaohjelmien levittämiseen. Haavoittuvuuksiin kuuluu myös nollapäivähaavoittuvuudet, joilla tarkoitetaan tietoturvahaavoittuvuutta, jolle ei ole vielä olemassa korjausta.

2.5 Yleisimmät organisaation tietoturvaa heikentävät työntekijöiden toimet

Työntekijöiden toimet voivat johtaa tietoturvallisuuden vaaratilanteisiin eli tietoturvarikkomuksiin. Kaikki tietoturvarikkeet eivät aina johda tietoturvaloukkaukseen. Tietoturvaloukkaus on tapahtuma, jossa kuulumaton taho pääsee luvattomasti tietokoneen tietoihin, verkkoon tai järjestelmiin käsiksi. Tietomurto on tapaus, jossa tietoturvaloukkaus on tapahtunut ja hyökkääjä on saanut vietyä tietoja mukanaan. Monissa tutkimuksissa työntekijät nostetaan johtavaksi syyksi tietoturvaloukkausten tapahtumiselle (Ncubukezi, 2022; KasperskyDaily, 2017). Työntekijät voivat tehdä virheitä joko siksi, että he ovat huolimattomia ja tekevät vahingossa virheitä, tai siksi, että heillä ei ole tarvittavaa tietämystä siitä, miten toimia asianmukaisesti, jotta he pystyisivät suojelemaan yritystä.

Syitä tietoturvarikkomusten tapahtumiselle voi olla monia. El-Bably (2021) selvitti tutkimuksessaan, että työntekijät itse kokevat häiriötekijöiden olevan yhtenä syynä virheiden tapahtumiselle. Toisena johtavana tekijänä on väsymys ja sen seurauksena tuleva keskittymisen puute. El-Bablyn (2021) tutkimuksessanostetaan esiin, että osa työntekijöistä kokee etätyön edistävän virheiden tapahtumista, sillä kotona keskittyminen herpaantuu helpommin, jolloin virheet ovat

mahdollisia. Ncubukezi (2022) nostaa myös osaamattomuuden sekä työntekijän huonon päätöksenteon tekijöiksi, jotka edistävät virheiden syntymistä.

Vaaratilanteita, jotka voivat johtaa tietoturvaloukkauksiin on lukemattomia ja riippuen työntekijän roolista rikkeet voivat olla erityyppisiä. Alla olevaan listaan on koottu tutkimuksissa (Alsharif, Mishra & AlShehri, 2022; El-Bably, 2021; Ncubukezi, 2022) nousseita yleisempiä tietoturvarikkeitä, joita työntekijöiden on yleisesti työroolista riippumatta tunnistettu tekevän:

- Heikko salasana sekä sama salasana kaikissa keskeisissä järjestelmissä.
- Henkilökohtaisen laitteen käyttö työasioiden hoitamiseen.
- Tietojen lähettäminen tai jakaminen virheellisiin osoitteisiin.
- Laitteita ei päivitetä.
- Epäilyttävien sähköpostiliitetiedostojen lataaminen.
- Tuntemattomien linkkien avaaminen.
- Applikaatioiden lataaminen tuntemattomista lähteistä.
- Tuntemattomien muistitikkujen tai lisälaitteiden yhdistäminen työasemaan.
- Julkisten Wifi-yhteyksien käyttäminen.

Sosiaalinen manipulointi ja sen kautta tapahtuva tietojenkalastelu yhdistettynä työntekijöiden huolimattomuuteen on lisääntynyt ja se on merkittävä tekijä haittaohjelmien leviämiseen, sekä kohdennettujen hyökkäysten lisääntymiseen (Kaspersky Daily, 2017). Yllä olevasta listasta nähdään, että tekijöitä, jotka kuuluvat tähän osa-alueeseen ovat “Epäilyttävien sähköpostiliitetiedostojen lataaminen.” ja “Tuntemattomien linkkien avaaminen.”.

Edellä olevasta luettelosta huomataan, että osa rikkeistä on selvästi seurausta työntekijän omasta ajattelemattomuudesta, eikä niinkään hyökkääjään aktiivisen yrityksen tulosta. Aina ei ole kyse, että työntekijä joutuu uhriksi vaan työntekijä voi omalla toiminnallaan aiheuttaa riskejä. Kohta “Henkilökohtaisen laitteen käyttö työasioiden hoitamiseen.” on hyvä esimerkki tästä, sillä varsinkin yrityksissä, joissa työntekijät saavat itse hankkia työssä käytettävän mobiililaiteen, on työntekijän vastuulla huolehtia laitteella olevista tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta. Toinen esimerkki työntekijän omasta ajattelemattomuudesta on kohta “Tuntemattomien muistitikkujen tai lisälaitteiden yhdistäminen.”.

Yllä olevassa listassa olevien rikkeiden lisäksi Kaspersky Daily (2017) nostaa myös tietoturvariskeiksi työntekijöiden fyysisten laitteiden kadottamisen. Varsinkin BYOD (Bring-Your-Own-Device) on herättänyt paljon keskustelua riskeistä liittyen työntekijöiden fyysisten laitteiden käyttöön, sillä omien laitteiden käyttö työssä antaa hyökkääjille lisää sisäänpääsymahdollisuuksia yritysten järjestelmiin (Chen, Li, Chen & Yin, 2021). Pahimmassa tapauksessa työntekijä voi aiheuttaa suuren tietoturvariskin, jos hän hukkaa laitteensa ja ei noudata yrityksen tietoturvaprotokollia tilanteen tapahtumisen jälkeen.

2.6 Työntekijöiden vapaa-ajan internetkäyttäytyminen

Sosiaalinen media on tuonut omia haasteitaan yritysten tietoturvaan. Sosiaalisessa mediassa jaetaan helposti liikaa tietoja, mikä helpottaa valtavasti hyökkääjien työtä luoda tietyille työntekijöille kohdennettuja hyökkäyksiä sosiaalisen manipuloinnin avulla (Singh, 2016). Tällä tavalla hyökkääjät voivat saada myös selville kaikkein mielenkiintoisimmat uhrit esimerkiksi heidän työroolinsa mukaan. Alla olevaan listaukseen on koottu Singh (2016) luettelemat asiat, joita hyökkääjä voi sosiaalisen median kautta saada pahimmassa tapauksessa selville henkilöstä, ja joita hyökkääjä voi käyttää hyväkseen kohdentaessaan personoitua hyökkäystä:

- nimi
- kaupunki
- sähköposti ja puhelinnumero
- työnantaja ja ammatti
- työkaverit
- osaaminen ja harrastukset
- parisuhde ja/tai perheenjäsenet
- mielipiteet.

Suurin osa yritysten turvatoimista on tarkoitettu etähyökkäyksiä vastaan palomuurien ja muiden digitaalisten suojausten muodossa. Helpoin tapa hyökkääjille on ohittaa kaikki turvatoimet pääsemällä yrityksen rakennukseen sisään ja jättää sinne ansoja, kuten muistitikkuja, jotka sisältävät haittaohjelman, tai asentaa suoraan haittaohjelma yrityksen järjestelmään. Monesti työntekijät eivät yksinkertaisesti käsitä esimerkiksi, kuinka tärkeää on pitää kulkukortin ulkonäkö salassa, kun he jakavat kuvia kulkukorteista sosiaalisessa mediassa, sillä työntekijän kulkukortti on hyökkääjän avain yritykseen (Morand, 2023). Kulkukortista on helppo tehdä väärennös, jolloin yrityksen sisälle pääseminen on helppoa esimerkiksi lounasaikaan muiden mukana samalla oven avauksella.

Työntekijöiden vapaa-ajan internet käyttäytyminen vaikuttaa myös heidän yrityksensä turvallisuuteen, jonka takia siihen olisi tärkeää kiinnittää huomiota. Singh (2016) nostaa esille, kuinka nykyisin on kummallinen käsitys, että on hyväksyttävää jakaa yksityistä tietoa julkisuuteen, mikä on suuri ongelma, sillä se lisää riskiä kohdennetuille hyökkäyksille. Näin ollen työntekijöiden on hyvä tiedostaa, että heidän tietoturvakäyttäytymisensä ei rajoitu pelkästään työaikana tapahtuviin toimiin, vaan siihen kuuluu myös heidän vapaa-aikansa käyttäytyminen.

2.7 Esimerkkejä tietomurroista

Tietomurto tarkoittaa tietojärjestelmään, palveluun tai sovellukseen kohdistuvaa luvatonta tunkeutumista tai käyttöä esimerkiksi anastettujen tunnusten avulla

sekä tämän jälkeistä tiedon luvatonta jakamista tai tiedon myymistä eteenpäin kohteesta. Jotta saadaan havainnollistettuna laajuus, joita työntekijöiden rikkeistä johtuvat tietoturvaloukkaukset ja sitä kautta tietomurrot voivat aiheuttaa, alla olevaan taulukkoon 1 on koottu seuraavaksi muutama tapaus tietomurtoihin liittyen.

TAULUKKO 1 Tietomurto tapauksia

Yritys	Syy	Seuraus
OP-ryhmä (Yle. 7.12.2023)	Työntekijä joutui tietojenkalastelun uhriksi ja antoi tätä kautta ulkopuoliselle taholle M365 tunnuksensa.	Asiakkaiden henkilötietoja saattoi päätyä ulkopuolisen tahon käsiin.
Okta (Tekniikka & Talous 6.11.2023)	Työntekijä kirjautui henkilökohtaiselle Google-tililleen yrityksen tietokoneella, jonka hyökkääjä sai murrettua ja sitä kautta pääsi Oktan verkossa oleviin tileihin.	134 asiakkaan tiedostot vaarantuivat ja 5 asiakkaan järjestelmiin hyökättiin varastettujen tietojen avulla.
American Airlines (Tekniikka & Talous, 2022)	Ulkopuolinen taho pääsi työntekijöiden sähköpostitileihin.	Hyökkääjä sai käsiinsä asiakkaiden ja työntekijöiden sensitiivisiä tietoja.
Colonial Pipeline (Kerner, 2022)	Työntekijä uudelleen käytti vaarantunutta salasanaa ja hyökkääjät pääsivät verkkoon VPN-tilin kautta, josta alkoi kiristyshaittaohjelma hyökkäys (Ransomware attack).	Hyökkäyksen seurauksena putkilinjojen digitaaliset järjestelmät saastuivat ja pysähtyivät päiviksi. Yritys maksoi hakkereille 4,4 miljoonaa dollaria lunnaita, jotta he saivat työkalun järjestelmän palauttamiseen.

Kuten taulukon 1 hyökkäyksistä nähdään, sähköposti on yleinen tapa, jonka kautta lähetetään haittaohjelmia työntekijöille kalasteluviestien muodossa. Haittaohjelmat voivat myös päästä latautumaan työasemalle huolimattoman selailun tai muiden ohjelmien mukana, eivätkä välttämättä näyttäydy heti. Hyökkääjät voivat päästä yrityksen IT järjestelmiin jossain tapauksissa jo viikkoja ennen kuin he käynnistävät hyökkäyksen ja odottavat sopivaa hetkeä hyökkäyksen aloitukselle (Kyberturvallisuuskeskus, 2022). Usein jo työntekijän sähköpostiin pääsy on hyökkääjien keino päästä sensitiiviseen tietoon käsiksi, sillä työntekijät valitettavasti usein säilövät tietoja sähköpostissaan. Sähköposti ei ole arkaluontoisen tiedon säilytyspaikka.

Kohteena olevalle yritykselle tietomurrot voivat aiheuttaa taloudellisten tappioiden lisäksi mainehaittoja. Tai kuten taulukossa 1 nähdään, organisaation

toiminta voi estyä pitkäksikin aikaa korjausten tai jopa IT-ympäristön uudelleenasennuksen takia, mitkä voivat luoda merkittäviä rahallisia menetyksiä pitkäksi aikaa. Hyökkäyksessä vaarantuneiden henkilötietojen avulla hyökkääjät voivat tehdä identiteettivarkauksia ja käyttää henkilöiden tietoja muun muassa petolliseen toimintaan. Työntekijän tietoturvarikkeen seuraukset voivat huonoimmissa tapauksissa olla todella laajat ja levitä myös yrityksen ulkopuolelle.

3 TIETOTURVATIETOISUUS

Tässä luvussa käsitellään tietoturvatietoisuutta. Luku jakautuu kolmeen alalukuun. Ensin määritellään, mitä tietoturvatietoisuus tarkoittaa. Tämän jälkeen tarkastellaan tietoturvatietoisuuden mittaamista sekä lopuksi keinoja tietoturvatietoisuuden levittämiseksi.

3.1 Tietoturvatietoisuuden määritelmä

Tietoturvatietoisuudessa (eng. Information Security Awareness (ISA)) keskeistä on tiedon ymmärtäminen resurssina, josta organisaatio on erittäin riippuvainen (Khan, Alghathbar, Nabi ja Khan, 2011). Tieto on toiminnassa kaiken keskiössä, sillä jos organisaation kriittiset tiedot vaarantuvat, siitä voi olla organisaatiolle merkittäviä seurauksia. Tietovuodot voivat esimerkiksi aiheuttaa vakavia taloudellisia vahinkoja, mutta myös mainehaittaa ja asiakkaiden luottamuksen menetystä, joista ei ole helppo toipua.

Tutkimuskirjallisuuden pohjalta on huomattu, että tietoturvatietoisuudelle ei ole yhtä yleispätevää määritelmää, mutta käsitteen tulkinnassa on havaittavissa kaksi suuntausta. Toisessa näkemyksessä tietämyksen tasoa voidaan konkretisoida yksilön tietojen ja taitojen pohjalta. Tässä näkemyksessä tietoturvatietoisuus määrittyy tietoturvauhkien ja niiden torjuntakeinojen tietämyksestä. Toinen lähestymistapa painottuu enemmän toiminnan ulottuvuuteen. Siinä tietoisuuden määrittää se, missä määrin työntekijä paitsi ymmärtää tietoturvan merkityksen ja tuntee organisaatiolle riittävät tietoturvatasot sekä yksilöllisen tietoturvaan liittyvien velvollisuuksiensa lisäksi myös arjessaan toimii niiden käytänteiden mukaisesti. (Stefaniuk, 2020).

Edellisten pohjalta tietoturvatietoisuus voidaan siten selittää työntekijöiden ymmärryksenä yrityksen tietoturvastrategioista ja -toimenpiteistä sekä heidän näkökulmansa niiden noudattamiseen. Alotaibi ja Alfehaid (2018) tuovat esiin, että tämä tiedon kartuttaminen työntekijöiden keskuudessa ja heidän suhtautumisensa tietoturvaan vahvistavat organisaation suojaa monella tasolla, nimittäin tietoturvatietoisuus lisää suojaa fyysisiä uhkia kuin myös tietoturvaloukkauksia

vastaan. Koska tietojärjestelmät ovat kulmakivi, jonka kautta yritykset toimivat ja niiden parissa työskentely kuuluu organisaatioiden työntekijöiden päivittäisiin työtehtäviin, on niiden suojaaminen entistä tärkeämpää (Bullee, Montoya, Pieters, Junger & Hartel, 2015).

Tietoturvatietoisuus ei ole pelkästään asia, jota yritys voi halutessaan pohtia noudattavansa, vaan se on vahvasti suositeltavaa ennaltaehkäisevää toimea. Tämä on nähtävissä esimerkiksi siitä, että kansainväliset standardit kuten ISO 27005, vaatii tietoturvatietoisuussuunnitelmaa sekä sen harjoittamista edellytyksenä standardin saamiseen (Alotaibi & Alfehaid, 2018). Myöskin ISO/IEC 27001, joka on standardi tietoturvallisuuden hallintaan organisaatiossa, vaatii, että organisaation työntekijöiden, merkittävien toimittajien sekä kolmansien osapuolien on saatava riittävää tietoisuuskoulutusta, jota ylläpidetään heidän työtehtäväänsä nähden sopivalla säännöllisyydellä. Näiden lisäksi EU:n tietosuoja-asetus eli GDPR (eng. General Data Protection Regulation) vaatii artikla 39 b-kohdassa:

> 1. Tietosuojavastaavalla on oltava ainakin seuraavat tehtävät:
>
> b) seurata, että noudatetaan tätä asetusta, muita unionin tai jäsenvaltion tietosuojalainsäännöksiä ja rekisterinpitäjän tai henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan, mukaan lukien vastuunjako, tiedon lisääminen ja käsittelyyn osallistuvan henkilöstön koulutus ja tähän liittyvät tarkastukset;

Kuten standardeista sekä tietosuoja-asetuksesta pystytään huomaamaan, tietoturvatietoisuus on perustavanlaatuinen vaatimus yrityksen toiminnassa. McIlwraith (2021) myös huomauttaa, että monet toimialat ovat vahvasti reguloituja eli säänneltyjä, kuten finanssiala tai julkinen hallinto ja nämä regulaatiot linkittyvät standardien noudattamiseen, joten tietoturvatietoisuus on ennalta määrättynä jo vaatimus näiden alojen toiminnalle.

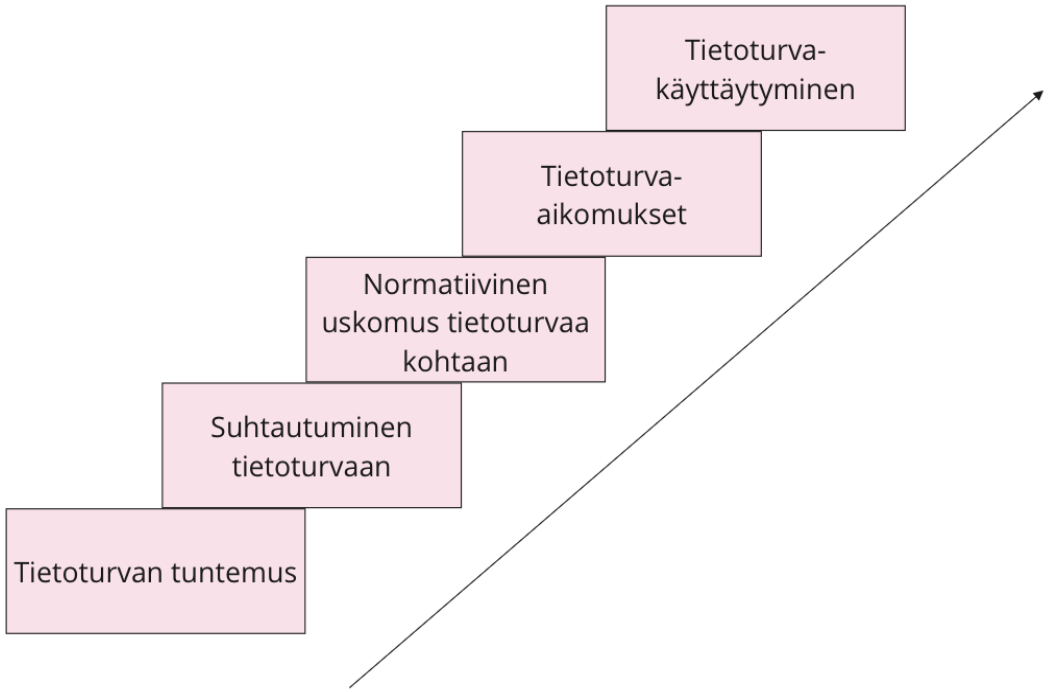
Monien yritysten kohdalla, jotka käsittelevät esimerkiksi henkilötietoja, tietoturvatietoisuus voidaan katsoa osana myös yrityksen kokonaisvaltaista vastuullista toimintaa. Kun tietoisuuteen panostetaan, tehdään samalla toimia järjestelmien turvaamisen eteen, sekä työtä tärkeiden tietojen suojaamiseksi ja luottamuksen säilyttämiseksi. Näillä toimilla tuetaan yhteiskuntaan nähden myös vastuullisesta toimintaa. Lauhia (2022) nostaakin kirjoituksessaan, kuinka tietoturvallisuus liittyy myös sosiaaliseen vastuullisuuteen mm. ESG-tekijöissä (Environmental, Social ja Governance), sillä tietomurrolla voi olla merkittävät seuraukset yksilöön (henkilö- tai potilastietojen vaarantuminen) tai yhteiskuntaan (kriittisen toimen, kuten energianjakelun keskeytyminen).

3.2 Tietoturvatietoisuuden mittaaminen

On merkittävää tiedostaa käyttäytyminen osana tietoturvatietoisuutta ja se, että oikeaoppisen eli tietoturvallisen käyttäytymisen edellytys on, että yksilöllä on kerrytettynä tarvittava tietämys aiheesta. On myös huomattava, että tieto itsessään ei kuitenkaan välttämättä vaikuta suoraan käyttäytymiseen (Khan et al., 2011). Tästä syystä tietoturvatietoisuutta mitattaessa on hyvä ottaa mukaan

käyttäytymiseen perustuvia mittareita, jotta tietoisuuden aito taso pystytään saamaan selville.

Tietoturvallisten toimintatapojen harjoittamisen päätavoitteena on tehdä myönteisiä muutoksia työntekijöiden toimintaan sekä korjata nykyistä malleja, jotta ne olisivat linjassa toivottujen toimintamallien kanssa. Khan ym. (2011) kuitenkin toteavat tutkimuksessaan, että ei voida olettaa, että kaikki työntekijät ovat ymmärtäneet tai noudattavat tietoturvallisia toimintatapoja, vaikka organisaatiossa olisikin pyrkinyt levittämään tietoa. Niinpä he suosittelevat, että tietoisuuden tasoa on hyvä mitata, jotta nähdään, kuinka hyvin eri menetelmät ovat tehonneet. Alla olevasta kuvio 2 nähdään Khan ym. (2011) esittämä viisiportainen tikapuumalli tietoturvatietoisuuden mittaamiseksi.



KUVIO 2 Khan ym. (2021) viisiportainen tikapuumalli tietoturvatietoisuuden mittaamiseen

Tietoturvatietoisuuden mittaaminen tapahtuu useimmiten tietämyksen mittaamisen avulla, mutta lisäksi tarvitaan mittaustekniikoita, jotka keskittyvät työntekijöiden tai käyttäjien käyttäytymiseen (Fertig, Schütz & Weber, 2020). Myös Hänsch ja Benenson (2014) huomioivat tämän osa-alueen heidän kolmiosaisessaan jaossaan tietoturvatietoisuudelle: havainto, suojautuminen ja käyttäytyminen. Havaitseminen määrittelee, että työntekijöiden on tiedettävä olemassa olevat uhat ja osattava tunnistaa ne. Tämän lisäksi työntekijöiden on tiedettävä, miten he voivat suojella itsensä lisäksi myös yritystä näitä uhkia vastaan. Viimeinen osa eli käyttäytyminen kuvaa sitä, että työntekijät tietävät, mitä he voivat tehdä uhkien suhteen. Khan ym. (2011) noudattavat juuri näitä näkökulmia, sillä he huomioivat mallissaan myös tietoturvakäyttäytymisen osana tietoturvatietoisuutta.

Myös Parsons, Calic ja Pattinson (2017) huomasivat, että monet tietoturvatietoisuuden mittaamiseen liittyvät tutkimukset ovat olleet suppeita, keskittyneet vain tietyn aihealueen tietoturvaan tai ne ovat kohdistettu tietoturva-alan

ammattilaisille. Tästä syystä he ovat kehittäneet HAIS-Q kyselyvälineen (Human Aspects of Information Security Questionnaire), joka pyrkii olemaan kokonaisvaltaisempi mittari tietoturvatietoisuuden mittaamiseen. HAIS-Q:n avulla voidaan tarkastella työntekijöiden tietoturvatietoisuutta muusta kuin teknisestä näkökulmasta. HAIS-Q on kyselytutkimus, jota voidaan hyödyntää määrällisissä tutkimuksissa. Tämä tutkimus toteutetaan laadullisena tutkimuksena, jonka takia HAIS-Q:ta ei hyödynnetä.

3.3 Tietoturvatietoisuuden levittämisen keinoja

Tietyillä aloilla vaaditaan vaatimustenmukaisen toiminnan täyttymiseksi tiettyjä koulutuksia, joihin voi kuulua myös vuosittaiset tietoturvakoulutukset (Haney & Lutters, 2017). Osissa yrityksissä on taas yrityksen oman harkinnan mukaista kouluttaa työntekijöilleen tietoturvatietoisuutta. Aloul (2012) suosittelee, että kaikkien yritysten olisi tarjottava työntekijöilleen tietoturvallisuuskoulutusta. Yritysten on hyvä pitää mielessä, että tietoturvatietoisuuden toteuttaminen on pääsääntöisesti edullisempaa, kuin tietoturvaongelman korjaaminen, mikä ei välttämättä ole joka tapauksessa edes mahdollista, sillä pahimmillaan yritys ei toivu tietoturvaloukkauksen seurauksista. Aina yrityksen ei ole helppo panostaa tietoturvaan, sillä se sisältää paljon ennaltaehkäiseviä toimia, joilla ei ole suoria näkyviä säästöjä.

Tutkimuksessa on havaittu, että pelkästään tietoturvatietoisuuskoulutukset, joissa keskitytään vain koulutuksen suorittamiseen tietyllä tavalla eivät riitä tiedon syvälliseen omaksumiseen, vaan koulutukset on muutettava työntekijän käyttäytymiseen vaikuttaviksi ohjelmiksi (Haney & Lutters, 2017).

Tietoturvaa edistäessä viestintätaidot ovat erittäin tärkeitä. Selkeällä viestinnällä työntekijät käsittävät tietoturvan heitä koskevassa kontekstissa, mikä edistää tiedon omaksumista (Haney & Lutters, 2017). Alotaibi ja Alfehaid (2018) suosittelevat tietoturvatietoisuuden sisällön yksinkertaistamista, sillä se auttaa työntekijöitä, koska heidän on helpompi ymmärtää selkeitä tiiviitä kokonaisuuksia. Aloul (2012) myös korostaa, että oikeiden viestintäkanavien käyttö on tärkeää, jotta haluttu kohdeyleisö saadaan saavutettua.

Kun tietoisuutta lähdetään levittämään, on oleellista kohdentaa sisältö työntekijöiden rooliin sopivaksi, jotta tiedotus on asianmukaista. Alotaibi ja Alfehaid (2018) myös suosittelevat, että työntekijöille pitäisi näyttää todellisia esimerkkejä turvallisuuden rikkomisen seurauksista ja antaa työntekijöiden itse peilata näitä ja oppia niistä.

Esteves, Ramalho ja De Haro (2017) kannattavat, että tietoturvatietoisuudesta olisi hyvä luoda osa työntekijöiden jokapäiväistä toimintaa, sekä he kannustavat tekemään tietoturvan tiedottamisesta mielenkiintoista. Yksi keino mielenkiintoisuuden lisäämiseen on ottaa pelillistämistä mukaan tietoisuuden levittämiseen (Haney & Lutters, 2017). Esimerkiksi HoxHunt on yritys, joka tarjoaa inhimillisten riskien harjoitusjärjestelmää, joka yhdistää tuotteessaan tekoälyä yksilöllisten tietojenkalasteluun liittyvien mikrokoulutusten luomiseen.

4 TYÖNTEKIJÄN TIETOTURVAKÄYTTÄYTYMISEEN VAIKUTTAVAT TEKIJÄT

Tässä luvussa esitetään perusteltuihin toimiin perustuva lähestymistapa (Ajzen & Fishbein, 2009) sekä käydään läpi tekijöitä työntekijöiden tietoturvakäyttäytymisen taustalla.

4.1 Yleistä työntekijöiden tietoturvakäyttäytymisestä

Ncubukezi (2022) toteaa tutkimuksessaan, että inhimilliset tietoturvarikkeet ovat seurausta työntekijöiden asenteesta, tietämyksestä ja käyttäytymisestä. Vaikka tietoturvakoulutuksista voi olla apua parantamaan tietoturvallisia toimintatapoja, mittarit, jotka osoittavat koulutuksen suorittaneiden työntekijöiden määrän ovat kovin pinnallisia. Nämä mittarit kertovat vain vähän syvemmistä vaikutuksista: siitä, miten turvallisuuskäyttäytyminen, -ymmärrys ja -asenteet ovat muuttuneet myönteisesti (Haney & Lutters, 2017).

Kun pohditaan tietoturvallisuutta ja sen kehittämistä, on tärkeää pyrkiä ymmärtämään ja ennustamaan työntekijöiden käyttäytymistä, mihin asenteella on suuri vaikutus. On ymmärrettävä ne tavat, jotka vaikuttavat työntekijöiden muodostamaan kuvaan yrityksen turvallisuuskulttuurin käytäntöistä sekä tavat niiden omaksumiseen, jotta pystytään toteuttamaan asianmukaisia toimia tietämyksen parantamiseen. Tämä ei ole uusi havainto, sillä Thomson ja von Solms (1998) pyrkivät selvittämään, kuinka psykologisia periaatteita hyödyntämällä yritykset saisivat tehostettua tietoturvatietoisuusohjelmaa. Toisin sanoen, jotta ihmisten asenteita ja käyttäytymistä pystyy muuttamaan, pitää keksiä keinot suostutella heidät uusiin ajattelu- ja toimintatapoihin.

Kuten todettu, jotta työntekijöiden tietoturvallisuuskäyttäytymistä voidaan tutkia, tulee ymmärtää, mitkä tekijät vaikuttavat työntekijän käyttäytymisen taustalla. Asenteen ja käyttäytymisen suhde ei ole yksiselitteinen, sillä henkilö voi esimerkiksi piilotella omaa asennettaan tilanteissa, joissa se voisi tuottaa hänelle negatiivisia seuraamuksia (Ashenden, 2018). On kuitenkin tunnistettu, että

asenne on positiivisessa yhteydessä aiottuun käyttäytymiseen. Muutkin tekijät kuin asenne vaikuttavat lopulliseen käyttäytymiseen ja ne on hyvä pyrkiä huomioimaan tarkasteltaessa käyttäytymistä (Ajzen & Fishbein, 2009).

Asenteen ja käyttäytymisen välistä suhdetta on tutkittu paljon ja suosituin malli tämän tutkimiseen on Martin Fishbeinin ja Icek Ajzenin vuonna 1967 kehittämä teoria perustellun toiminnan teoriasta. Se perustuu sosiaalipsykologiseen tutkimukseen, suostuttelumalleihin ja asenneteorioihin ja pyrkii selittämään asenteiden ja käyttäytymisen välistä suhdetta ihmisen toiminnassa. Tähän tutkimukseen on valikoitunut Fishbeinin ja Ajzenin perustellun toiminnan teoriaan pohjautuva malli: perusteltuihin toimiin perustuva lähestymistapa (The Reasoned Action Approach).

4.2 Perusteltuihin toimiin perustuva lähestymistapa

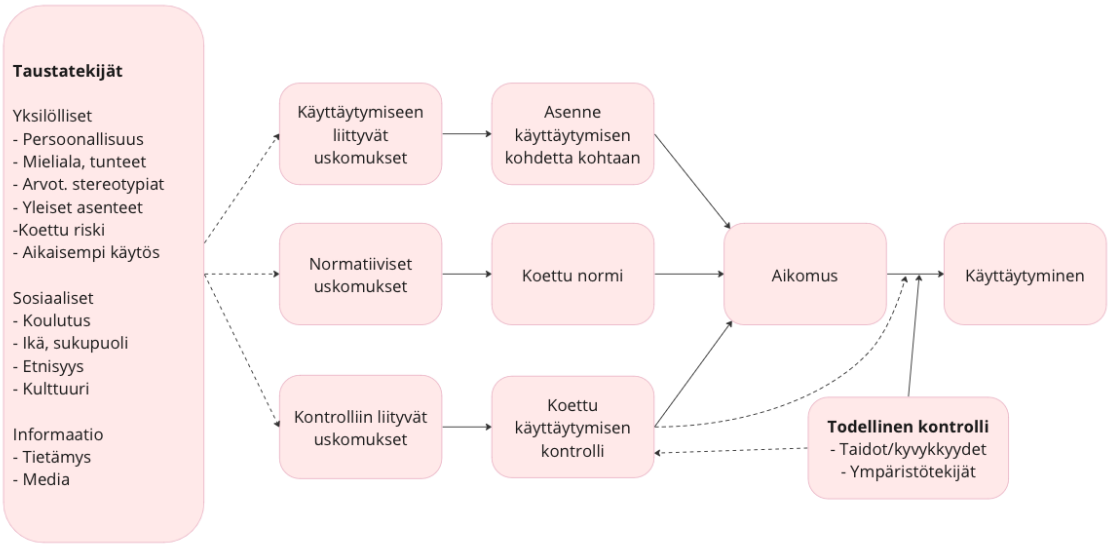
Perusteltuihin toimiin perustuvaa lähestymistapaa käytetään tässä tapauksessa, jotta pystytään ymmärtämään tietoturvallisuuskäyttäytymisen psykologiaa. Jotta mallia voidaan hyödyntää käytännössä, on tärkeää, että tarkasteltava käyttäytyminen on selkeästi tunnistettu ja asianmukaisesti operationalisoitu eli käsitteet ja ideat on muutettu mitattavaksi ilmiöksi (Ajzen & Fishbein, 2009). Tässä tapauksessa tutkimuksessa kiinnostuksen kohde on työntekijöiden tietoturvakäyttäytyminen.

Lähtökohtaisesti on oletettu, että ihmisten sosiaalinen käyttäytyminen on johdonmukaista tai spontaania seurausta tiedoista tai uskomuksista, joita ihmisillä on kohteena olevasta käyttäytymisestä (Ajzen & Fishbein, 2009). Uskomukset, joilla on vaikutusta, voivat olla peräisin monista lähteistä, kuten henkilökohtaisista kokemuksista, muodollisesta koulutuksesta, sosiaalisesta mediasta tai myös vuorovaikutuksesta perheen ja ystävien kanssa. Työympäristössä työkaverit ja työyhteisö ovat merkittäviä vuorovaikuttavia tekijöitä. Ajzen ja Fishbein (2009) toteavat, että erilaisista sosiaalisista taustoista tai erilaisista persoonallisuuspiirteistä tulevat henkilöt eroavat todennäköisesti myös uskomuksissaan. Riippumatta siitä, miten tiettyyn käyttäytymiseen liittyvät uskomukset on hankittu, ne ohjaavat päätöstä toteuttaa tai olla toteuttamatta kyseistä käyttäytymistä. Ajzen ja Fishbein (2009) määrittävät, että uskomuksia voidaan erottaa kolmea tyyppiä:

- Myönteinen tai kielteinen arvio käyttäytymisen suorittamisesta (Käyttäytymiseen liittyvät uskomukset).
- Henkilön kokemien tärkeiden henkilöiden tai ryhmien näkemys käyttäytymisen suorittamiseen eli sosiaalinen paine (Normatiiviset uskomukset).
- Uskomukset henkilökohtaisista ympäristötekijöistä, jotka voivat auttaa tai haitata heidän pyrkimyksiään toteuttaa käyttäytymistä (Kontrollin liittyvät uskomukset).

Nämä uskomukset vaikuttavat suoraan koettuihin tekijöihin. Esimerkiksi jos henkilö kokee, että ympärillä olevat ihmiset paheksuvat salaisten tietojen

jakamista tai eivät itse ikinä jaa salaiseksi luokiteltua tietoa muille, henkilö luultavasti kokee sosiaalista painetta kyseisen käyttäytymismallin harjoittamiseen. Yhdessä asenne käyttäytymisen kohdetta kohtaan, koettu normi ja koettu käyttäytymisen kontrolli johtavat aikomuksen muodostumiseen eli valmiuteen suorittaa käyttäytyminen. Yleisesti ottaen siinä määrin kuin käyttäytymisen suorittamisen koetaan johtavan enemmän myönteisiin kuin kielteisiin tuloksiin, asenne käyttäytymistä kohtaan on pääsääntöisesti suotuisa. Ajzen ja Fishbein (2009) kuitenkin toteavat, että kolmen aikomukseen vaikuttavan tekijän suhteellisen merkityksen tai painoarvon voi kuitenkin vaihdella riippuen käyttäytymisestä toiseen ja henkilöstä toiseen. Kuviossa 3 on kaaviomainen esitys Ajzen ja Fishbein (2009) perustellun toiminnan viitekehyksestä.



KUVIO 3 Ajzen ja Fishbein (2009) perustellun toiminnan viitekehys

Yleisesti ottaen suunnitellun käyttäytymisen teoria selittää sitä, että ihmisillä on taipumus suorittaa tietty käyttäytyminen, jos sitä arvioidaan myönteisesti (asenne käyttäytymistä kohtaan), jos siihen kohdistuu sosiaalista painetta (koettu normi) ja jos he uskovat kykenevänsä suorittamaan sen (koettu käyttäytymisen kontrolli) (Ajzen, 1991). Jotta kuitenkin pystytään ennustamaan ja ymmärtämään käyttäytymistä täydellisesti, Ajzen ja Fishbein (2009) nostavat perusteltuihin toimiin perustuvassa lähestymistavassa esille, että aikomuksen lisäksi on myös arvioitava todellista käyttäytymisen kontrollia. Nimittäin, jos henkilöltä puuttuu tarvittavat taidot ja kyvyt tai jos ympäristö asettaa rajoitteen käyttäytymisen toteuttamiselle, ei henkilö välttämättä pysty suorittamaan aikomuksensa mukaisesti. Henkilöltä voi puuttua todellinen kontrolli käyttäytymisen toteuttamiseen. Tästä syystä perustellun toiminnan viitekehys huomioi todellisen kontrollin vaikuttavana tekijänä käyttäytymiseen, sekä huomioi sen vaikutuksen myös henkilön koettuun käyttäytymisen kontrolliin.

Tässä tutkimuksessa hyödynnetään Ajzen ja Fishbein (2009) perusteltuihin toimiin pohjautuvaa lähestymistavan viitekehystä tutkimuksen empiirisessä osuudessa. Osuus toteutetaan laadullisena tutkimuksena, jonka takia viitekehystä ei hyödynnetä kokonaisuudessaan, vaan niiltä osin, kuin se nousee

tutkimuksessa esille. Keskiössä ovat viitekehyksen kolme käyttäytymiseen vaikuttavaa tekijää: asenne käyttäytymistä kohtaan, koettu normi ja koettu käyttäytymisen kontrolli sekä näiden taustalla vaikuttavat uskomukset. Valittujen osien pohjalta muodostetaan haastatteluissa käsiteltävät teemat, joita tuloksissa myöhemmin analysoidaan. Tutkimuksessa huomioidaan myös todellinen kontrolli vaikuttavana tekijänä, sillä tietoturvassa esimerkiksi tietämättömyys on tunnistetusti rajoittava tekijä. Tämä todellinen kontrolli sisällytetään tutkimuksen haastatteluissa kontrolliin liittyvään kokonaisuuteen.

4.3 Tekijöitä työntekijöiden tietoturvalliseen käyttäytymisen taustalla

Kuten kuviosta 3 olevasta viitekehyksestä kävi ilmi, henkilön käyttäytymisen taustalla voi olla vaikuttamassa lukuisia taustatekijöitä. Taustatekijät voivat olla kulttuurista omaksuttuja tai yleisen ilmapiirin luomaa vaikutusta. Ashenden (2018) nostaa tutkimuksessaan esille, että riippumatta siitä, pyritäänkö lisäämään työntekijöiden tietoisuutta tai muuttamaan heidän käyttäytymistään, on ensin ymmärrettävä, miksi työntekijät ajattelevat tällä hetkellä niin kuin ajattelevat, ennen kuin toimenpiteitä aletaan suunnitella.

Caldwell (2016) nostaa esille, että persoonallisuuspiirteet saattavat tehdä joistakin henkilöistä alttiimpia tietoturvaloukkauksille kuin toisista, sillä yksi kriittinen ihmisen ominaisuus on kognitiivinen pohdinta. Se määrittää, kuinka hyvin henkilö analysoi ja käsittelee yksityiskohtia sen sijaan, että hän uskoisi vain vaistoonsa. Mitä analyyttisempi henkilö on, sitä vähemmän hän on esimerkiksi altis arkaluonteisten tietoturvatietojen keräämiseen tarkoitetuille epäilyttäville sähköpostiviesteille.

Persoonallisuuden lisäksi muita tekijöitä ovat henkilön omat kokemukset. Ashenden (2018) nostaa esille, että jos työntekijällä ei ole henkilökohtaisella tasolla tai työn kautta kokemusta tietoturvasta tai tietojen suojaamisesta, hänellä ei luultavasti ole voimakkaita asenteita tietoturvaa kohtaan. Puolestaan, jos henkilö on henkilökohtaisesti tai joku hänen lähipiiristään on joutunut tietoturvatapauksen uhriksi, asenne on todennäköisesti voimakkaampi, sillä heillä on suoraa kokemusta aiheesta.

Vaikka henkilön asenne tietoturvaa kohtaan ei olisi merkittävä, voi tieto siitä, että tietoturvan laiminlyönnistä saa mahdollisia seurauksia luoda ilmapiiriä sosiaalisesti suotuisista toimista (Ashenden, 2018). Eli toisin sanoen pelko seurauksista on suurempi kuin koettu hyöty väärästä toiminnasta.

Amankwa, Loock ja Kritzinger (2022) huomasivat tutkimuksessaan, että tietoturvassa tilivelvollisuus eli mahdollinen tarve perustella oma käyttäytyminen, jonka kautta lopputuloksiin on päädytty toiselle osapuolelle, jolla on valtuus tuomita toinen teon mahdollisista seurauksista, on merkittävä motiivi toimia tietoturvallisesti. Tämä osa-alue on huomioitu myös Ajzen ja Fishbein (2009) perustellun toiminnan viitekehyksessä kohdassa “Koettu käyttäytymisen kontrolli”. Kirjallisuudessa liittyen työntekijöiden tilivelvollisuuteen ehdotetaan neljää

keskeistä toimea, joilla pystytään edistämään vastuullisuuden tuntua työntekijässä (Amankwa, Loock & Kritzinger, 2022):

- Tunnistettavuus eli yksilön toimet pystytään liittämään häneen tavalla, jota ei voi kieltää.
- Arvioinnin odotukset kuvaavat ennakointia siitä, että eri ryhmä arvioi yksilön toimia joidenkin standardoitujen periaatteiden mukaisesti ja tietyin sanattomin seurauksin.
- Tietoisuus seurannasta eli ajatus siitä, että henkilön työskentelyä tietojärjestelmien parissa seurataan.
- Tietoisuus sosiaalisesta läsnäolosta määrittelee tiedon muiden yksilöiden olemassaolosta.

Amankwa, Loock ja Kritzinger (2022) kuitenkin toteavat, että yksittäisellä toimella ei ole merkittävää vaikutusta työntekijän asenteisiin ja aikomuksiin, mutta kun kaikki keskeiset toimet ovat käytössä tämä luo työntekijälle painetta toimia tietoturvallisesti.

Voidaan siis huomata, että henkilön käyttäytymisen taustalla voi olla vaikuttamassa monia tekijöitä rinnakkain. Henkilön omalla kognitiivisen pohdinnan taidoilla on merkitystä, mutta myös henkilön omilla kokemuksilla on vaikutusta. Näiden rinnalla myös mahdollinen tarve perustella oma toiminta vaikuttaa tietoturvallisen käyttäytymisen.

5 TUTKIMUKSEN TOTEUTUS

Tässä luvussa tarkastellaan, miten tämän tutkielman empiirinen osuus on toteutettu. Luku on jaoteltu kolmeen alalukuun ja ne etenevät seuraavasti: Luvussa 5.1 esitellään tutkimusmenetelmä ja sen valintaan vaikuttaneet tekijät. Luvussa 5.2 käydään läpi tarkemmin tutkimusprosessia ja perehdytään aineiston keruuseen sekä lopuksi luvussa 5.3 sen pohjalta tehtyyn analyysiin ja menetelmiin.

5.1 Tutkimusmenetelmä

Empiirinen osuus tutkimuksessa toteutetaan yleisesti kahdella tavalla: määrällisenä eli kvantitatiivisena tutkimuksena tai laadullisena eli kvalitatiivisena tutkimuksena. Vilkka (2007) mukaan kvantitatiivisessa tutkimuksessa tyypillistä on suuri vastaajamäärä, jonka kautta pyritään antamaan yleiskuva mitattujen asioiden suhteista ja eroista. Kvalitatiivisessa tutkimuksessa puolestaan painottuu merkityksien tutkiminen ja pyrkimys ymmärtää syvemmin tutkittavissa olevaa asiaa (Saaranen-Kauppinen & Puusniekka, 2006). Laadulliseen tutkimukseen aineiston määrään ei ole olemassa tiettyä sääntöä vaan siinä korostuu aineiston laatu, sillä keskiössä on ilmiön ymmärtäminen, ei tilastollisten yhteyksien etsintä (Saaranen-Kauppinen & Puusniekka, 2006). Aineiston määrä laadullisessa tutkimuksessa voi olla pieni, jos se on laadukas. Tähän tutkimukseen aineistoa lähdettiin keräämään laadullisen menetelmän kautta.

Haastattelut ovat yleinen tapa tutkimusaineiston luomiseksi, sillä haastattelussa ollaan suoraan vuorovaikutuksessa tutkittavan eli haastateltavan kanssa ja tutkija saa mahdollisuuden kysyä suoraan ihmisten toiminnasta ja käsityksistä (Hirsjärvi & Hurme 2001). Haastattelu voi kohdistua yksilöön tai ryhmään ja haastattelu voidaan jakaa sen järjestelmällisyyden eli strukturoinnin mukaan: strukturoimaton haastattelu, puolistrukturoitu haastattelu tai teemahaastattelu ja strukturoitu haastattelu. Haastattelut ovat erittäin suosittuja tiedonkeruun muotoja, sillä ne ovat joustavia ja ne sopivat monenlaisiin tutkimustarkoituksiin.

Usein tutkimuskysymykset ratkaisevat tutkimusmenetelmän valinnan, sillä esimerkiksi puolistrukturoitu haastattelu sopii tilanteisiin, joissa halutaan

tietoa juuri tietyistä asioista ja painotus on "mitä-" ja "miten-" kysymyksissä (Hyvärinen, Suoninen & Vuori, 2021). Tähän tutkimukseen valikoitui teemahaastattelu aineiston keruu- ja analysointimenetelmäksi. Teemahaastattelu ei noudata yksityiskohtaisia ja tarkasti valmiiksi muotoiltuja kysymyksiä, vaan haastattelussa on avoimempi ilmapiiri, joka keskittyy ennalta suunniteltuihin teemoihin (Hirsjärvi & Hurme 2001). Haastattelija voi kysyä kysymykset vapaasti valitusta teemasta eikä kysymyksiä välttämättä esitetä kaikille haastateltaville samassa muodossa tai samassa järjestyksessä. On huomattava, että vaikka teemahaastattelussa haastattelut voivat liikkua joustavasti, se on kuitenkin jäsennetympi kuin kokonaan avoin haastattelu, koska siinä on valmiit aihepiirit eli teemat, jotka on luotu aiempien tutkimusten tutustumisen pohjalta (Hirsjärvi & Hurme 2001).

Tutkijalta teemahaastattelu vaatii aihepiiriin huolellista perehtymistä sekä kykyä johdatella haastattelutilannetta niin, että haastattelu kohdistuu juuri haluttuihin teemoihin, joista keskustellaan (Saaranen-Kauppinen & Puusniekka, 2006). Teemahaastattelussa ei tarvita yhteistä kokemusta, josta keskustelua lähdetään edistämään vaan siinä haastateltavan elämysmaailma on etusijalla ja kiinnostus on yksilön omissa tunteissa, kokemuksissa, uskomuksissa ja ajatuksissa. Teemahaastattelusta voidaan usein käyttää myös nimitystä puolistrukturoitu haastattelu, koska esimerkiksi englanniksi ei tunneta käsitettä teemahaastattelu (Saaranen-Kauppinen & Puusniekka, 2006). Hirsjärvi ja Hurme (2001) luokittelevatkin teemahaastattelun kuuluvan osaksi puolistrukturoituun menetelmään, koska siinä yksi haastattelun näkökulma on kaikille sama eli haastattelussa käsiteltävät aihepiirit. Puolistrukturoidussa haastattelussa aiheet, joita haastattelutilanteessa hyödynnetään, on etukäteen suunniteltu ja haastattelijan vastuulla on varmistaa, että kaikki haastatteluun osallistuvat ymmärtävät kysymykset yhtenäisesti, jotta tulokset ovat luotettavia ja verrattavissa.

Tässä tutkimuksessa painopiste on työntekijöiden tietoturvakäyttäytymiseen vaikuttavissa tekijöissä. Teemahaastattelu sopii tähän, sillä sen kautta voidaan mahdollisesti ymmärtää jokaisen haastateltavan omaa näkemystä kyseiseen asiaan, kun vastaamisessa on vapaus antaa haastateltavien puhua (Saaranen-Kauppinen & Puusniekka, 2006). Rubin ja Rubin (2011) nostavat haastatteluiden eduksi myös sen, että tulokset ovat yleensä helposti ymmärrettäviä ja käyttökelpoisia. Haasteena kuitenkin on, että haastattelut ovat aikaa vieviä ja vaativat tutkijalta taitoa kuunnella ja tulkita vastauksia oikein.

5.2 Aineiston keruu

Laadullisessa tutkimuksessa tavoitteena on saada selville vastaajan kokemuksia ja näkökulmia aiheista. Tästä syystä kysymysten on tärkeitä olla tarpeeksi laajoja, jotta niitä varten pitää työstää ajatuksenkulkua, eikä vastaus pysty olemaan pelkästään "kyllä" tai "ei" vaan vastaukset vaativat vastaajan puolelta enemmän pohdintaa. Toinen tärkeä huomio on pitää kysymykset sellaisina, että ne eivät sisällä mitään varausta, jotta vastaajaa ei johdeta vastauksessa tiettyyn suuntaan. Tämä on erittäin tärkeää varsinkin käsiteltäessä arkaluonteisia aiheita.

Haastattelun kysymysten rakenteessa hyödynnettiin Hyvärinen, Suoninen ja Vuori (2021) ohjetta puolistrukturoidun haastattelun muodostamiselle:

- Ensimmäisten kysymyksien on hyvä olla laajoja, jotta vastaaja saadaan rentoutumaan ja ajatuksen kulku sekä keskustelu käyntiin.
- Haastattelun puolivälissä siirrytään tarkempiin kysymyksiin ja sitä kautta vastaajalta pyritään saamaan tarkempia vastauksia tutkimuksen aiheeseen liittyen.
- Lopuksi vielä pyritään saamaan vastaus avoimeksi jääneisiin kohtiin ja tehdään tarkentavia kysymyksiä.

Haastattelun pääteemat johdattelivat Ajzen ja Fishbein (2009) perustellun toiminnan viitekehyksestä nostettuja uskomuksia, joita käyttäytymisen taustalla voi vaikuttaa. Valittuja teemoja oli kolme ja ne olivat haastateltavan koettu kontrolli, haastateltavan käsitys aiheesta ja yleinen asenne, sekä viimeisenä aiheena oli haastateltavan koettu normi. Koetussa kontrollissa käsiteltiin omaan osaamiseen liittyviä rajoitteita niin atk-laitteiden suhteen kuin itse tietoturvaosaamiseen. Seuraavassa teemassa pyrittiin selvittämään haastateltavan yleistä asennetta tietoturvaa kohtaan ja käsityksiä tietoturvaan liittyen. Viimeisenä vielä käsiteltiin, miten lähellä olevien ihmisten toimet vaikuttavat tietoturva suhtautumiseen. Haastattelussa käytiin tiiviit määritelmät käsitteistä, jotta tutkija ja haastattelija olivat samalla aaltopituudella. Haastattelu keskittyi teemoihin sekä niitä tukeviin haastattelukysymyksiin.

Tutkimusaineiston keruussa hyödynnettiin Saaranen-Kauppinen ja Puusniekka (2006) mainitsemaa lumipallotekniikkaa eli haastateltavia lähdettiin etsimään olemassa olevien kontaktien kautta kysyen osallistujilta vinkkejä muista kiinnostuneista ja soveltuvista osanottajista. Tutkimukseen osallistuminen oli vapaaehtoista ja haastateltavilta pyydettiin lupa tutkimuksen suorittamiseen. Tutkimusta varten haastateltiin lopulta kuutta eri ammateissa työskentelevää henkilöä.

Jotta pystyttiin varmistumaan haastateltavien sopivuudesta liittyen tietoturvakäyttäytymisen tutkimukseen, haastateltaville oli muutamia kriteereitä. Kriteereitä haastateltavien valitsemiselle oli, että heidän oli oltava haastatteluhetkellä vakituisessa tai pitkäaikaisessa työsuhteessa, sekä että heillä on kiinnostusta osallistua tutkimukseen ja halu keskustella avoimesti omista näkemyksistään. Haastateltavien oli oltava jossain yrityksessä työsuhteessa, sillä kiinnostuksen kohteena oli yritysten työntekijät. Haastateltavien oli myös käytettävä työssään omaa työasemaa sekä haastateltavan työn piti olla luonteeltaan sellainen, että tietoturvalla oli siinä merkitystä eli haastateltava pääsi esimerkiksi työssään sensitiivisen tietoon käsiksi tai toimi yrityksen kriittisen järjestelmän parissa. Kaikki haastatteluun valitut henkilöt työskentelivät aloilla ja työtehtävissä joissa edellä mainitut vaatimukset täyttyivät.

Haastattelut ajoittuivat kevääseen 2024 ja ne toteutettiin osaksi kasvotusten ja osaksi videopuhelun välityksellä. Kaikki haastattelut toteutettiin tiloissa, jotka olivat hiljaisia ja rauhallisia, jotta vältyttiin ulkopuolisilta häiriötekijöiltä. Haastattelut kestivät noin puolesta tunnista melkein tuntiin. Aluksi käytiin rauhassa läpi tutkimuksen aihe ja tulevat teeman sekä haastattelun luonne. Tämän jälkeen

käynnistettiin nauhoitus, jossa alkuun kysyttiin haastateltavasta muutamia tietoja, kuitenkin niin, että anonymiteetti säilyi. Tämän jälkeen haastatteluosuus alkoi. Haastattelun lopuksi osallistujilla oli vielä mahdollisuus kysyä itse tutkimuksesta lisää, jos heillä oli siihen liittyen kiinnostusta. Haastattelutilanteessa kaikilta osallistujilta kysyttiin samat pääkysymykset, joihin he saivat kertoa omista kokemuksistaan ja näkemyksistään vapaasti. Haastattelija kysyi tarvittaessa lisäkysymyksiä, jos vastaus jäi pintapuoliseksi. Haastatteluissa käytetty runko on liitteenä tutkimuksen lopussa (liite 1).

5.3 Aineiston analysointi

Teemahaastattelun analysoinnissa yleisesti pyritään löytämään käydyistä haastatteluista toistuvia teemoja ja tulkintoja, joita peilataan johonkin koottuun viitekehykseen sekä teemoihin, joita sen yhteydessä on noussut esille (Hirsjärvi & Hurme, 2008). Tässä tutkimuksessa aineistoa lähdettiin analysoimaan juuri tätä teemahaastattelulle tyypillistä menetelmää hyödyntäen.

Kerätyn aineiston analysoiminen aloitettiin jo haastatteluvaiheessa, kun haastattelija esitti haastateltavalle keskustelun aikana tarkentavia kysymyksiä ja auttoi näin ohjaamaan haastattelua tiettyjen tunnistettujen teemojen suuntaan. Kunkin yksittäisen haastattelun jälkeen haastattelusta puhtaaksikirjoitettiin, eli litteroitiin. Tämä tehtiin käyttäen hyväksi mobiilipohjaista ohjelmaa nimeltä Transkriptor. Ohjelma kirjoitti molempien osapuolten, haastateltavan ja haastattelijan (tutkijan), haastattelut melkein sanatarkasti puhtaaksi. Kun ohjelma oli tehnyt automaattisen transkription, tutkija tarkisti tuloksena syntyneen tekstin ja teki tarvittavat korjaukset, kuten korjasi oikeat sanamuodot tai automaation väärin ymmärtämät sanat. Puhtaaksikirjoitus pyrittiin tekemään sanatarkasti, mutta siitä jätettiin pois kaikki ylimääräiset äännähdykset.

Kun kaikki aineisto oli kerätty ja puhtaaksikirjoitettu. Aineisto yhdistettiin ja sitä alettiin läpikäydä ja tarkastella, minkä aikana haastattelut värikoodattiin haastattelussa käytyjen yleisten teemojen mukaan. Tuloksena oli 100 sivua aineistoa. Aineiston käsittelyvaiheessa haastateltavien taustatiedot koottiin taulukkoon (Taulukko 2), jossa haastateltavaan viitataan kirjaimella H ja sen perässä olevalla haastattelunumerolla. Vastaukset pidetään anonyyminä, jonka takia haastateltavien nimiä ei mainita.

TAULUKKO 2 Haastateltavien tiedot

Haastateltava	Ikä	Ammatti	Toimiala
H1	28	Tietoturva-asiantuntija	Finanssiala
H2	25	IAM-asiantuntija	Finanssiala
H3	59	Työfysioterapeutti	Työterveyshuolto
H4	24	IT-konsultti	Vakuutus- ja eläkepuoli
H5	30	Ohjelmistokehittäjä	Media-ala
H6	62	Röntgenhoitaja	Hoitoala

Kun haastattelut oli yhdistetty, järjestelty ja värikoodattu, aineistoa alettiin analysoida ja sieltä nostettiin havaintoja esille rinnastamalla näkökulmia ja kokemuksia yhteen, joita käsiteltävien teemojen sisällä oli noussut. Havaintojen perustelemiseen käytettiin hyväksi lainauksia aineistosta eli käydyistä haastatteluista. Käytetyt lainaukset on tiivistetty lukijaystävällisempään muotoon karsimalla lauseista toistuvia sisällölle epäoleellisia sanoja kuten “tuota”, “niin päin pois” tai “niinkun”. Lainauksissa on myös hyödynnetty merkintää [...] ilmaisemaan kyseiseen aiheeseen liittymätöntä tietoa, joka on jätetty nostosta pois. Lauseet, jotka ovat jääneet kesken lainauksen välissä, ilmaistaan kolmella pisteellä.

6 TULOKSET

Työntekijöiden henkilökohtainen kyberturvallisuuskulttuuri Da Veigan (2016) mukaan ulottuu niin henkilön työelämään, mutta myös vapaa-aikaan eli henkilökohtaiseen elämään. Singh (2016) myös nostaa esille, kuinka vapaa-ajan toimilla, kuten sosiaalisen median käytöllä on vaikutusta henkilön tietoturvaan, sillä sitä kautta saatuja tietoja voi hyödyntää mm. kalasteluhyökkäyksiin. Tutkimuksessa käsiteltiin haastateltavien tietoturvanäkemyksiä ja -toimintatapoja niin työkontekstissa, mutta myös sivuten vapaa-ajan toimia, sillä tutkimuksessa on oletus, että työ- ja vapaa-ajan tietoturvatoimet eivät ole kaksi täysin irrallista tekijää, vaan niillä on vaikutusta toisiinsa. Tavoitteena oli selvittää tietoturvatoimintatapojen vaikuttavia taustatekijöitä monipuolisesti esimerkiksi yleisen ilmapiirin tai henkilökohtaisten kokemusten kautta. Tavoitteena oli tunnistaa mahdollisia erottavia tai yhdistäviä tekijöitä haastateltavien näkemyksiin, jotka vaikuttavat heidän tietoturvakäyttäytymiseensä.

Tässä luvussa keskitytään tarkastelemaan ja analysoimaan aineistoa heijastaen sitä valitun viitekehyksen kanssa. Tutkimuksessa tunnistetaan, että perustellun toiminnan viitekehys ei täysin istu laadulliseen teemahaastatteluun, jonka takia sitä käytetään enemmän tukena, johon havaintoja peilataan. Tulosten teemojen kannalta tuloksien analysoinnissa on päädytty jakamaan haastattelut kolmeen osaan. 6.1 Koettu kontrolli, 6.2 Yleinen asenne ja 6.3 Koettu normia tarkastelevaan teemaan.

6.1 Koettu kontrolli

Haastattelut etenivät teemoittain ja ensimmäinen teema käsitteli haastateltavan koettua kontrollia. Perustellun toiminnan viitekehys huomioi todellisen kontrollin vaikuttavana tekijänä käyttäytymiseen (Ajzen & Fishbein, 2009). Todelliseen kontrolliin voi vaikuttaa ulkopuolisten kontrollien ohella toimea varten tarvittavat taidot ja kyvykkyydet, sillä ne ovat edellytys toiminnan onnistumiselle. Tätä näkökulmaa hyödynnettiin haastatteluissa kartoittaessa kokemuksia kontrollista.

Koska tietoturva liittyy vahvasti tietotekniseen osaamiseen niin, tutkimuksessa aluksi selvitettiin henkilöiden atk-laitteiden käytön osaamista. Atk-laitteilla haastattelussa viitattiin niin tietokoneisiin ja puhelimiin, kuin haastateltavien käyttämiin järjestelmiin. Kaikki haastateltavista kokivat oman atk-osaamisensa olevan hyvällä tai ainakin omaa työtehtävää nähden tarvittavalla tasolla. Vastauksissa tuli myös ilmi, että vastaajilla on tarvittaessa halukkuutta lähteä kehittämään omaa osaamistaan, jos se tulee esteeksi työn tai tarvittavan toimen suorittamiselle.

> No, mä koen, että mulla on ihan ok osaaminen. Mä tiedän, että mä en esimerkiksi tietokoneista ihan kaikkea syvällisintä osaa, mutta semmoinen peruskäyttö musta tuntuu, että mulla on hallussa ja mä kyllä sitten tarvittaessa esimerkiksi Googlaan tai etsin tietoa, jos mä tiedän tavallaan, että on olemassa joku ominaisuus, mut mä en vaan osaa käyttää sitä. -H2

> Mä luulen, että mun atk-osaaminen on riittävä tähän mun työhön nähden. [...] meillä on aina tällaiset koulutukset, kun otetaan uusia ohjelmistoja käsiteltäväksi ja käyttöön niin siellä on mahdollista myöskin saada lisää yksilöopetusta, jos on tarve. -H3

Samaa teemaa käsiteltäessä myös pyrittiin selvittämään, miten henkilöt kokivat heidän oman tietoturvaosaamisen tason olevan. Kyseisessä vastauksessa ilmeni hieman eroja, sillä osa koki työnantajan vuosittaisten pakollisten koulutusten olevan suora edellytys siihen, että oma tietoturvaosaaminen on työn kontekstissa tarvittavalla tasolla, eli suoritettuaan koulutukset on tehnyt osaltaan tarpeellisen tietoturvan oppimisen eteen.

> Mä luulen, että se on tällä hetkellä kohtalaisella. Meillä on joka vuosi työpaikalla tällainen tietoturvakoulutus, ja siinä on myöskin tällainen kysely, josta täytyy selvitä. Mulla on joka kerta mennyt se ekalla kerralla läpi [...] -H3

Osa vastaajista taas näki tietoturvan suurempana kokonaisuutena, mikä ulottuu oman työroolin ulkopuolelle. Tässä oman osaamisen vertauskohde oli tietoturvaa työtä tekeviin henkilöihin, jolloin tunnistettiin omassa osaamisessa puutteita. Oma osaaminen silti nähtiin olevan kohtalaisella tasolla ainakin perusteiden osalta.

> Silleen basic taso. Mulla on kuitenkin perustietämys ihan kunnossa, mutta en mä mikään tietoturvan ammattilainen ole. -H4

Conetta (2019) nostaa, että pelkkä kyky käyttää tieto- ja viestintätekniikkaa sujuvasti ei yksinään kuitenkaan lisää tietoturvaosaamista tai viittaa, että henkilöllä on hyvä tietämys tietoturvasta, vaan oleellista myös on, että henkilö on tietoinen tietoturvalinjauksista sekä ohjeista, ja osaa noudattaa oikeita ohjeita tietoturvaan liittyen. Tästä syystä haastattelun ensimmäistä teemaa eli kontrollia käsiteltäessä haastattelijoilta tiedusteltiin myös, miten he toimisivat tilanteessa, jos he havaitsisivat tietoturvapoikkeaman.

Kaikissa vastauksissa korostui selvästi, että poikkeamista ilmoitettaisiin joko yrityksen järjestelmään tai jollekin vastuuhenkilölle. Yksi vastaajista H1,

joka teki tietoturvaa ammatikseen ja hänellä oli kokemusta aiheesta, otti erityisesti esiin, että hän toimisi aina sen työnantajayrityksen linjausten ja prosessien mukaan, minkä kautta ilmoittaisi poikkeamat eteenpäin. Kuitenkin osalla esiintyi hieman epävarmuutta osaisiko poikkeaman tunnistaa, sillä tällaisista tietoturvapoikkeavuuksien havaitsemisista ei ollut kokemusta. Tämä ei kuitenkaan poissulkenut, etteikö havaintoa tuotaisi esille, jos sellainen tulisi vastaan.

Kontrolliin voi osaamattomuuden lisäksi kuulua rajoitukset ja valvonta. Amankwa, Loock ja Kritzinger (2022) sekä myös Ajzen ja Fishbein (2009) nostavat esille, että motiivina toimia tietyllä tavalla, tässä tapauksessa tietoturvallisesti, voi vaikuttaa tieto, että omia tekojaan joutuu perustelemaan sekä se, että teoistaan on tilivelvollinen. Haastateltavat eivät kuitenkaan kokeneet suuresti tämän ulkopuolelta tulevan kontrollin vaikuttavat heidän toimiinsa, sillä he näkivät tietoturvaan liittyvät kontrollit, kuten seurannan, arkipäiväisinä asioina, joita ei oikeastaan tule edes mietittyä. Kaikki haastateltavat tiedostivat, että heidän toimiaan työnantajan työasemalla seurataan, mutta he eivät kokeneet tätä epäluottamuksena työnantajan puolelta vaan pikemminkin tarpeellisena varmistuksena, että väärinkäyttöä ei tapahdu. Osa koki myös työnantajan puolelta tietoturvaan liittyvät kontrollit hyviksi, sillä ne ohjaavat työntekijöitä toimintaan oikeaan suuntaan, jolloin tavallaan oikeat toimintatavat juurtuvat käyttöön.

> No, mä koen, että työntekijään luotetaan, mutta sitten koska tavallaan ollaan niin reguloidulla alalla, niin totta kai siellä pitää olla semmoisia tsekkejä lähtökohtaisestikin kun tehdään tietoturvaa, että tehdään esimerkiksi tietoturvallisia palveluita asiakkaille [...] vahvistetaan, että ne asiat on miten niiden pitää. -H1

6.2 Yleinen asenne

Haastattelun seuraava teema liittyi käyttäytymiseen liittyviin uskomuksiin eli haastateltavien omaan käsitykseen aiheesta. Kaikille haastateltaville tietoturva oli suhteellisen tuttu asia, ja kaikki kuvailivat tietoturvaa osittain samantyyppisesti. Osa oli itsevarmempia tuodessaan esiin näkökulmia ja kuvaillessaan, mitä tietoturva tarkoittaa, mutta loppujen lopuksi melkein kaikissa näkemyksissä korostui tietoturvan kolme pilaria eli luottamuksellisuus, eheys ja saatavuus tai edes osia kyseisestä kokonaisuudesta (Smaonas & Coss, 2014).

> [...] pidetään kaikki tiedot suojassa, että vain tarvittavat ihmiset pääsevät niihin. Koen, että siihen tietoturvaan liittyy myös oma aktiivisuus. Jokaisen tekemisillä on vaikutus siihen, että pyritään pitämään kokonaisuus eheänä [...] - H2

> Kaikki asiakastiedot, joita mä kirjaan, niin ne on luottamuksellisia ja on tärkeää, että ne ei päädy väärin käsiin. Eikä myöskään ihmisille tai työntekijöille, joilla ei ole asiakkaan kanssa, niin he eivät pääse katsomaan asiakkaan tietoja [...] - H3

> Mulle tietoturva tarkoittaa mun mielestä tiedon eheyttä ja luotettavuutta ja sitä, että se saadaan turvattua, että se ei häviä myöskään. […] Jos on jotain asiakkaita tai muita sidosryhmiä, niin kaikki me pystytään luottaa siihen, että tieto säilyy ja on saatavilla silloin, kun me sitä tarvitaan. -H5

Tietoturvan tekniset ratkaisut ovat inhimillisten toimien ohella tärkeitä ja ne ovatkin olleet usein keskiössä puhuttaessa tietoturvasta (Khando ym., 2021). Osa haastateltavista nostikin esille tekniset ratkaisut kuvaillessaan tietoturvaa. Esimerkiksi työasemien säännölliset päivitykset tai salasanavaatimukset olivat tekijöitä, jotka nousivat positiivisina asioina esille. Kaikki haastateltavat näkivät oman organisaationsa tietoturvan toimivana ja heillä oli luotto, että organisaation tietoturva on kunnossa.

> Tietoturvaa päivitetään jatkuvasti, eli meillä päivitetään koneita ja sitä kautta tietoturva on kehittynyt vuosia varmasti. -H3

Tekniset ratkaisut nousivat monella kuitenkin myöhemmin haastattelussa esille, vaikka niitä ei tietoturvaa kuvaillessa olisi esitellyt. Etätyöskentelyssä mm. VPN nähtiin tärkeänä asiana, jolla työnantaja pyrkii suojaamaan työaseman turvallisuutta ja sitä käytettiin mielellään. Myös käyttöoikeuksienhallintajärjestelmät nähtiin positiivisena asiana, eikä mitenkään työtä rajoittavana tekijänä.

> Muuten perusasiat (yrityksen tietoturvassa) on mun mielestä ihan hyvällä mallilla, että käytetään VPN:ää, ja kaikki on tavallaan silleen suljettujen ovien takana, mitkä pitääkin olla. Oikeuksista pidetään huolta, että henkilöillä ole mitään ylimääräisiä oikeuksia mihinkään palveluihin tai mihinkään tietoon, mitä ne ei itse työssä tarvitse. -H5

Varsinkin iäkkäämmät haastateltavat näkivät työpaikan työaseman todella turvallisena. Turvallisempana kuin henkilökohtaiset laitteet, ja heillä oli oletus, että työpaikan tietokoneessa on suojaukset niin korkealla, että sillä ei ole edes mahdollista päästä haitallisille sivuille. Tästä syystä he myös käyttivät työpaikan työasemaa omien pankkiasioidensa hoitamiseen. Tähän toimeen oli annettu aikanaan lupa, kun tietokoneet olivat tulleet käyttöön, mutta jäi epäselväksi, oliko vielä kyseinen lupa voimassa.

> Mähän hoidan sillä kaikki pankki asiani ja näin. On annettu lupa, että saa hoitaa pankkiasioita. Sitten kun alkoi tulemaan tietokoneet, niin kannustettiinkin, että niillä voi hoitaa omia pankkiasioita. -H6

Kyseisessä näkökulmassa oli selvä ero nuorempiin haastateltaviin, sillä he näkivät työpaikan työaseman olevat lähtökohtaisesti pelkästään vain työn tekemiseen ja vapaa-ajan toimet hoidetaan henkilökohtaisilla laitteilla. Työhön ja vapaa-aikaan tarkoitettujen laitteiden välillä oli selkeä ero, kuten myös Singh (2016) suosittelee. Varsinkin, jos netistä pitää ladata jotain niin tiedostettiin, ettei siihen voi käyttää työpaikan työasemaa.

> [...] ettei ala tallentelemaan mitään netistä tai ettei käytä työpaikan työasemaa muuhun lähtökohtaisesti kuin sitten sen työn tekemiseen. -H1

Ashenden (2018) selvitti tutkimuksessaan, että henkilön omilla tai hänen lähipiirinsä kokemuksilla tietoturvaan, esimerkiksi tietoturvahyökkäyksen uhriksi joutuminen, on vaikutusta tietoturvaan kohdistuvaan asenteeseen. Haastatteluissa nousi esille, että haastattelijoiden omat kokemukset tietoturvahyökkäyksistä ovat vaikuttaneet heidän toimintaansa ja lisänneet käsitystä, miten erilaisia hyökkäyksiä on olemassa ja niiden seurauksista. Vaikka kaikilla osallistujilla oli tietty suhtautuminen tietoturvaan tärkeänä asiana, henkilöt, joilla oli omaa henkilökohtaista kokemusta tietoturvahyökkäyksestä, suhtautuivat tietoturvaan tietyllä vakavuudella.

> Mä koen, että sitten tavallaan niitä uhkia voi tulla hieman eri tasoilla, mutta sitten tällaisessa normaali käyttäytymisessä, niin se voi olla sitten sitä kalastelua, mikä saattaa tulla sähköpostiin tai voi olla joku yksittäinen tapaus, kuin että joku yrittää murtautua mun tilille. [...] Joo kyllä muhun on kohdistunut kalasteluhyökkäyksiä. -H1

> Esimerkiksi tuota tässä 15 vuotta sitten tuli semmoinen, me jouduttiin semmoisen verkkohyökkäyksen kohteeksi. Se tuli vaan tietyn merkkisiin laitteisiin, että se tuli vaan Canonin laitteille. [...] Ensin luultiin, että siinä oli joku tekninen vika, mutta sehän tuli sitten pian selville, että niihin laitteisiin oli hyökätty. [...] no on nämä kokemukset vaikuttaneet vahvasti. Pitää olla todella tarkkana. - H6

Kaikki tietoturvahyökkäyskokemukset eivät olleet töissä tapahtuneita. Yhdellä haastateltavista oli henkilökohtainen kokemus kalasteluhyökkäyksen onnistumisesta sosiaalisen median tililleen. Haastateltava ei ollut ennen hyökkäyksen tapahtumista ollut kiinnittänyt huomioita monivaiheisen tunnistautumisen tärkeyteen, mutta kyseinen tapaus oli vaikuttanut haastateltavaan niin voimakkaasti, että nykyisin hän huolehtii, että hänellä on vahva salasana ja monivaiheinen tunnistautuminen käytössä kaikilla tileillään.

> Mun henkilökohtainen Facebook-tili on kaapattu. Silloin mulla välähti, että kaikki tietoturva-asiat ei ole kunnossa, minkä takia mun tili just kaapattiin. Mutta sen hyökkäyksen aikana niin mä sain riittävää tukea ja opastusta ammattilaisilta. Sen jälkeen mä tajusin kaksiosaisen tunnistautumisen merkityksen. -H3

Henkilökohtaisella kokemuksella on vaikutusta asenteeseen ja/tai toimintaan. Kaikki haastateltavat olivat tietoisia kuitenkin tietoturvatapahtumista vähintään yleisen median uutisoinnin kautta, ja sitä kautta tietoturvan tärkeys oli noussut heille esille. Tässä yhteydessä haastateltavat kuitenkin tunnistivat, että tietoturva usein nousee uutisointiin ja tärkeäksi ilmiöksi aina piikeittäin, kun jotain ikävää on tapahtunut. Vain yksi osallistujista seurasi aktiivisesti juuri tietoturva-aiheista uutisointia työpaikan kanavien ulkopuolella, mutta kyseinen henkilö teki tietoturvaa myös työkseen.

Haastateltavat kuvailivat tietoturvaan liittyvää asennettaan varsinkin tietokoneella työskennellessään varovaisena. Vastauksissa korostui varsinkin tietyn varovaisuuden ylläpitäminen, kun tarkastellaan, jaetaan tai kirjataan tietoja. Erityisesti haastateltavat, jotka pääsivät työnsä kautta mahdollisten hyökkääjien

kannalta kiinnostaviin tietoihin käsiksi, pitivät tietoturvaa tärkeässä asemassa ja kokivat merkittävää vastuuta pitää tiedot turvassa.

> [...] mulla on esimerkiksi pääsy järjestelmiin, josta näkee tosi paljon meidän työntekijöiden tietoja, niin kyllä mä koen omalta osaltani semmoista vastuuta pitää ne tiedot turvassa ja silleen, että kukaan ei tarkoitettu, ei pääse niihin käsiksi. -H2

Kuitenkin saman tyyppinen varovaisuus ei kaikilla haastateltavista jatkunut työaseman ulkopuolelle tapahtuviin toimiin, vaan esimerkiksi työkavereiden kanssa keskustelu tunnistettiin asiana, jolloin tulee jaettua avoimemmin tietoa.

> Mutta kyllä mä aika lailla vapaasti puhun työkavereitten kanssa kaikesta, että enemmän se on ehkä se, että koneella työskentely tarkempaa. -H4

Teemaan kuuluvaa yleistä asennetta käsiteltäessä haastateltavilta kysyttiin myös heidän vapaa-aikansa internet käyttäytymisestään ja siitä tunnistavatko he vapaa-ajan toimiensa vaikuttavan yrityksensä tietoturvaa. Harva haastateltavista näki omaa työrooliaan tarpeeksi kiinnostavana, että he sen takia aktiivisesti vähentäisivät henkilökohtaisten tietojensa jakamista sosiaalisessa mediassa, mutta tiettyjä mainintoja yleisistä tietoturvatoimista tuli esille, kuten se, että tilit pidetään yksityisenä ja esimerkiksi H1 ja H4 mainitsivat, ettei omaa työpaikan kulkukorttia saa jakaa sosiaalisessa mediassa.

> Koen, että jos joku haluaisi mun yritykseen kohdistaa jonkun ison tietoturvahyökkäyksen, niin sen ei olisi mitään järkeä mun kautta sitä yrittää tehdä, koska mä oon niin tavallaan alhaalla siinä organisaatiossa [...] -H5

Osa haastateltavista kuitenkin kertoi ymmärtäneensä, kuinka hyökkääjät voivat sosiaalisen median kautta kerätä tietoa ja siihen liittyvät uhkat vasta myöhemmin siirtyessä työelämään, mikä on johtanut toimintamallien muuttamiseen, kun he ovat saaneet lisää tietoa aiheesta. Tieto, joka oli johtanut uusiin toimintatapoihin, oli tullut työpaikan tietoturvakoulutuksista.

> Nyt kun mä oon siirtynyt työelämään ja meilläkin on jonkin verran jotain koulutuksia, niin ne nykyään vaikuttaa jonkin verran. Mä oon huomannut, että mä en postaa esimerkiksi someen samalla tavalla. Mä en näe järkeväksi, mitenkään jakaa mun sijainteja aina tai miltä meidän yrityksessä näyttää. -H2

Tutkimuksissa on noussut esille, että osa työntekijöistä näkee tietoturvan olevan etäinen asia, jossa päävastuu on yrityksellä (Ashenden, 2018; Mikkola, 2021), mikä voi olennaisesti myös vaikuttaa työntekijän käyttäytymiseen. Haastatteluun osallistuneet henkilöt kuitenkin kaikki toivat vahvasti esille, että he kokivat tietoturvan olevan ehdottomasti kaikkien yrityksen työntekijöiden vastuulla ja asia, mihin kaikkien pitää panostaa ja olla valppaana. Osa haastateltavista kuitenkin toi esille, että on yrityksen vastuulla tehdä yleisiä teknisiä toimia, joilla tuetaan tietoturvan toteuttamista.

Haastateltavat toivat esiin myös tietoturvakoulutusten tärkeyden yrityksessään. Jokaisella haastateltavalla oli yrityksen puolesta pakollisia koulutuksia,

mutta koulutusten luonne vaihteli suuresti. Pelillistetyt koulutukset, kuten sähköpostiin tulevat tarkoituksenmukaiset epäaidot kalasteluyritykset, koettiin mielekkäiksi ja tietoturvaosaamista edistäviksi. H3:n yrityksessä onnistuneesti suoritetut tietoturvakoulutukset olivat edellytys palkankorotuskierrokselle, jonka takia hän oli erittäin motivoitunut suorittamaan koulutukset. Hänen näkemyksessään ei kuitenkaan korostunut itse tietämyksen lisääminen tietoturvasta vaan varmistus siitä, että suorittamattomat koulutukset eivät rajoita hänen urallansa edistymistään. Motiivina hänellä oli enemmän oma hyötyminen kuin tietoturvatietämyksen kasvattaminen.

6.3 Koettu normi

Haastattelun viimeinen teema liittyi haastateltavien koettuihin normeihin. Koetulla normilla (Ajzen & Fishbein, 2009) viittaavat sosiaaliseen paineeseen tai vaikutteisiin toimia tietyllä tavalla, mikä muodostuu henkilön kokemien tärkeiden henkilöiden tai ryhmien näkemyksistä. Tärkeiksi vaikuttavaksi ryhmiksi haastattelussa tunnistettiin työkaverit ja työyhteisö sekä vapaa-ajan läheiset ihmiset kuten perhe tai ystävät.

Yhdellä vastaajista (H6) työyhteisössä vallitsi työpaikalla erittäin vahva luottamus ja arvostus kollegoita kohtaan. Kaikki työpaikalla suhtautuvat vakavasti tietoturvaan ja se näkyi avoimuutena tuoda esiin epäkohtia muille, sekä uskallus puuttua, jos näkee toisen toimivan väärin. Haastateltava koki myös työkavereiden suhtautumisen vaikuttavan positiivisesti haluun toimia tietoturvallisesti ja pitää työpaikka turvallisena.

> Musta se tosi kiva, että kun ollaan siinäkin suhteessa samanhenkisiä, niin kyllä se vaikuttaa siihen työviihtyvyyteen ja siihen työmoraaliin. [...] kyllä meillä töissä on välittömät suhteet, että koen, että pystyisin heti kysymään, jos tulisi tilanne, että joku toimisi väärin, että hei haloo, että mikä juttu tämä nyt on. -H6

Muilla vastaajilla ei ollut samantyyppistä avoimuutta havaittavissa työyhteisössä. Jokainen vastaajista totesi, että he pyrkivät toimimaan tietoturvallisesti, mutta kynnys puuttua muiden toimiin on suuri. Ihan lähimpien kollegoiden tekemiseen koettiin mahdollisesti pystyvä puuttumaan, varsinkin jos oma tekeminen oli sidoksissa toisen tekemiseen, mutta kokonaan ulkopuoliselle toiminnan huomauttaminen koettiin vaikeaksi. Erona tähän oli haastateltava H1, joka ammattinsa puolesta joutui painostamaan eri tiimejä toimimaan tietoturvallisesti ja käsittelemään näitä aiheita päivittäin. Hänellä työroolin puolesta korostui tarve tuoda epäkohtia esiin, jos hän niitä havaitsi.

Tietyn tyyppisen auktoriteetin, kuten kokeneempien kollegoiden näkemysten koettiin vaikuttavan omaan toimintaan. Kokeneempi kollega nähtiin tahona, jonka toimintatapaan ja osaamiseen voi pääsääntöisesti luottaa, vaikka itse ei olisi asiasta täysin varma. Kokeneempien kollegoiden ammattitaitoon näin ollen pääsääntöisesti luotettiin tietoturvamielessä.

> Musta tuntuu, että jos mun vanhemmat kollegat sanoo, että toimitaan tietyllä tavalla, niin kyllä mä luotan niiden osaamiseen, vaikka mä en ite tiedä, onks se välttämättä oikein. Mut mä ehkä luotan sit mua kokeneempiin ihmisiin, että ne kyllä tietää, miten pitää tehdä. -H2

Osassa haastattelussa puolestaan nousi esille, että nuorempiin työntekijöihin luotetaan tietoturvamielessä, koska he nähdään tietoturvaa parantava tekijänä, koska he osaavat käyttää sujuvasti laitteita ja järjestelmiä sekä ymmärtävät paremmin tietoturvaa ja sen riskejä. Myös uuden oppimisen sisäistäminen nähtiin tekijäksi, joka nosti nuorempia ylös.

> [...] tavallaan nopea sisäistää verrattuna aikaisempiin sukupolviin, jotka sitten ei ole ehkä syntynyt niin paljon vahvasti teknologian parissa. Kun teknologia on kehittynyt, niin tavallaan huomaa, että niiden on vaikeampi sisäistää uusia asioita. -H1

> Nuoret osaa käyttää tietokoneita ja tietoturva ja kaikki menee heille ihan todella sujuvasti. -H4

Lähipiirin toiminnalla vapaa-ajalla koettiin olevan positiivisesti vaikutusta omaan tietoturvatoimintaan, jos lähipiirissä oli henkilöitä, jotka olivat kiinnostuneita tietoturvasta tai toivat tietoturvaan liittyviä asioita ilmi. Puolestaan, jos lähipiirissä oli henkilöitä, joiden tietoturva käyttäytyminen koettiin olevan heikolla tasolla, niin heidän toiminnallaan ei koettu olevan negatiivista vaikutusta omaan toimintaan. Haastateltavat pikemminkin kokivat huolta tai osa koki jopa vastuuta auttaa kyseisiä henkilöitä, sekä tarvetta katsoa hieman heidän toimiensa perään. Haastateltavat kuitenkin tunnistivat, että he eivät pysty, eikä se ole heidän vastuullaan muuttaa toisten toimintatapoja, jos toiset eivät sitä halua.

> Mulla on lähipiiristä kyllä tullut hyviä vaikutteita omaan arkeen ja käyttäytymiseen ja sieltä musta tuntuu, että mun tietoturvaosaaminen onkin lisääntynyt ja tullut yleistä varovaisuutta lisää. -H2

Haastatteluissa nousi esille, että pääsääntöisesti haastateltavat uskoivat yleiseen tietoturvaan liittyvän huolimattomuuden tai välinpitämättömyyden johtuvan tietämättömyydestä. Ainakin käsiteltäessä henkilöiden omia tietoja, mutta he uskoivat joissain tapauksissa myös laiskuudella olevan vaikutusta, sillä tietoturvaan liittyvää uutisointia ja ohjeistusta löytyy kyllä, jos sitä vaan jaksaa etsiä.

7 POHDINTA

Tässä pro gradu tutkielmassa tarkasteltiin työntekijöiden tietoturvaa. Tutkielman tavoitteena oli selvittää tekijöitä, josta tietoturvallinen työskentely koostuu sekä tekijöitä, jotka vaikuttavat työntekijöiden tietoturvakäyttäytymiseen. Tutkimusongelmiin vastaamiseksi ensin lähdettiin syventymään siihen, mitä tietoturva on ja, mitä se pitää sisällään yleisellä tasolla. Samalla myös tuotiin esiin käsite tietoturvatietoisuus, jolla on tunnistetusti ollut vaikutusta työntekijöiden tietoturvakäyttäytymiseen. Samalla myös sivuttiin tietoturvarikkeiden seuraamuksia, jotta saatiin luotua kuva siitä, kuinka tärkeää työntekijöiden tietoturva on yrityksen toiminnalle. Tutkimuksen empiirisessä osuudessa puolestaan pyrittiin selvittämään, työntekijöiden asenteita tietoturvaa kohtaan, sekä mitä tekijöitä työntekijöiden tietoturvakäyttäytymisen taustalla on.

Tutkimuksessa hyödynnetty teoreettinen viitekehys pohjautui Ajzen ja Fishbein (2009) perustellun toiminnan viitekehykseen, jossa todetaan, että henkilön käyttäytymisen taustalla on eri vaikuttavia tekijöitä liittyen asenteeseen, koettuun kontrolliin sekä koettuun normiin. Tutkimuksen empiirisessä osuudessa tunnistettiin kyseisen viitekehyksen teemoja ja peilattiin näitä laadullisen teemahaastattelun avulla. Tässä luvussa keskitytään aikaisemmin esiin tulleiden tietojen ja havaintojen perusteella vastaamaan tutkimuksen alussa esitettyihin tutkimuskysymyksiin. Lopuksi tarkastellaan vielä tutkimuksen luotettavuus ja esitetään jatkotutkimusaiheita.

7.1 Johtopäätökset tietoturvallisesta työskentelystä

Tutkimuksessa kirjallisuuskatsausosiossa käsiteltiin tekijöitä, joita työntekijöiden, mutta myös työnantajien olisi hyvä huomioida luodessaan tietoturvallisia työskentelytapoja. Vastausta ensimmäiseen tutkimuskysymykseen lähdettiin hakemaan tarkastelemalla nykyisiä tutkimuksia, sekä hyödyntämällä tunnettuja parhaita käytänteitä, kuten Suomen kyberturvallisuuskeskuksen ohjeistuksia.

Työntekijät ovat mielenkiintoinen kohde hyökkääjille, sillä ihmisiin on helppo vaikuttaa ja huijata varsinkin kalasteluyritysten kautta, jotka ovat

jatkuvasti lisääntyneet. Työntekijöiden tietoturva on tärkeää, sillä edistämällä tietoturvatietämystä työntekijöiden keskuudessa organisaatiot voivat parantaa yleistä tietoturvatasoaan ja suojautua paremmin tietoturvauhkia vastaan. Työntekijöiden onkin tunnistettu olevan niin sanottu ensimmäinen puolustuslinja tietoturva riskejä vastaan.

Tutkimuksissa nousi esille, että henkilöt, jotka eivät tee tietoturvan kanssa töitä voivat väheksyä omaa rooliaan yrityksen tietoturva kokonaisuudessa. Tietoturva kuitenkin on ehdottomasti aivan jokaisen työntekijän vastuulla ja se on pidettävä aina mielessä. Huomattiin, että työntekijöiden tietoturva muodostuu kokonaisuudessaan laajasti eri tekijöistä, mutta muutamia perusasioita tunnistettiin, joita kaikilla olisi toivottavaa olla kunnossa, jopa työn ulkopuolella. Työntekijöiden tietoturvan tunnistettiin ensisijaisesti koostuvan aivan perustekijöistä, kuten siitä, että työntekijöillä on käytössä vahvat yksilölliset salasanat eri käyttäjätileilleen. Myös työntekijöiden laitteiden turvallisuus voidaan katsoa kuuluvaksi näihin perustekijöihin. Tähän kuuluu se, että kaikki päivitykset tehdään niiden tullessa saataville ja tätä kautta laitteet pidetään ajan tasalla. Monivaiheisen tunnistautumisen käyttöönotto kuuluu myös laitteiden turvallisuuteen sekä, että laitteet pidetään lukittuna niiden ollessa käyttämättöminä.

Tietoturvarikkeitä, jotka ovat peräisin inhimillisistä toimista, on lukuisia ja rikkeiden vakavuus voi vaihdella riippuen työntekijän roolista. Nykyisen tutkimuskirjallisuuden pohjalta huomattiin, että tekijät kuten väsymys tai stressi voivat nostaa riskiä virheiden sattumiselle, jolloin voi tulla tehdyksi virheitä, jotka eivät edes tarvitse hyökkääjien osalta suurta panostusta. Huomattiin, että kalasteluyritykset, jotka tapahtuvat sähköpostiviestien, tekstiviestien tai puhelujen kautta, ja joissa pyydetään arkaluonteisia tietoja tai kehotetaan napsauttamaan linkkejä tai lataamaan liitetiedostoja, ovat ehdottomasti suosituin hyökkäystapa, jota hyökkääjät harjoittavat. Myös tutkimuksen empiirisessä osuudessa huomattiin, että suurin osa haastateltavista oli kokenut itseensä kohdistuvan kalasteluyrityksiä.

Tietoturva perustuu kolmeen pilariin, jotka ovat luottamuksellisuus, eheys ja saatavuus. Nämä kolme näkökulmaa on tärkeää pitää toiminnassa mielessä jatkuvasti, sillä tietoturva on ennen kaikkea ennaltaehkäisevää toimea, jolla pyritään estämään mm. tiedon luvaton käyttö. Tutkimuksessa esitettiin tietoturvatietoisuus keinona kehittää työntekijöiden tietoturvallista työskentelyä. Huomattiin, että tietoturvatietoisuus on laaja kokonaisuus, mutta sillä pääsääntöisesti tarkoitetaan tietoa, asenteita ja käyttäytymistä, jotka liittyvät tietojen suojaamiseen organisaatiossa. Keinoja edistää tietoturvatietoisuutta ovat työntekijöiden säännöllinen kouluttaminen tietoturvasta ja tietojen suojaamisen tärkeydestä sekä auttaa työntekijöitä tunnistamaan mahdollisia tietoturvauhkia. Tietoturvatietoisuus edistää turvallisen työympäristön ylläpitämistä, mutta vaikutukset voivat olla laajemmat, sillä tietoturvatietoisuuden ennaltaehkäisevät vaikutukset, kuten tietoturvaloukkausten tai -murtojen väheneminen säilyttää niin yrityksen maineen kuin tuo myös sitä kautta säästöjä yritykselle.

Tutkimuksessa saatiin selville, että vaikka tietoturvatietoisuus on tärkeää ja tunnistetusti olevan edistävä tekijä työntekijöiden tietoturvalliselle työskentelylle, sen levittäminen ei ole helppoa, sillä kaikkiin ihmisiin ei tehoa samat koulutuskeinot, eikä kaikilla ole samaa kiinnostusta oppia uusia asioita. Huomattiin

myös, että työntekijöiden tietoturvatietoisuuden tason mittaamisessa on omia haasteita, sillä tieto ei aina heijastu käytökseen, jolloin pakollisten testien tulokset eivät välttämättä viittaa tietoturvalliseen työskentelyyn. Keinoja mittaamisen parantamiseen on kuitenkin kehitetty, jotka pyrkivät kokonaisvaltaisemman tuloksen saamiseen.

7.2 Johtopäätökset työntekijöiden tietoturvakäyttäytymiseen vaikuttavista tekijöistä

Tämän tutkimuksen pohjalta sekä peilaten perustellun viitekehyksen ”asenne käyttäytymistä kohdetta” -kohtaan, voidaan todeta, että haastateltavien työntekijöiden asenne ja sitä myötä myös käyttäytyminen tietoturvaa kohtaan, oli hyvällä tasolla. Kaikki tutkimukseen osallistuneet haastateltavat olivat itse halukkaita kertomaan omista kokemuksistaan ja näkemyksistään tietoturvaa kohtaan, joten siitä ehkä johtui, että asenne tietoturvallista käyttäytymistä kohtaan oli jokaisella haastateltavalla hyvä. Asenteen on havaittu olevan merkittävä tekijä käyttäytymiselle, mutta myös tietoturva-alan tieteellisissä tutkimuksissa on tunnistettu, että asenne vaikuttaa henkilön aikomukseen, joka puolestaan ennustaa tulevaa toimintaa eli käyttäytymistä. Kaikki haastateltavista tunnistivat tietoturvauhkien läsnäolon, varsinkin vapaa-ajan toimissaan kalasteluyritysten muodossa. Osalla uhkien läsnäolon tunnistus painottui vahvemmin myös työkontekstiin, varsinkin henkilöille, jotka olivat IT-alla itse töissä. Haastateltavat tunnistivat tarpeen rajoittaa ja suojata henkilökohtaisia tietojaan edes jollain tasolla, kuten pitää omat tilinsä yksityisinä. Kuitenkin henkilökohtainen kiinnostus ja asenne tietoturvaa kohtaan vaikutti positiivisesti, vaikka henkilöllä ei ollutkaan teknistä taustaa. Näiden ryhmien välillä oli eroja siinä mitä yksityiskohtia he painottivat näkemyksissään tai mitä ilmiöitä he toivat esille. Kaikki kuitenkin suhtautuivat tietoturvauhkiin vakavuudella, osalla oli vain laajempi käsitys mahdollisten riskien seurausten vakavuudesta.

Peilaten perustellun toiminnan viitekehykseen, tutkimuksessa ilmeni, että työntekijän koettu normi eli esimerkiksi sosiaalinen ympäristö vaikuttaa siihen, miten henkilö käyttäytyy. Tunnistettiin, että avoin ja hyvä työilmapiiri kannustaa työskentelemään toivotuilla tavoilla ja samalla kynnys keskustella ja puuttua havaittuihin virheisiin on matalampi, kun puolestaan työyhteisöissä, joissa ei ole samanlaista avoimuutta. Yleisesti kynnys puuttua muiden tietoturva-asioihin on korkea, sillä monesti työntekijät kokevat omasta osaamisestaan kuitenkin jonkin verran epävarmuutta tai he eivät näe asiakseen puuttua muiden asioihin. Tämä kynnys korostuu varsinkin työpaikalla, jossa on enemmän hierarkkinen ilmapiiri. Vapaa-ajallaan henkilön on helpompi puuttua läheisten tekemiseen. Varsinkin esimerkiksi iäkkäämpien läheisten tietoturvallisuuteen pyritään kiinnittämään huomioita. Kuitenkaan edes vapaa-ajalla, ei koeta asiakseen puuttua aivan kaikkien lähipiirin tietoturva-asioihin.

Nykyisin melkein kaikissa ammateissa käytetään teknologioita, mikä heijastuu myös työntekijöiden tietoteknisiin taitoihin. Omat taidot koetaan hyväksi tai kohtalaiseksi ja työntekijät eivät yleisesti säikähdä uusia järjestelmiä, vaan

luottavat, että saavat niihin tarvittaessa tukea ja koulutusta. Tämä näkyy myös työntekijöiden koetussa tietoturvaosaamisessa. Yleisesti työntekijät luottavat työnantajan tarjoavan työssä tarjotun tietoturvatietämyksen koulutusten mukana ja he myös luottavat, että työnantaja pitää huolen tarvittavasta tasosta testaamalla työntekijöitä. Työntekijät eivät yleisesti itse perehdy tietoturvaan liittyviin asioihin vapaa-ajallaan, ellei henkilön työrooliin tai erityisiin kiinnostuksen kohteisiin kuulu tietoturva. Työntekijöillä on myös vahva luottamus, että jos jotain tietoturvamielessä epäilyttävää tulee vastaan, niin ilmoittamalla yrityksen IT- tai turvallisuusosastolle, he huolehtivat sillä asian hoitamisen. Luottamus työnantaja yrityksen toimintatapoihin on siis korkealla ja tämä heijastuu käyttäytymiseen tiettynä luottamuksensa, että asioista uskalletaan ilmoittaa eteenpäin ja omaan työhön nähden koetaan omaavan tarvittava tietoturvatietämys.

7.3 Tutkimuksen luotettavuus ja jatkotutkimusaiheet

Toisin kuin määrällisessä tutkimuksessa, jossa luotettavuus liittyy yleensä johdonmukaisuuteen ja toistettavuuteen, laadullisessa tutkimuksessa luotettavuus keskittyy mm. uskottavuuteen ja vahvistettavuuteen. Laadullisen tutkimuksen luotettavuuden varmistamiseen liittyy eri tekijöitä. Tässä tutkimuksessa on pyritty, että tutkimusprosessi kuvataan selkeästi ja läpinäkyvästi. Tutkimukseen valitut menetelmät on perusteltu ja saatuja tulkintoja on pyritty esittämään nykyisten tutkimusten pohjalta tai haastatteluaineiston lainauksien avulla. Tutkimuksen vaiheista on myös pyritty tekemään läpinäkyviä.

Tutkija on myös pyrkinyt kokoamaan haastatteluaineiston perehtymällä haastattelun toteuttamiseen sekä valitun haastattelumenetelmän kannalta oikeisiin toimintatapoihin. Huomiona kuitenkin, että tutkija ei ollut aikaisemmin tehnyt minkäänlaisia haastatteluita, jonka vaikutusta aineiston laatuun ei voida ohittaa. Kokemattomuudesta johtuen voi olla, että haastattelutilanteissa tutkija ei pystynyt tai osannut kysyä tarvittavia lisäkysymyksiä tai luoda tarvittavaa pohtivaa ilmapiiriä aikaiseksi. Toiseksi voidaan todeta, että koska haastateltavat kerättiin vapaaehtoisten kiinnostuneiden pohjalta, niin otanta ei sisältänyt monipuolisesti eri ammatin edustajia. Vastaajien sukupuoli ja ikäjakauma oli kuitenkin otannan kokoon nähden suhteellisen tasapuolinen. Haastattelun osallistujien vapaaehtoisuudesta johtuen voi olla, että kaikilla haastateltavilla oli siksi suhteellisen hyvä tietoturvatietämys, vaikka kirjallisuuden pohjautuen oletus oli, että vaihtelevuutta olisi ollut enemmän. Toisaalta tietoturva mielletään usein hieman arkana aiheena, eikä haastateltavat välttämättä kerro avoimesti näkemyksistään, vaikka tutkimuksen tulokset toteutettaisiinkin anonyyminä.

Tutkimuksessa tuli esille, että henkilöillä ei välttämättä ole kovin paljon kiinnostusta tietoturvaa opiskelua kohtaan omalla ajallaan, vaikka tietoturva koetaan erittäin tärkeäksi. Työntekijät kokivat työnantajan tarjoamat pakolliset koulutukset keskimäärin hyviksi, sillä he kokivat näin varmistuvansa, että oma tietoturvatietämyksen taso on tarvittavalla tasolla. Työnantajan koulutukset eivät välttämättä ole kuitenkaan aina täydellisiä tai muodossa, joka on oppimisen kannalta paras. Yksi mielenkiintoinen jatkotutkimuksen aihe voisi tästä syystä

olla, mikä on paras tapa tehdä tietoturvakoulutuksia ja, miten pystyttäisiin lisäämään työntekijöiden omaa kiinnostusta tietoturvaa kohtaan.

Toinen mielenkiintoinen jatkotutkimuksen aihe voisi koskea jonkin tietyn alan työntekijöiden asennetta tietoturvaa kohtaan. Tässä tutkimuksessa pyrittiin antamaan yleispätevä kuva työntekijöiden asenteista, mutta keskittymällä johonkin tiettyyn sektoriin voitaisiin mahdollisesti saada kyseiselle kohdealueelle paremmin yleistettäviä tuloksia.

LÄHTEET

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of advances in information technology*, *3*(3), 176-183.

Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges and solutions. *Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018, Cambridge, UK.*

Alsharif, M., Mishra, S., & AlShehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science & Engineering*, *40*(3).

Amankwa, E., Loock, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors. *Information & Computer Security*, *30*(4), 583-614.

Ashenden, D. (2018). In their own words: employee attitudes towards information security. *Information & Computer Security*, *26*(3), 327-337.

Ajzen, I. (1991), "The theory of planned behaviour", *Organisational Behaviour and Human Decision Processes*, Vol. 50 No. 2.

Ajzen, I. & Fishbein, M. Predicting and Changing Behavior : The Reasoned Action Approach, Taylor & Francis Group, 2009. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=668501.

Borkovich, D. J., & Skovira, R. J. (2019). CYBERSECURITY INERTIA AND SOCIAL ENGINEERING: WHO'S WORSE, EMPLOYEES OR HACKERS?. *Issues in Information Systems*, *20*(3).

Caldwell, Z. B. (2016). A security measure paradigm for assessing industrial control system cyber security management effectiveness. (*Doctoral dissertation, Capella University)*.

Chai, W., (2023). CIA triad (confidentiality, integrity and availability). Techtarget. Osoitteesta. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Chen, H., Li, Y., Chen, L., & Yin, J. (2021). Understanding employees' adoption of the Bring-Your-Own-Device (BYOD): the roles of information security-related conflict and fatigue. *Journal of Enterprise Information Management*, *34*(3), 770-792.

Conetta, C. (2019). Individual Differences in Cyber Security, McNair Research Journal SJSU: Vol. 15 , Article 4.

Da Veiga, A. (2016). A Cybersecurity Culture Research Philosophy and Approach to Develop a Valid and Reliable Measuring Instrument. SAI Computing Conference 2016, July 13-15, 2016, Pages 1006-1015.

Dharmawansa, A. D., & Madhuwanthi, R. A. M. (2020). Evaluating the information security awareness (ISA) of employees in the banking sector: a case study.

El-Bably, A. Y. (2021). Overview of the impact of human error on cybersecurity based on ISO/IEC 27001 information security management. *Journal of Information Security and Cybercrimes Research*, *4*(1), 95-102

Esteves, J., Ramalho, E., & De Haro, G. (2017). To Improve Cybersecurity, Think Like a Hacker. *MIT Sloan Management Review*, *58*(3), 71.

Fertig, T., Schütz, A. E., & Weber, K. (2020, June). Current Issues Of Metrics For Information Security Awareness. In ECIS.

Fisher, R., Porod, C., & Peterson, S. (2021). Motivating employees and organizations to adopt a cybersecurity-focused culture. *Journal of Organizational Psychology*, *21*(1), 114-131.

Haeussinger, F., & Kranz, J. (2017). Antecedents of elpoyees' information security awareness-rewiev, synthesis, and directions for future research. *Association for Infromation Systems.*

Haney, J. M., & Lutters, W. (2023). From Compliance to Impact: Tracing the Transformation of an Organizational Security Awareness Program. *arXiv preprint arXiv:2309.07724*.

Haney, J. M., & Lutters, W. G. (2017). Skills and Characteristics of Successful Cybersecurity Advocates. *In SOUPS*.

Hänsch, N., Benenson, Z., 2014. Specifying IT Security Awareness. *2014 25th International Workshop on Database and Expert Systems Applications*. pp. 326–330.

Heiskanen, K. (2020). Ihmispalomuuri organisaation suojana. Osoittesta. https://blogit.jamk.fi/cyberdi/2020/05/27/ihmispalomuuri-organisaation-suojana/

Hirsjärvi, S. & Hurme, H. (2001) Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hyvärinen, M., Suoninen, E. ja Vuori, J. (2021). Etnografia. Teoksessa Vuori, J. (toim.) *Laadullisen tutkimuksen verkkokäsikirja*. Tampere: Yhteiskuntatieteellinen tietoarkisto. Osoitteesta https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus.

Bullee, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *J. Exp. Criminol.*, vol. 11, no. 1, pp. 97–115, 2015.

Kaspersky Daily. (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Osoitteesta https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Kerner, M. (2022). Colonial Pipeline hack explained: Everything you need to know. *TechTarget*. Osoitteesta https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, *5*(26), 10862.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106, 102267.

Kyberturvallisuuskeskus. (2020). Näin pidät huolta tietoturvasta kotona ja työpaikalla. Osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla

Kyberturvallisuuskeskus. (2022). Toimintaohje - Tietomurto. *Traficom*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf

Kyberturvallisuuskeskus. (2023). Tietoturva on koko organisaation asia - vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun. Osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston

Kyberturvallisuuskeskus. (2024). Autoreporterin haittaohjelmahavainnot. Osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/havainnointi-ja-avunanto/autoreporterin-haittaohjelmahavainnot

Lauhia, J., (2022). Miten vastuullinen kyberturvallisuus tukee kasvua? *EY*. https://www.ey.com/fi_fi/consulting/miten-vastuullinen-kyberturvallisuus-tukee-kasvua-

McIlwraith, A. (2021). Information security and employee behaviour: how to reduce risk through employee education, training and awareness. *Routledge*.

Mikkola, M. (2021) Työntekijöiden pitää olla aktiivinen osa yrityksesi tietoturvaa. *Digia*. Osoitteesta: https://digia.com/blogi/tyontekijoiden-pitaa-olla-aktiivinen-osa-yrityksesi-tietoturvaa

Morand, G., (2023). Employee Badges on Social Media. *LinkedIn*. https://www.linkedin.com/pulse/employee-badges-social-media-greg-morand-cpp-lpc/

Ncubukezi, T. (2022, March). Human errors: A cybersecurity concern and the weakest link to small businesses. In *Proceedings of the 17th International Conference on Information Warfare and Security* (p. 395)

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security*, *66*, 40-51.

Pattinson, M., Parsons, K., Butavicius, M., McCormac, A., & Calic, D. (2016). Assessing information security attitudes: a comparison of two studies. *Information & Computer Security*, *24*(2), 228-240.

Rubin, H. J., & Rubin, I. S. (2011). Qualitative interviewing: The art of hearing data (3rd ed.). *Sage Publications*.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto. Osoittesta https://www.fsd.tuni.fi/menetelmaopetus/

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3).

Singh, L. (2016). Privacy & Social Media. *Georgetown University*.

Stefaniuk, T. (2020). Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, *7*(3), 1832.

Tekniikka & Talous. (2022). Maailman suurimman lentoyhtiön asiakkaiden tietoja päätyi hakkerien käsiin. Osoitteesta. https://www.tekniikkatalous.fi/uutiset/maailman-suurimman-lentoyhtion-asiakkaiden-tietoja-paatyi-hakkerien-kasiin/0283ee85-7ef9-4d43-a4c5-972923482a4f

Tekniikka & Talous. (2023). Työntekijän arkinen moka Oktan tietomurron taustalla – hyökkääjä pääsi ainakin 134 yrityksen tietoihin. Osoitteesta https://www.tekniikkatalous.fi/uutiset/tyontekijan-arkinen-moka-oktan-tietomurron-taustalla-hyokkaaja-paasi-ainakin-134-yrityksen-tietoihin/17cf1506-ff5e-413b-b2e6-61938e7ae345

The Institute of Internal Auditors. (2020). The IIA's Three Lines Model. Osoitteesta. https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *Thomas, JE (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. International Journal of Business Management*, *12*(3), 1-23.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167-173.

Traficom. (2024). Kyberuhkiin varautuminen on kustannustehokkaampaa kuin kyberhyökkäyksestä toipuminen. Osoitteesta https://www.traficom.fi/fi/kyberuhkiin-varautuminen-kustannustehokkaampaa-kuin-kyberhyokkayksesta-toipuminen

Vilkka, H. (2007). Tutki ja mittaa: Määrällisen tutkimuksen perusteet.

Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security–what goes where?. *Information & Computer Security*, 26(1), 2-9.

Yle. (2023). OP:ssä tietomurto – asiakkaiden nimiä ja henkilötunnuksia saattoi joutua vääriin käsiin. Osoitteesta https://yle.fi/a/74-20063927

Yleinen tietosuoja-asetus (GDPR) 2016/679.

LIITE 1 ENSIMMÄINEN LIITE

Alustus

Taustatiedot:

- Ikä
- Ammatti
- Toimiala

TEEMA 1. Haastateltavan koettu kontrolli. (Tämä tarkoittaa esimerkiksi eri rajoitteita aiheeseen liittyen. Tähän kuuluu myös oma osaaminen)

- Miten koet itsesi Atk-laitteiden käyttäjänä (Tietokoneet, puhelimet...)?
    - Onko uudet teknologiat helppo sisältää?
- Miten toimit tai toimisit, jos havaitset tietoturvapoikkeaman tai tietoturva mielessä jotain epäilyttävää (työ kontekstissa)?
- Miten koet oman tietoturvaosaamisesi?

TEEMA 2. Haastateltavan käsitys aiheesta ja yleinen asenne

- Miten kuvailisit tietoturvan omin sanoin? Mitä se sinulle tarkoittaa?
    - Kenellä mielestäsi on vastuu tietoturvasta?
- Millaisia tietoturvauhkia koet itseesi kohdistuvan?
    - Onko esimerkkejä?
    - Miten nämä uhat vaikuttavat omiin toimiin ja valintoihin?
- Minkä koet yleisen suhtautumisen tietoturvaa kohden olevan?)
    - Mikä ovat rehellisesti omin sanoin asenteesi tietoturvaa kohtaan töissä?
    - Mikä ovat rehellisesti omin sanoin asenteesi tietoturvaa kohtaan vapaa-ajallasi?
- Seuraatko tietoturva-aiheisia uutisointia?
    - Entä työpaikalla (jos sitä on)?
- Koetko siviilielämän toimiesi vaikuttavan yrityksesi tietoturvaan?
    - Miten siviilielämässä huomioit tämän vaikutuksen?
    - Käytätkö työpaikan työasemaa muuhunkin kuin työkäyttöön?

TEEMA 3. Haastateltavan koettu normi eli miten haastateltava kokee muiden lähellä olevien ihmisten tai tärkeiden henkilöiden suhtautumisen tietoturvaa kohden olevan.

- Miten työpaikallasi käsitellään tietoturvaa ja miten tämä ilmenee?
    - Onko tarpeeksi selkeät ohjeistukset? Millaisia ohjeistuksia on? Luotetaanko työntekijöihin, koetko että valvotaanko työntekijöiden toimia? Vaikuttaako tämä omiin toimiin?
    - Millaisia seurauksia tietoturva rikkeistä voi olla?
- Miten koet kollegoidesi suhtautumisen tietoturvaa kohtaan?

    - Miten tämä vaikuttaa omaan käyttäytymiseen?
- Miten koet vapaa-ajan lähipiirin suhtautumisen tietoturvaa kohtaan? (perhe, ystävät)