Janne Kastepohja

KYBERTURVALLISUUSKULTTUURI – OHJELMISTOYRITYS REAKTORIN RATKAISUJA HENKILÖSTÖN KAUTTA KOHDISTUVIEN KYBERUHKIEN VÄHENTÄMISEKSI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Kastepohja, Janne Johannes
Kyberturvallisuuskulttuuri – ohjelmistoyritys Reaktorin ratkaisuja henkilöstön kautta kohdistuvien kyberuhkien vähentämiseksi
Jyväskylä: Jyväskylän yliopisto, 2020, 98 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

Organisaatioiden tietoturvaa ja kyberturvallisuutta kohtaan kohdistuu käyttäjien kautta tai toimesta vakavia uhkia, jotka voivat ilmetä organisaatioiden sisä- tai ulkopuolelta. Yksin tietoturvaohjeilla ei kyetä vastaamaan uusien hyökkäysmetodien ja -työkalujen kehitysnopeuteen, eikä inhimillisiin virheisiin. Päätelaitteiden sekä tietoverkkojen ja -järjestelmien käyttäjät kohtaavat jatkuvasti valintatilanteita, joissa organisaation kyberturvallisuuden vaarantuminen on mahdollista. Käyttäjien kautta toteutuvaan uhkaan vastaaminen ja organisaation kyberturvallisuuden kehittäminen on mahdollista muun muassa vaalimalla kyberturvallisuuskulttuuria. Vahva kyberturvallisuuskulttuuri tarkoittaa koko organisaation sitouttamista ylläpitämään ja kehittämään kyberturvallisuutta. Kyberturvallisuuskulttuuri ei rajoitu organisaation sisälle kuten tietoturva- ja turvallisuuskulttuurit, vaan ulottuu elämän kaikille osa-alueille. Kyberturvallisuuskulttuurin kannalta on olennaista tunnistaa mitkä tekijät, esimerkiksi erilaiset kulttuurit ja toimintamallit, vaikuttavat organisaatioon, sen toimintaympäristöön, toimintaan ja henkilöstöön. Tähän ongelmaan vastattiin tässä tutkimuksessa analysoimalla aiempien tutkimusten tulosten ja haastattelemalla ohjelmistoyritys Reaktorilla henkilöstöä, jotta pystyttiin tunnistamaan Reaktorin kyberturvallisuuskulttuurin muodostumiseen vaikuttavia tekijöitä. Holistisen ja syvällisen tarkastelun takaamiseksi tutkimusmenetelmäksi valittiin fenomenografia, jossa ilmiötä kuvataan yksilöiden kokemusten ja näkemysten kautta. Henkilöstön tapa nähdä ja kokea organisaationsa kyberturvallisuuskulttuuri on itse ilmiön tutkimista olennaisempaa, koska yksilö kokee kulttuurin aina subjektiivisesti. Tutkimuksessa haastateltujen Reaktorin henkilöstön käsitysten perusteella yrityksessä on yhtenäinen ja vahva kyberturvallisuuskulttuuri. Se perustuu luottamukseen, hajautettuun päätöksentekoon, toisten auttamiseen, jatkuvaan oppimiseen ja sosiaalisiin verkostoihin. Yrityksessä kyberturvallisuus nähdään luonnollisena osana kaikkea liiketoimintaa ja ratkaisuja, minkä vuoksi organisaatiokulttuurin rooli kyberturvallisuuskulttuurissa on keskeinen. Reaktorin organisaatiokulttuuri tukee luonnostaan vahvaa kyberturvallisuuskulttuuria, koska organisaatiokulttuuri tukee vuorovaikutusta, avoimuutta, kehittämistä ja tiedon jakamista. Organisaation keskeisimmät toimijat myös kyberturvallisuuden ylläpidossa ovat itseohjautuvat yksilöt ja tiimit, jotka ottavat kyberturvallisuuden huomioon yhtenä osana teknisiä ratkaisuja ja toimintaa. Yrityksen kyberturvallisuuskulttuurissa turvallisuusratkaisut räätälöidään tapauskohtaisesti kontekstin, käytettävyyden ja asiakkaan tarpeiden mukaan.

Asiasanat: kyberturvallisuus, kyberturvallisuuskulttuuri, kansallinen kulttuuri, organisaatiokulttuuri

ABSTRACT

Kastepohja, Janne Johannes
Cyber security culture – solutions of a Finnish software development company Reaktor to decrease cyber threats, which manifest via personnel
Jyväskylä: University of Jyväskylä, 2020, 98 pp.
Cyber Security, Master's Thesis
Supervisor(s): Siponen, Mikko

Malicious actions and anomalies, which manifest by or via users, are a serious and constant threat to companies' information and cyber security. These threats can manifest from inside or outside of the company. Information security policies fail to respond to the pace of new attack methods and tools as well as to human errors in general. Users of end-point devices as well as computer networks and systems face constantly situations, where company's cyber security may be compromised. As an answer to these threats, researchers have proposed creating and fostering cyber security culture as a solution. A functioning cyber security culture demands efforts from the whole organization to maintain and develop cyber security. Cyber security culture is affected by organizational structures and culture, nature of company's business and national and individual level cyber security cultures. Unlike security and information security cultures, cyber security culture is not limited just within the company, but it touches all aspects of life and users may have many different roles in it. In order to foster a robust cyber security culture, it is essential to identify the context in which such culture operates. This means the wide variety of factors affecting to the company, business, and the company's employees. The formation of the views and capabilities of an individual to maintain cyber security are affected for example by multiple levels of culture, individual know-how and experiences. Culture is a concept, which is seen subjectively by an individual. A company's cyber security culture therefore consists of and is informed by the mindsets of the employees: how employees see and experience the cyber security culture of the company. Qualitative research offers a robust methodological approach to explore and understand such in-depth and complex concepts as culture. In addition to analyzing findings of previous research, this research used qualitative interviews to analyze the expressions and mindsets of employees of Finnish software and consulting low hierarchy company Reaktor as a case study of maintaining high-level and successful cyber security culture at a company level. To analyze the phenomenon through expressions and mindset of individuals, phenomenography was chosen as a research method. The findings indicate that Reaktor fosters a robust cyber security culture, which is based on trust, decentralized decision making, helping others, constant development, and social networks within the company. Continuous learning of the company and employees is seen as a requirement for maintaining the cyber security culture. The research found that the most essential actors of the company in fostering cyber security culture are self-controlled individuals and teams, who consider cyber security aspects as a natural part of technical

solutions and all activity. All security solutions within Reaktor's cyber security culture are based on context, usability, and client's needs. Cyber security is seen as an integral part of all business activity, which makes organizational culture a crucial component of the company's cyber security culture.

Keywords: cyber security, cyber security culture, national culture, organizational culture

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tietojärjestelmät ovat sosio-teknisiä kokonaisuuksia, jotka koostuvat teknologiasta, käyttäjistä ja prosesseista. Ihminen on keskeinen osa kokonaisuutta, koska ihmisellä on rooli niin teknologian kehittäjänä, rakentajana, käyttäjänä kuin ylläpitäjänäkin. Huolimatta lisääntyvästä tietoisuudesta ihmisiä kohtaan tai heidän kauttaan toteutetuista kyberuhkista, on ihminen edelleen tietoturvan ja kyberturvallisuuden näkökulmasta merkittävä riski. Käyttäjien kautta toteutetut hyökkäykset ovat hyvin yleisiä. Tietoturvayhtiö Verizonin vuoden 2018 Data Breach Investigations Report -julkaisussa esitettiin lukuisia erilaisia havaittuja hyökkäystapoja, mutta lähes jokaisen ihmisen käyttämä yksinkertainen väline, sähköposti, liittyi jollain tavalla jopa 96 prosenttiin havaituista hyökkäyksistä. Suurin osa organisaatioihin kohdistuvista uhkista on lähtöisin niiden ulkopuolelta. Ihmisten kautta tai avulla toteutettuihin hyökkäyksiin kuuluvat kuitenkin myös organisaation sisäpuolelta toteutetut hyökkäykset (Schultz, 2002), joilta on haastavaa suojautua yksin teknisten menetelmien avulla.

Koska käyttäjät on tunnistettu yhdeksi merkittäväksi hyökkäysten kohteeksi, vaatii tietoverkkojen ja -järjestelmien turvallisuuden ja sitä kautta kyberturvallisuuden kehittäminen myös ymmärryksen lisäämistä ihmisen roolista, toiminnasta ja vaikutuksesta. Tämä mahdollistaa aiempaa paremmin ihmisen ominaisuuksien huomioimisen suunniteltaessa tietojärjestelmiä tai laadittaessa tietoturvakontrolleja. (Gonzalez & Sawicka, 2002; Krombholz ym., 2014). Haasteena on kuitenkin se, että vaikka ihmisen käyttäytymiseen vaikuttavia tekijöitä jollain tasolla tunnettaisiin, on niihin kohdistetun tavoitteellisen vaikuttamisen tulosten ennustaminen vaikeaa (Sowell, 2007).

Yksi ratkaisu käyttäjien kautta toteutettujen hyökkäysten vähentämiseksi ja organisaation kyberturvallisuutta parantamiseksi on tietoturva- ja kyberturvallisuuskulttuurien vaaliminen sekä ylläpitäminen organisaatioissa (Schlienger & Teufel, 2002; von Solms & Van Niekerk, 2013; Da Veiga, 2016). Kulttuurin luominen ja ylläpitäminen organisaatiossa tietoisesti vaatii kuitenkin ymmärrystä sen muodostumisesta. Tietoturva- ja kyberturvallisuuskulttuurien muodostumiseen vaikuttaa merkittävästi yksilöiden arvojen, asenteiden ja uskomusten perusta, kansallinen kulttuuri, jonka huomioimisella kyetään räätälöimään

tietoturvakäytännöt toimiviksi organisaation kontekstissa (Schein, 1985; Hofstede, 1991; Rocha Flores, Antonsen & Ekstedt, 2014). Myös organisaatiokulttuurin vaikutus on tunnistettu merkittäväksi tekijäksi, joka vaikuttaa käyttäjien asenteisiin turvallisuutta ja turvallisuusohjeita kohtaan (Knapp, Morris, Marshal & Byrd, 2009). Tarkastelemalla ja vaikuttamalla organisaatiossa vallitseviin kulttuureihin on mahdollista vaikuttaa organisaation yksilöiden sisäisiin motiiveihin siinä missä ohjeistaminen, ja ohjesääntöjen noudattamisen valvominen vaikuttavat ulkoisiin. Kyberturvallisuuden parantaminen organisaatiokulttuurin avulla mahdollistaa käyttäjien aktiivisemman osallistumisen uhkien havaitsemiseen, tiedonjakoon ja organisaation kyberturvallisuuteen liittyvien käytänteiden kehittämiseen.

Tämän tutkimuksen tavoitteena on selvittää, mitä tekijöitä täytyy ottaa huomioon, kun suomalaisessa asiantuntijaorganisaatiossa halutaan vähentää käyttäjien kautta organisaatioon kohdistuvia kyberuhkia ylläpitämällä tietoisesti vahvaa kyberturvallisuuskulttuuria. Tutkimus on luonteeltaan laadullinen. Tutkimusmenetelmänä käytetään fenomenografiaa, koska tavoitteena on selvittää ilmiön esiintymistä yksilöiden käsitysten kautta. Tutkittava ilmiö on ohjelmistoyritys Reaktorin kyberturvallisuuskulttuuri, johon liittyviä käsityksiä selvitetään avoimella teemahaastattelulla. Haastattelututkimusta edeltää aihepiirin teoreettinen tarkastelu. Tutkimus painottuu kyberturvallisuuskulttuurin muodostumiseen vaikuttavien tekijöiden tunnistamiseen sekä haastateltavien käyttäjien kyberturvallisuuskulttuuriin liittyvien käsitysten ilmaisuun, analysointiin, ryhmittelyyn ja kuvaamiseen. Tutkimuksessa tarkastellaan asioiden merkityksiä, vaikutusyhteyksiä ja niistä muodostuvia rakenteita.

Tutkimuksessa keskeisiä käsitteitä ovat kyberturvallisuus, kyberturvallisuuskulttuuri, siihen vaikuttavat kulttuurin muut osa-alueet sekä yksilön tietoturvaan ja kyberturvallisuuteen liittyvään toimintaan vaikuttavat tekijät. Koska tutkimus toteutetaan Suomen kansallisen kulttuurin kontekstissa, on olennaista tunnistaa ja esittää Suomen kansallisen kulttuurin erityispiirteet, jotta voidaan arvioida niiden välitöntä ja välillisiä vaikutuksia organisaation kyberturvallisuuskulttuuriin.

1.1 Tutkimuksen keskeiset käsitteet

Tutkimuksessa keskeistä on sen rakentuminen käsitteellisten ratkaisujen ja merkitystulkintojen varaan. Tieteellisessä tutkimuksessa tutkittavia ilmiöitä pyritään käsitteellistämään eli hahmottamaan yleisellä, teoreettisella, tasolla. (Hirsjärvi, Remes & Sajavaara, 2007). Tässä luvussa esitellään tutkimuksen kannalta keskeiset käsitteet ja perustellaan valittujen määritelmien soveltuminen tutkimuskohteeseen. Käsitteiden määrittelyä ei tässä tutkimuksessa ole tarvetta toteuttaa tiukasti, koska niitä ei mitata ja jokainen yksilö ymmärtää käsitteet eri tavoin. Haastattelua varten keskeiset käsitteiden yleinen ja operationaalinen määritelmä kerrotaan tarvittaessa haastateltaville, jotta käsite konkretisoituu.

Tutkimuksen ensimmäinen keskeinen käsite on kyberturvallisuus. Se on monitahoinen käsite, jolle ei ole yksiselitteistä määrittelyä vaan sen määritelmään vaikuttavat näkökulma ja tarkastelun taso. Kyberturvallisuus on määritelty abstraktilla tasolla Suomen kyberturvallisuusstrategiassa (Turvallisuuskomitea, 2013), jonka mukaan kyberturvallisuudella tarkoitetaan ”tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.” ISO/IEC:n standardissa 27032 (ISO/IEC, 2012) kyberturvallisuus määritellään tietojen luottamuksellisuuden, saatavuuden ja eheyden säilyttämiseksi ja suojelemiseksi kybertoimintaympäristössä (*eng*. cyber domain). Kyberturvallisuus jaetaan usein teknisiin (*eng.* technical factors) ja inhimillisiin tekijöihin (*eng.* human factors). Tässä tutkimuksessa käsitellään laajasti inhimillisten tekijöiden vaikutusta kyberturvallisuuteen, koska ihminen toimii teknisten järjestelmien rakentajana, kehittäjänä, ylläpitäjänä ja käyttäjänä. Tällöin inhimillisen virheen mahdollisuus ulottuu kaikille edellä mainituille osa-alueille.

Kyberturvallisuudessa on keskeistä, että erilaisilla tieto- ja viestintätekniikan välineillä käsiteltävät ja tallennetut tiedot ovat saatavilla ainoastaan hyväksytyille käyttäjille. Lisäksi on pystyttävä luotettavasti varmistamaan, ettei mitään tietojen osia ole muutettu tai poistettu. Kyberturvallisuudella on ainutlaatuisia ominaisuuksia, mutta myös riippuvuuksia ja yhdistäviä tekijöitä muiden turvallisuuden lajien kanssa esimerkiksi koskien tieto- ja tietoverkkoturvallisuutta sekä internetin ja kriittisen infrastruktuurin turvaamista. (ISO/IEC, 2012).

Rauscher ja Yashenko (2011) ovat määritelleet kyberturvallisuuden kybertoimintaympäristön ominaisuudeksi vastustaa, vastata ja toipua tahallisista tai tahattomista uhkista. Toistaiseksi täydellisin, ja esimerkiksi useissa monikansallisten työryhmien dokumenteissa käytetty, määritelmä löytyy Euroopan unionin kyberturvallisuusviraston Enisan julkaisusta ”Definition of Cybersecurity - Gaps and overlaps in standardisation” (2016). Siinä kyberturvallisuus määritellään työkalujen, ohjeistusten, turvallisuuskonseptien ja -kontrollien, ohjeiden, riskienhallinnan lähestymistapojen, toimintojen, koulutuksen, parhaiden käytäntöjen, turvaamisen ja teknologian kokoelmaksi, jota voidaan käyttää kybertoimintaympäristön sekä organisaatioiden ja käyttäjien välineiden turvaamiseen. Suojattavat välineet sisältävät verkkoon liitetyt laitteet, henkilöstön, infrastruktuurin, ohjelmat, palvelut, operaattoreiden järjestelmät sekä kaiken kybertoimintaympäristössä lähetettävän tai sinne tallennetaan tiedon. Keskeiset kyberturvallisuuden tavoitteet ovat saatavuus, eheys, luottamuksellisuus, autentikointi ja kiistämättömyys. (Enisa, 2016).

Toinen tutkimuksen keskeisistä käsitteistä, kyberturvallisuuskulttuuri, kuvaa yksilöiden henkilökohtaista tai kollektiivista tapaa toimia digitaalisessa eli kybertoimintaympäristössä. Kyberturvallisuuskulttuuri jakautuu yksilö-, organisaatio-, kansallisen ja kansainvälisen tason kyberturvallisuuskulttuureihin, jotka vaikuttavat toisiinsa (Da Veiga, 2016). Kyberturvallisuuskulttuurin muodostumiseen eri tasoilla vaikuttavat muun muassa kansallinen kulttuuri, organisaatiokulttuurit, ammatilliset alakulttuurit sekä yksilöt. Kyberturvallisuuskulttuuri perustuu tietoon, uskomuksin, havaintoihin, asenteisiin, oletuksiin, normeihin ja ihmisten arvoihin, mitkä liittyvät kyberturvallisuuteen ja siihen, miten

edellä mainitut tekijät ilmenevät ihmisten käyttäytymisenä tieto- ja viestintätekniikan käytössä (Enisa, 2017). Kyberturvallisuuskulttuuri on monitahoinen ja jatkuvasti muuttuva konstruktio, koska se on sidottu tiettyyn aikaan, toimintaympäristöön, tietoon ja henkilöihin.

1.2 Tutkimuksen rakenne

Tutkimuksen ensimmäisessä luvussa johdatetaan lukija aiheeseen, esitellään tutkimusongelma ja tarve tutkimuksen toteuttamiselle sekä määritellään keskeiset käsitteet. Toisessa luvussa esitellään tutkimusotteen ja -menetelmien teoriataustaa, perustellaan tutkimuksessa tehdyt menetelmälliset valinnat sekä esitellään tutkimuksen käytännön toteutus ja siihen vaikuttaneet tekijät.

Tutkimus on kaksivaiheinen. Kolmannessa luvussa käsitellään tutkimuksen ensimmäistä vaihetta, jonka perusteella vastataan ensimmäiseen pää- ja alakysymykseen. Kolmannessa luvussa käydään tarkemmin läpi tutkimuksen keskeinen teoriatausta: kulttuurin käsitteellinen määrittely, kansallisen kulttuurin muodostuminen, organisaatiokulttuuri ja kyberturvallisuuskulttuuri. Kolmas luku sisältää myös teorioiden vertailun suhteen toisiinsa ja tutkimuksen kontekstin kannalta olennaisen Suomen kansallisen kulttuurin kuvauksen.

Neljännessä luvussa käsitellään tutkimuksen toista vaihetta, jonka perusteella vastataan toiseen pääkysymykseen ja sen alakysymyksiin. Luvussa esitellään empiirisen aineiston perusteella syntynyt kuva asiantuntijoiden käsityksistä Reaktorin kyberturvallisuuskulttuurista.

Viidennessä luvussa vastataan tutkimuskysymyksiin ja pohditaan löydösten suhdetta tutkimusongelmaan. Kuudes luku sisältää pohdinnan, johtopäätökset ja jatkotutkimusaiheet.

2 TUTKIMUSKYSYMYKSET JA MENETELMÄT

Tässä tutkimuksessa hyödynnetään laajasti ihmistieteiden ja tietoturvan eri tutkimustuloksia, koska keskitytään ilmiön hahmottamiseen ihmisen näkökulmasta. Tällöin keskeistä on ihmisen asenteiden, arvojen ja toiminnan arviointi. Tutkimus on luonteeltaan laadullinen, koska sen tavoitteena on todellisen elämän tutkiminen ja käsitys todellisuuksien moninaisuudesta (Hirsjärvi ym., 2007). Tutkimuksessa pyritään ymmärtämään erilaisia käsityksiä kyberturvallisuuskulttuurin muodostumiseen vaikuttavista tekijöistä yleisesti ja tapauskohtaisesti Reaktorilla.

Suurin osa tietoturvaa ja kyberturvallisuutta koskevasta tutkimuksesta on toteutettu määrällisiä tutkimusmenetelmiä käyttäen ja tiedonkeruu on usein toteutettu lomakehaastatteluna. Wash, Rader ja Fennel (2017) tunnistivat lomakehaastattelun käytön ongelmalliseksi, koska tutkimushavainnoista selvisi vastaajien vastausten ja todellisen toiminnan eroavaisuus. Ihmisten on tunnistettu muistavan hyvin ja vastaavan luotettavasti aktiivista toimintaa arvioiviin kysymyksiin, mutta muistavan huonosti ja kuvailevan epätarkasti havainnointia ja tiedostamista koskeviin kysymyksiin (Wash ym., 2017). Myös Euroopan unionin kyberturvallisuusviraston Enisan (2018) toteuttamassa tietoturvan ja kyberturvallisuuden tutkimuksia arvioivassa katsauksessa todettiin, että määrällinen tutkimus ja siinä käytetyt mittaustekniikat eivät tuota riittävästi ymmärrystä ihmisten tietoturvaan ja kyberturvallisuuteen liittyvästä käytöksestä vaan rinnalla tarvitaan myös laadullista tutkimusta ja eri tutkimusmetodeja yhdistelyä. Näkökulma tulisi myös vaihtaa teknologia- ja prosessikeskeisestä ihmiskeskeiseksi etenkin käyttäjiä ja heidän toimintaansa koskevassa tutkimuksessa (Enisa, 2018).

Kulttuuri on dynaamisesti muuttuva järjestelmä, jota ei voi luotettavasti tutkia eristämällä osia siitä. Kulttuuria tai sen osa-alueita on tutkittava kokonaisuutena tietyssä kontekstissa. Kulttuurin vaikutus ilmenee vuorovaikutustilanteissa eri tavoin. Edellä mainittujen ongelmien vaikutusta pyritään tässä tutkimuksessa vähentämään taustatekijöiden vaikutuksen huomioimisella tutkimuksessa, tutkijan perehtyneisyydellä taustatekijöihin ja niiden vaikutukseen sekä vuorovaikutteisen haastattelu- ja tutkimusmenetelmän käyttämisellä.

Tutkimus ei voi koskaan olla täysin objektiivista, mutta tutkimukseen luotettavuutta voidaan parantaa tunnistamalla ja tuomalla esiin siihen vaikuttavia tekijöitä sekä kuvaamalla tutkimusprosessi kattavasti (Metsämuuronen, 2011). Laadullisessa tutkimuksessa tutkijan arvolähtökohtien ja ennakkokäsitysten tunnustetaan ohjaavan tutkimusta (Hirsjärvi ym., 2007). Tutkijan henkilökohtaisten käsitysten ja niiden mahdollinen vaikuttavuus tunnistetaan etukäteen ja tunnustetaan, jotta kyetään vähentämään niiden vaikutusta (Ashworth & Lucas, 2000; Uljens 1992). Tämän tutkimuksen toteuttamiseen ja haastattelumateriaalin tulkintaan vaikuttaa tutkijan työskentely hierarkkisessa turvallisuusalan organisaatiossa. Tutkijan käsitysten ja uskomusten vaikutusta tutkimukseen pyritään vähentämään toteuttamalla tiedonkeruu yksityisellä sektorilla toimivassa matalan hierarkian organisaatiossa.

2.1 Tutkimusongelma ja -kysymykset

Tutkimusongelma on, mitä tekijöitä täytyy ottaa huomioon, jotta suomalainen asiantuntijaorganisaatio pystyy tietoisesti luomaan ja ylläpitämään vahvaa kyberturvallisuuskulttuuria vähentääkseen organisaatioon käyttäjien kautta kohdistuvia kyberuhkia. Tutkimusongelman käsittely on jaettu tutkimuksessa kahteen vaiheeseen. Ensimmäisessä vaiheessa selvitetään, mitkä tekijät olemassa olevan tutkimustiedon perusteella vaikuttavat kyberturvallisuuskulttuurin muodostumiseen. Toisessa vaiheessa selvitetään haastattelujen avulla, miten kyberturvallisuuskulttuuri esiintyy Reaktorilla. Toinen vaihe perustuu ensimmäisen vaiheen löydöksiin ja on siten jatkumoa ensimmäiselle vaiheelle. Tutkimustulosten tarkastelussa pohditaan löydösten vaikutusta kyberturvallisuuskulttuuriin tutkimusongelman kannalta, verrataan kahden vaiheen tuloksia keskenään ja esitetään haastatteluissa ilmenneitä uusia, poikkeavia tai tapauskohtaisia löydöksiä.

Aihepiiristä tehdyn aiemman tutkimuksen määrä vaikuttaa tutkimuskysymyksen muotoiluun (Metsämuuronen, 2011). Tietoturvaa tai kyberturvallisuutta ei ole vielä tutkittu laajasti kulttuurillisesta näkökulmasta laadullisia tutkimusmenetelmiä käyttäen. Koska yleistä tutkimusta tietoturvasta ja kyberturvallisuudesta sekä turvallisuuskulttuurista on kuitenkin olemassa, on osa tutkimuskysymyksistä muotoiltu kuvaileviksi ja osa selittäviksi. Tutkimuksella on kaksi pääkysymystä ja neljä alakysymystä:

1. Mitkä tekijät vaikuttavat kyberturvallisuuskulttuurin muodostumiseen organisaatioissa?
    a. Miten kyberturvallisuuskulttuuriin vaikuttavat tekijät ilmenevät suomalaisen asiantuntijaorganisaation kontekstissa?
2. Millainen kyberturvallisuuskulttuuri ohjelmistoyritys Reaktorilla on käyttäjien kautta kohdistuvaan uhkaan vastaamisen näkökulmasta?
    a. Mistä ovat Reaktorin kyberturvallisuuskulttuuri muodostumisen kannalta keskeiset tekijät?
    b. Miten haastateltavien tausta ja henkilökohtainen kyberturvallisuuskulttuuri vaikuttavat heidän käsityksiinsä kyberturvallisuudesta?
    c. Millä tavalla organisaatiokulttuuri vaikuttaa Reaktorin kyberturvallisuuskulttuuriin?

Ensimmäisen pää- ja alakysymyksen tarkoituksena oli tutkia kirjallisuuskatsauksen kautta kyberturvallisuuskulttuurin muodostumiseen ja ylläpitämiseen vaikuttavia tekijöitä. Sen perusteella muodostettiin haastattelun teemat ja haastattelua tukevat kysymykset.

Toisen pääkysymyksen ja sen alakysymysten tarkoitus oli selvittää empiirisen tiedonkeruun ja fenomenografisen analyysin avulla Reaktorin haastateltavan henkilöstön käsityksiä henkilökohtaisesta ja organisaationsa kyberturvallisuuskulttuurista sekä siihen vaikuttavista tekijöistä. Tavoitteena oli havainnoida,

miten ensimmäisessä vaiheessa tunnistetut tekijät ilmenevät käytännössä Reaktorin kyberturvallisuuskulttuurissa.

2.2 Tutkimusmenetelmä

Tutkimuksen toteuttamisessa valittiin käytettäväksi fenomenografista tutkimusmenetelmää. Fenomenografian valintaa tutkimusmenetelmäksi puolsi yksilöiden käsitysten tapaan tutkimuksen kohteena olevien kulttuurien ominaisuus jatkuvasti muuttuvina ja moniulotteisina kokonaisuuksina, jotka ihmiset käsittävät ja kokevat eri tavoin. Alasuutari (2011) mainitsee, että merkitys kontekstina on keskeinen kulttuuria tutkittaessa. Sitä voidaan tutkia kahdesta eri näkökulmasta: strukturalismi näkee kulttuurin rakenteet tärkeämmäksi kuin sen tuottamat subjektit. Fenomenologinen traditio puolestaan keskittyy siihen, kuinka ihmiset pyrkivät kuvaamaan todellisuutta ja ymmärtämään sitä. (Alasuutari, 2011). Tässä tutkimuksessa tutkitaan merkitystä fenomenologisen tradition näkökulmasta, jossa itse ilmiötä tärkeämpää on sen ilmeneminen haastateltaville yksilöille.

Myös todellisuutta on mahdollista kuvata kahdesta näkökulmasta. Ensimmäisen asteen näkökulmassa kuvataan tutkittavan ilmiön kannalta mielenkiintoisia todellisuuden ulottuvuuksia. Toisen asteen näkökulmassa kuvataan ihmisten kuvailemia todellisuuden ulottuvuuksia, jotka ovat heidän mielestään ilmiön kannalta mielenkiintoisia. (Marton, 1981). Jälkimmäiseen tapaan hahmottaa ja kuvata todellisuutta vaikuttavat yksilön käsitysten muodostamisen kannalta merkitykselliset kulttuurit ja niiden erityispiirteet.

Fenomenografiassa todellisuutta kuvataan toisen asteen näkökulmasta. Maailma esiintyy yksilölle aina sen suhteen kautta, mikä hänellä on maailmaan. Ihminen luo asioille merkityksiä sitomalla niitä kokonaisuuksiin, minkä perusteella syntyvät henkilökohtaiset käsitykset asioista. Sen vuoksi on olennaista mistä osista kokonaisuus rakentuu. Fenomenografinen tutkimus ei pyri esittämään väitteitä todellisuudesta, vaan ihmisten käsityksiä siitä. Todellisuutta tulkitaan tutkijan ollessa jatkuvassa vuorovaikutuksessa tutkimuskohteen kanssa. (Uljens, 1989; Huusko & Paloniemi, 2006). Todellisuus on olemassa ihmisille merkitysvälitteisesti. Se rakentuu merkitystulkinnoista ja arkielämän toimintaan vaikuttavista tulkintasäännöistä. (Uljens, 1989).

Fenomenografisessa tutkimussuuntauksessa hyväksytään olettamus, että on olemassa yksi todellisuus, jonka ihmiset kokevat eri tavoin. Huolimatta yksilöiden käsitysten merkityksen painottamisesta, fenomenografisen tutkimuksen keskeinen tavoite ei ole tuottaa yksilötason kuvauksia, vaan löytää ja systematisoida sosiaalisesti merkittäviä ajattelutapoja. (Huusko & Paloniemi, 2006).

Fenomenografian luonteeseen kuuluu haaste tutkimuksen toistettavuudesta, koska tutkimustilanne, käsitykset ja konteksti ovat ainutlaatuisia. Tutkimustilanteen ainutlaatuisuuden, laadullisen tutkimuksen vahvan tulkinnallisuuden, tutkimustilanteessa tapahtuvan vuorovaikutuksen ja tutkijan käsitysten vaikutuksen vuoksi ei tutkimus ole toistettavissa täysin samanlaisissa olosuhteissa. Tutkimus on oppimisprosessi, jossa tiedonkeruu- ja analysointitapoja ei voi

erottaa toisistaan. Tutkijan käsitykset myös muuttuvat tutkimusprosessin aikana. (Marton & Booth, 1997).

Ihmisten tapaan esittää käsityksensä ilmiöstä vaikuttavat tutkimuksen konteksti ja kysymyksenasettelut. Ihminen voi haastattelun aikana myös muuttaa kuvaustaan käsityksistään. Koska tutkimusaineiston keräämiseen vaikuttaa myös kielellinen ilmaisu ja vuorovaikutus, on yksittäisiä sanoja tai syiden ymmärtämistä keskeisempää kuvauskategorioiden muodostaminen. (Marton, 1981; Häkkinen, 1994; Uljens, 1989).

Michael Uljensin (1989) mukaan käsitykset ovat merkitykseltään arkikielen mielipidettä laajempia ja syvempiä, perustavanlaatuisia suhteita yksilön ja ympäröivän maailman välillä. Yksilön tapa jäsentää todellisuutta perustuu hänen subjektiivisiin kokemuksiinsa tietyssä kulttuurillisessa kontekstissa (Uljens, 1989). Kulttuurilla on vaikutusta yksilön käsityksiin, koska eri kulttuureissa käsitteillä on erilaisia merkityksiä, minkä vuoksi yksilön ymmärrys ja ajattelun logiikka eivät välttämättä toimi erilaisessa kulttuurikontekstissa (Häkkinen, 1994). Käsitykset voivat toki vaihdella saman kulttuurin sisälläkin, mihin Wenestamin (1984) mukaan vaikuttaa sosiaalinen konteksti eli esimerkiksi sosioekonominen asema tai ikäerot.

Koska tutkittava ilmiö on sidoksissa tutkimuksen kontekstiin, päätettiin tutkimus kirjoittaa suomeksi. Kieli on ihmisen ajattelun ja ilmaisemisen väline, jonka avulla ihminen muodostaa käsityksiä ja ilmaisee niitä (Huusko & Paloniemi, 2006). Lisäksi kieli on olennainen osa yksilön omaksuessa ja toteuttaessa kansallisen kulttuuriin liittyviä käsityksiä ja tapoja. Tutkittaessa haastateltavien suomeksi ilmaistuja käsityksiä Suomen kansallisen kulttuurin kontekstissa vältetään kääntämisestä aiheutuvat virheet ja vääristymiset pitäytymällä suomen kielen käytössä. Ilmaisuissa läsnä olevien herkkyyksien ja nyanssien säilyttäminen auttaa pysymään lähellä alkuperäistä tutkimusaineistoa sekä vähentää täten myös tutkijan tulkinnan vaikutusta.

2.3 Tutkimuksen rajaaminen, näkökulma ja konteksti

Tutkimuksessa tiedostettiin kyberturvallisuuskulttuurin, siihen liittyvien yksityiskohtien ja erilaisten näkökulmien, olevan hyvin laaja kokonaisuus tutkittavaksi pro gradu -työssä, mikä asetti tarpeen rajata tutkimusta. Rajaaminen on olennaista tutkimusongelman hallittavuuden näkökulmasta (Hirsjärvi ym., 2007; Metsämuuronen, 2011). Tämän vuoksi tutkimus rajattiin koskemaan vain yhden, luonteeltaan matalan hierarkian, asiantuntijaorganisaation, Reaktorin, henkilöstön käsityksiä tutkittavasta ilmiöstä organisaation kontekstissa.

Tutkimuksen kohteena olevan yrityksen organisaatiorakenne ja toimintamallit poikkeavat perinteisistä hierarkkisista organisaatioista. Yrityksen toimiala on ohjelmistokehitys ja konsultointi, minkä vuoksi organisaation osaamisessa painottuu monipuolinen tieto- ja viestintätekniikan osaaminen, mutta myös ymmärrys asiakkaan tarpeista ja liiketoiminnasta. Yrityksen liiketoiminta perustuu

asiakkaan luona tapahtuvaan itseohjautuvien tiimien toimintaan. Tiimit vastaavat asiakassopimuksen perusteella käytännön ratkaisujen toteutuksesta.

Tutkimustulosten hyödynnettävyyden näkökulmasta kohdeorganisaatioksi ei valittu suoraan tietoturvaan keskittyvää organisaatiota, vaikka kyberturvallisuus vaikuttaa yrityksen liiketoimintaan. Tutkimuksessa keskityttiin tietoisesti Suomen kansallisen kulttuurin vaikutukseen yksilöiden käsitysten muodostumiseen, organisaatiokulttuuriin ja organisaation kyberturvallisuuskulttuuriin. Rajauksen vuoksi tässä tutkimuksessa ei käsitellä erilaisten organisaatiokulttuurien eroja.

Tutkimus toteutettiin kokonaan julkisena, mikä vaikutti tutkimuskysymysten asetteluun kyberturvallisuuteen sisältyvien herkkyyksien vuoksi. Haastattelukysymykset laadittiin koskemaan vain välttämättömimmän osalta Reaktorin yksityiskohtaisia käytäntöjä, laitteistoja tai ohjelmistoja. Reaktorin edustajalle annettiin mahdollisuus kommentoida haastattelukysymyksiä etukäteen sensitiivisyyden näkökulmasta, mutta hän ei ohjannut haastattelutilannetta kysymysten tai käsiteltävien teemojen osalta. Haastateltavilta henkilöiltä kysyttiin ainoastaan heidän työtehtävänsä organisaatiossa, koulutustaustansa, ikänsä ja sukupuolensa, minkä avulla yksittäisen haastateltavan identiteetti kyettiin anonymisoimaan. Sen tavoite oli henkilöllisyyden suojaaminen, mutta myös vastaamiskynnyksen madaltaminen.

Tutkimustulosten analysoinnissa verrattiin vastaajien näkemyksiä ja ilmaisuista muodostuneita merkityskategorioita Suomen kansallista kulttuuria ja koulutusjärjestelmää, organisaatiokulttuuria sekä ammatillisia alakulttuureja koskevaan teoriatietoon. Määrittelemällä tutkimuksen konteksti tarkasti mahdollistettiin tutkimuksen toteutuksen arviointi ja ymmärrys tulosten hyödynnettävyyttä koskevista rajoituksista. Kontekstin kuvaaminen on keskeistä myös ilmausten ymmärtämisessä oikeassa asiayhteydessä (Huusko & Paloniemi, 2006), minkä vuoksi tutkimuksen kohdeorganisaation toimiala, koko ja turvallisuuteen liittyvät valinnat kuvattiin yleisellä tasolla. Haastateltavien käsitykset eivät ole suoranaisesti valideja muussa yhteydessä kuin tutkitussa kontekstissa, mutta tulosten hyödynnettävyyden näkökulmasta käsitykset pyrittiin sitomaan tutkittavien ryhmään (Uljens, 1992).

Tutkimuksessa käytettiin yleisesti tunnustettuja ja hyödynnettyjä teorioita, mutta tuotiin esille niihin kohdistuva kritiikki ja havaitut rajoitukset. Kansallista kulttuuria peilattiin Geert Hofsteden kuuden kulttuurillisen dimension teoriaan (Hofstede ym., 2010). Organisaatiokulttuurin määrittelyssä hyödynnettiin Edgar Scheinin (1999) kolmitasoista organisaatiokulttuurin mallia. Kyberturvallisuuskulttuurin määrittely perustui Adele da Veigan (2016) kyberturvallisuuskulttuurin viitekehykseen. Määrittelyssä hyödynnettiin myös turvallisuus- ja tietoturvakulttuuria koskevia tutkimuksia, koska kyberturvallisuuskulttuuri liittyy tai sisältää osia turvallisuus- ja tietoturvakulttuureista. Yksilön toimintaympäristö on hyvin samankaltainen, vaikka osaaminen ja välineet eroavat kyberturvallisuutta ja esimerkiksi fyysistä turvallisuutta koskevissa tilanteissa. Monia tietoturva- tai turvallisuuskulttuuria koskevia tutkimuksia ei myöskään ole toteutettu puhtaasti kyberturvallisuuskulttuurin kontekstissa.

2.4 Kohdeorganisaation valinta ja ominaisuudet

Tutkimuksen kohdeorganisaatioksi valittiin Suomessa perustetun ohjelmisto- ja konsulttiyritys Reaktorin kotimaiset osat. Yritys soveltui tutkimuksen kohteeksi, koska kyberturvallisuuden taso ja maineenhallinta vaikuttavat sen liiketoimintaan, mutta tietoturva ei kuitenkaan ole sen ydinliiketoimintaa.

Kohdeorganisaation valintaan vaikuttivat tutkijan aiemmat keskustelut yrityksen henkilöstön kanssa ja niistä välittynyt kuva avoimesta, luovuutta arvostavasta ja kehityshakuisesta kulttuurista sekä organisaatiokulttuurin eroavaisuudesta verrattuna perinteisiin organisaatioihin. Nämä käsitykset vahvistuivat eri medioiden kautta tutkijan tietoon tulleen, kohdeyrityksen projekteja koskevan, uutisoinnin kautta. Tutkija myös varmisti käsityksiään sopivuudesta keskustelemalla organisaation turvallisuushenkilöstön kanssa.

2.5 Aineiston kerääminen

Aineiston keräämiseen vaikuttivat aihepiirin teoreettinen tarkastelu ja tutkimusmenetelmä. Teoreettisen tarkastelun avulla tutkija lisäsi ymmärrystään tutkittavasta ilmiöstä ja tuotti sen jälkeen soveltuvia tarkentavia kysymyksiä tiedonkeruuvaihetta varten. Aiempi tutkimus ja havainnot tutkimusmenetelmän käytöstä ja eri aineistokeruumenetelmien soveltuvuudesta suosivat tiettyjä vaihtoehtoja.

Aineiston kerääminen toteutettiin yksilöllisenä, avoimena haastattelututkimuksena. Haasteltavien määrä oli 10 henkilöä. Tällainen otos oli toteutettavissa pro gradu -tutkielmassa, mutta sillä silti kyettiin takaamaan riittävästi erilaisia näkökulmia ja ilmaisuja kuvauskategorioiden muodostamista varten. Kattavan otoksen takaaminen oli keskeistä, koska fenomenografisessa tutkimuksessa tutkijan määrittämällä ilmiöllä ei välttämättä ole merkitystä haastateltavan elämässä tai se voidaan ymmärtää täysin eri tavalla (Ashworth & Lucas, 2000).

Aineiston riittävyyttä laadullisessa tutkimuksessa arvioidaan saturaation eli kyllääntymisen avulla. Aineiston kerääminen lopetetaan, kun uusissa tapahtumissa ei ilmene enää tutkimusongelman kannalta uutta tietoa ja aineisto alkaa toistamaan itseään. (Eskola & Suoranta, 1998). Tämän vuoksi haastattelujen aikana ja jokaisen haastattelujakson toteuttamisen jälkeen arvioitiin tarvetta jatkaa haastattelumateriaalin keräämistä ja lisätä haastateltavien määrää. Kun toisen haastattelujakson aikana toteutetun kolmen haastattelun aineisto käytiin läpi, voitiin todeta, ettei ilmaisuissa tullut esille enää merkittävästi uusia asioita. Täten arvioitiin tiedonkeruun todennäköisesti lähestyvän saturaatiota. Tutkimuksen tavoitteena oli pääasiassa tuottaa tietoa käsitysten ja ilmaisujen yhteneväisyyksistä. Se edellyttää aineiston kyllääntymisen näkökulmasta pienemmän aineiston keräämistä kuin erilaisuuden painottaminen (Tuomi & Sarajärvi, 2002). Tällä perusteella 10 haastattelun oli perusteltua päättää tiedonkeruuvaihe.

Haastattelukysymysten muotoilu on fenomenografisen tutkimusmenetelmän takia tutkimuksen kannalta kriittinen vaihe. (Marton, 1986).

Yhteisymmärryksen lisäämiseksi haastattelussa käsiteltävät teemat ja tarkentavat kysymykset muotoiltiin mahdollisimman yksinkertaisiksi. Haastattelukysymysten huolellisesta muotoilusta ja pohjautumisesta teoriaan huolimatta tiedostettiin, etteivät kysymykset välttämättä saa haastateltavia kuvailemaan tai pohtimaan ilmiötä. Toisaalta kysymyksen merkitsemättömyys haastateltaville on lähes yhtä kiinnostavaa kuin laajempi vastaus (Ashworth & Lucas, 2000; Niikko, 2003).

Kun tutkimuskohteena ovat ihmiset ja heidän toimintansa vaikuttavat tutkimustuloksiin aina haastateltavien ”intentiot, pyrkimykset ja motiivit, päämäärät ja tavoitteet sekä mielikuvat ja asenteet” (Metsämuuronen, 2011). Valittaessa haastateltavia varmistettiin heidän kuuluvan tutkimuksen kohdejoukkoon kansallisen kulttuurin näkökulmasta. Haastattelun alussa selvitettiin haastateltavien tausta ja henkilökohtaista suhdetta tutkittavaan ilmiöön. Haastateltavat valittiin vapaaehtoisuuden perusteella organisaatiosta siten, että he edustivat eri sukupuolia, organisaation osia, koulutustaustoja ja työtehtäviä. Ikäjakauma oli laaja.

Haastattelukysymysten muotoilun merkitystä pyrittiin vähentämään käsittelemällä teemoja ja antamalla haastateltavien kertoa vapaasti ennen ennalta tunnistettujen ja haastateltavien ilmausten perusteella ilmenneiden yksityiskohtien kysymistä. Jotta taattiin haastateltaville mahdollisimman suuri vapaus kuvailla tutkittavaa ilmiötä, laadittiin haastattelua varten ainoastaan lista avoimista haastatteluteemoista (Ashworth & Lucas, 2000). Haastattelutilaisuus aloitettiin esittäytymällä ja kertomalla tutkimuksen aihe. Sen jälkeen vuorovaikutuksen lisäämiseksi pyrittiin rakentamaan luottamussuhde haastateltavan ja tutkijan välille. (Ruusuvuori & Tiittula, 2005). Tavoitteena oli luoda vapaamuotoinen ja keskusteleva haastattelutapahtuma. Edellä mainittujen valintojen avulla pyrittiin toteuttamaan fenomenografiselle tutkimukselle keskusteleva tiedonkeruu ja saamaan haastateltavat pohtimaan tutkittavan ilmiön eri ulottuvuuksia (Niikko, 2003). Epävarmoja haastateltavia kannustettiin osallistumaan osoittamalla ymmärrystä ja kehottamalla jatkamaan puhetta (Ruusuvuori & Tiittula, 2005).

2.6 Haastattelujen toteutus

Haastattelutilanteen rakentamisessa tehtyjen valintojen pohtiminen ja kuvaaminen toteutettiin tutkimuksessa kattavasti, koska valmisteluilla on huomattava vaikutus tutkimuksen toteuttamiseen ja toistamiseen (Potter & Hepburn, 2012). Haastattelut toteutettiin yhteensä neljän työpäivän aikana. Haastattelut kestivät keskimäärin noin tunnin. Haastattelujen välissä pyrittiin pitämään 20 minuutin tauko tutkijan keskittyminen takaamiseksi ja tasapuolisen haastattelutilanteen luomiseksi. Tämä ei toteutunut kahden haastattelun osalta.

Haastattelut toteutettiin Reaktorin Suomen pääkonttorin neuvotteluhuoneissa. Ympäristö oli haastateltaville tuttu, turvallinen ja ympäristö liittyi haastattelun aiheeseen. Haastateltaville oli välitetty etukäteen sähköpostiviesti, jossa kerrottiin tutkimuksen aiheesta ja toteutuksesta, esiteltiin tutkija sekä nimettiin tutkimuskohde. Hyvän ensivaikutelman antamiseksi, ammattimaisen kuvan

luomiseksi ja luottamuksen herättämiseksi tutkijaa sekä tutkimusta kohtaan haastateltaville kerrottiin tietosuojan huomioonottamisesta ja ilmausten pseudonymisoinnista. Haastateltaville kerrottiin heille itselleen ja heidän organisaatiolleen tutkimuksen kautta saatavista hyödyistä, millä pyrittiin motivoimaan haastateltavaa osallistumaan aktiivisesti.

Haastattelu tunnistettiin erityiseksi sosiaalisen vuorovaikutuksen muodoksi, minkä vuoksi haastattelun toteuttamisen valinnat ymmärrettiin merkityksellisiksi koko tutkimuksen onnistumisen kannalta (Johnson & Rowlands, 2012). Ennen varsinaisen haastattelun alkua keskityttiin luottamuksen rakentamiseen sekä rennon ja välittömän ilmapiirin luomiseen keskustelemalla ja tutustumalla haastateltaviin. Tarkoituksena oli muodostaa luottamuksellinen side haastateltavien kanssa ja tilanne, jossa tutkija ja haastateltava yhdessä työskentelevät yhteisen tavoitteen eteen. Haastattelutapahtumasta pyrittiin luomaan turvallinen ja luonnollinen, jotta haastateltavat uskaltaisivat reflektoida vapaasti sekä pohtia käsityksiään, perusteita käsityksilleen ja erilaisia näkökulmia.

Tutkimushaastattelussa on vahva rooli- ja vallanjako, koska tutkija on suunnitellut tilaisuuden ja johtaa sen kulkua. Tutkijalla on lisäksi aloite ja auktoriteetti esittää kysymyksiä. (Wang & Yan, 2012). Koska kyberturvallisuuskulttuuri on ilmiönä uusi ja suurimmalle osalle ihmisistä vieras käsite, tulkittiin tutkijalla olevan lähtökohtaisesti vahva asema ja aloite haastateltavaan nähden. (Ruusuvuori & Tiittula, 2005). Vuorovaikutuksen lisäämiseksi ja tasa-arvoisemman keskusteluasetelman luomiseksi tutkija painotti haastattelutilanteessa sitä, miten haastateltava on Reaktorissa tutkittavan ilmiön asiantuntija.

Haastateltaville kerrottiin ennen haastattelua, että vastausten tai pohdinnan tavoite ei ole miellyttää tutkijaa tai vastata niin kuin luulee olevan toivottua, vaan kertoa totuudenmukaisesti käsityksistään ja asenteistaan. Heille kerrottiin tutkimuksessa esiin tulevien, organisaation kannalta positiivisten ja negatiivisten havaintojen hyötyarvo heidän organisaationsa turvallisuuden ja kyberturvallisuuskulttuurin kehittämisen kannalta.

Vastaamisen kynnyksen madaltamiseksi haastateltaville kerrattiin vielä uudelleen, että kaikki tutkimuksessa käytettävät havainnot ja lausunnot pseudonymisoitiin, jolloin ei ole mahdollista yhdistää ilmaisuja henkilöön tai tunnistaa yksittäistä henkilöä yhdistelemällä hänen ilmaisujaan. Haastattelu aloitettiin yksinkertaisilla ja henkilökohtaisilla kysymyksillä, jotta varmistetaan haastateltaville luonteva aloitus reflektoinnille ja avautumiselle (Johnson & Rowlands, 2012). Haastateltavia kannustetiin ajattelemaan ääneen ja reflektoimaan vapaasti, mutta muistutettiin aktiivisesta roolista ja tutkijan tehtävästä kysyä tarkentavia kysymyksiä ymmärryksen takaamiseksi. Tutkijan kysymissä tarkentavissa kysymyksissä käytetty terminologia oli operationalisoitu eli muotoiltu ymmärrettävälle tasolle.

Haastattelun aikana tutkija pyrki toimimaan neutraalisti ja puolueettomasti. Tutkija pyrki välttämään henkilökohtaisten mielipiteiden esittämistä tai ilmausten kommentointia. Tutkija esitti sen sijaan haastateltaville tarkentavia kysymyksiä sekä kehottamaan jatkamaan. (Hirsjärvi & Hurme, 2008). Tutkija ei ollut tutustunut etukäteen tarkemmin Reaktorin rakenteisiin, strategiaan, prosesseihin

tai organisaatiokulttuuriin, jotta tieto ei ohjaisi hänen tulkintojaan tai empiirisen materiaalin analysointia. Haastattelussa ei korjattu virheellisiä väittämiä tai osoitettu tutkijan aiempaa tietämystä aiheesta, koska tutkijan rooliin ei kuulunut uuden tiedon tuottaminen keskusteluun. Tutkija tiedosti tunnereaktioidensa vaikutuksen haastateltavien vastauksiin. Tutkija pyrki olemaan ilmaisematta mielipidettään reaktioillaan tai eleillään haastateltavien vastauksiin. (Ruusuvuori & Tiittula, 2005). Tutkija osoitti reaktioillaan ymmärtävänsä haastateltavien vastausten sisällön ja reagoi esimerkiksi humoristisiin ilmaisuihin, koska ne kuuluvat vuorovaikutukseen ja rohkaisevat haastateltavaa reflektoimaan.

Haastattelussa tunnistettiin tutkijan aktiivinen rooli, osallistuminen vuorovaikutukseen ja ennakkokäsitysten vaikutus haastattelutilanteen ohjaamiseen ja suhteen muodostumiseen haastateltavaan. Tutkijan ennakkoluulojen minimoimiseksi haastateltavien henkilökohtaiset tiedot, joita tarvittiin vastausten mahdollisiksi selittäviksi tekijöiksi, kysyttiin vasta haastattelun lopussa. (Potter & Hepburn, 2012).

Haastattelu eteni vapaasti haastateltavien kertomusten ehdoilla, koska tällaisen toteutustavan on todettu olevan hyödyllinen (Johnson & Rowlands, 2012). Haastattelun enimmäispituudeksi oli määritelty yksi tunti. Tutkija kuitenkin totesi haastattelun päättyneeksi, kun kaikki teemat oli käsitelty kattavasti, tutkijalla ei ollut epäselviä asioita eikä haastateltavalla ollut enää kysymyksiä. Suurimmassa osassa haastatteluja kului koko siihen varattu aika tai enemmän.

2.7 Haastattelun teemat

Teemat muodostettiin teoreettisen tarkastelun perusteella, jonka perusteella haastattelun tueksi muotoilluista kysymyksistä pystyttiin löytämään neljä selkeää teemaa. Kansallista kulttuuria ei käsitelty erillisenä teemana. Kansallisella kulttuurilla on Adele Da Veigan (2016) mukaan ainoastaan välillinen vaikutus kyberturvallisuuskulttuurin muodostumiseen. Teoreettisen tarkastelun perusteella sen vaikutus näkyy yksilöiden toiminnassa ja organisaatiokulttuurin muodostumisessa, eli todennäköisesti Suomen kansalliseen kulttuuriin liittyviä asioita tulee esille eri teemojen kautta.

Ensimmäinen teema oli haastateltavan tausta ja hänen arvoihinsa vaikuttaneet kulttuurit. Sen tarkoituksena oli auttaa haastateltavien vastausten ja niiden erojen tulkinnassa sekä haastateltavien näkemysten ja kokemusten erovaisuuden selittämisessä. Toinen teema oli haastateltavien henkilökohtainen kyberturvallisuuskulttuuri. Yksilöt ovat toimijoita organisaatiossa ja vaikuttavat näin organisaation kyberturvallisuuteen ja kyberturvallisuuskulttuurin muodostumiseen henkilökohtaisten käsityksiensä, taitojensa ja käytöksensä kautta. Kolmas teema oli organisaatiokulttuuri, koska siihen liittyvät arvot, tuntemukset ja yhteiset kirjoittamattomat säännöt vaikuttavat myös turvallisuus-, tietoturva- ja kyberturvallisuuskulttuurien muodostumiseen. Neljäs teema oli organisaation kyberturvallisuuskulttuuri, jota jo sivutaan aiemmissa teemoissa.

2.8 Haastateltavien valinta ja kuvaus

Tutkimuksen rajauksen ja saatavilla olevan aiemman tutkimustiedon perusteella tehtiin etukäteen rajauksia sekä oletuksia. Haastateltavat

- edustivat oletetusti mies- tai naissukupuolta. Kumpikin sukupuoli oli edustettuna, koska sen on aiemmissa tutkimuksissa todettu mahdollisesti vaikuttavan haastateltavien näkemyksiin. Yksittäisessä haastattelutapahtumassa ei pyydetty haastateltavia määrittelemään sukupuoltaan.
- edustivat vaihtelevaa ikäjakaumaa, koska Suomen koulutusjärjestelmä ja sen vaikutus yksilöiden valmiuksiin sekä käsityksiin muuttuvat jatkuvasti.
- edustivat eri henkilöstöryhmiä ja erilaisia koulutustaustoja. Tällä haluttiin saada eri lailla tietotekniikkaa ja kyberturvallisuutta osaavien sekä ymmärtävien ihmisten näkemyksiä.
- toimivat yrityksessä erilaisissa tehtävissä, jotta haastattelusta saatiin erilaisia näkökulmia tutkittavaan ilmiöön ja yksittäinen paikallinen kulttuuri ei pääse vaikuttamaan kaikkien vastaajien näkemyksiin. Haastateltavilla oli tehtäviensä vuoksi vaihteleva näkymä organisaatioon ja sen toimintaan, mikä kertoi tutkimuksen keskeisen ilmiön ilmenemisestä eri tavalla organisaation eri osissa.
- olivat työskennelleet yrityksessä vaihtelevan ajan, 2-18 vuotta, minkä nähtiin vaikuttavan heidän näkemyksiinsä yrityksen toimintamalleista ja organisaatiokulttuurista.
- ovat kasvaneet Suomen kansallisen kulttuurin vaikutuksessa.

Haastateltavat osallistuivat tutkimukseen vapaaehtoisesti työajallaan. Haastatteluajat sovittiin joustavasti, jotta ne pystyttiin yhdistämään haastateltavien muihin sovittuihin tapaamisiin ja työtehtäviin. Joustavuuden ja mahdollisuuden käyttää työaikaa haastatteluun arvioitiin vähentävän negatiivisten asenteiden vaikutusta ja kiirehtimistä haastattelun toteuttamisessa.

2.9 Aineiston analysointi

Kerätyn aineiston analysointi toteutettiin fenomenografisella analyysilla, jolle ei ole käytännössä täysin selkeästi määritettyä ja yksityiskohtaista tapaa, vaan siinä noudatetaan laadulliselle tutkimukselle ja ihmistieteille ominaisia piirteitä. Aineiston keräämisen perusyksikkö on ilmaus, jolla esitetään tapa kokea tutkimuksen kohteena oleva ilmiö tai siihen liittyviä osia. Anneli Niikon (2003) mukaan fenomenografisen analyysin keskeisiä periaatteita ovat:

- koko aineiston keräämisen ajan kestävä analyysi,
- analyysiprosessin joustavuus, systemaattisuus, loogisuus ja reflektiivisyys,

- aineiston jako merkityksellisiin osiin ilman että kokonaisuuden idea kadotetaan,
- tunnistettujen merkityksellisen yksilöiden luokittelu organisoiduksi systeemiksi,
- sisällön erilaisten ulottuvuuksien jatkuva vertailu,
- aineiston lajittelun ja organisoinnin kriteerien jalostaminen analysointiprosessin kuluessa,
- analyysin tunnustaminen käytännölliseksi toiminnaksi ja
- tulosten muodostaminen abstraktion korkeammalla eli säännöllisten mallien, piirteiden tai teemojen kuvausten sekä teoreettisten kategorioiden tasolla.

Analysointivaihe toteutettiin vaiheittain. Ensimmäisessä vaiheessa aineisto luettiin useasti läpi, pyrittiin löytämään ongelmanasettelun kannalta tärkeitä ilmauksia ja hahmotettiin haastateltavien kokonaiskäsityksiä suhteessa tutkimusongelmaan. Ilmausten analyysiyksiköt tarkentuivat aineiston perusteella. Fenomenografisessa tutkimuksessa ilmausyksikkö voi olla sana, lause, kappale, puheenvuoro tai koko haastattelu. Kielellisten ilmausten tulkinta tehtiin kontekstissa, mistä ilmaus on peräisin, mutta ilmauksista muodostuvia merkityksiä hahmotettaessa hylättiin rajat haastateltavien väliltä (Uljens, 1992; Niikko, 2003).

Analyysin toisessa vaiheessa merkityksellisiä ilmauksia ryhmiteltiin ryhmiksi ja teemoiksi. Ilmauksia vertailtiin toistensa kanssa. Tavoitteena oli tunnistaa samankaltaisuuksia, variaatioita ja eroavaisuuksia, mutta myös harvinaisuuksia tai rajatapauksia. Käsitykset ryhmiteltiin kokonaisuuksiksi, joille määritettiin kriteerit niin että niistä syntyi ajatuksellisia kokonaisuuksia. (Niikko, 2003; Marton, 1986). Suomalaisessa kulttuurikontekstissa toteutettujen haastatteluissa kerrottuja ilmaisuja ja näkemyksiä sekä niiden tulkintaa voidaan pitää lähtökohtaisesti luotettavina, koska suomalaisten kommunikaatiotyyli on tunnistettu suoraksi ja asiakeskeiseksi (Nishimura, Nevgi & Tella, 2008; Lewis, 2005; Lewis, 2006).

Analyysin kolmannessa vaiheessa määritettiin kategorioiden ominaisuuksia ja rajoja siten, että ominaisuudet syntyivät tutkijan konstruktioissa tai ne kuvattiin abstrahoimalla haastateltavien ilmauksia ja kuvattiin ydinmerkitysten termeillä. Tavoitetilassa jokainen kategoria kertoi jotain erilaista tavasta kokea tutkittava ilmiö, ja kategorioiden rajat eivät limittyneet toistensa kanssa. (Niikko, 2003; Marton, 1986). Kategorioiden rajat taattiin laadullisten erojen tuottamisella kategorioiden välille (Häkkinen, 1996).

Neljännessä vaiheessa muodostettiin tutkimustoiminnan päätulos. Kategorioita yhdistettiin teorian perusteella laajemmiksi eli kuvauskategorioiksi, joista muodostui ylätason kategoriajoukko. Kuvauskategoriat olivat abstrakteja sisältäen käsitysten ja kokemuksen ominaispiirteet. Kategoriat olivat neutraaleja suhteessa yksilöihin, kontekstiin tai elämysmaailmaan ja kuvasivat ilmiötä yleisemmällä tasolla eli antoivat kuvaa kulttuurillisista ajattelutavoista. (Niikko, 2003; Marton & Booth, 1997). Analyysiprosessin lopuksi kategoriat nimettiin ja piirrettiin kuva, jonka tavoitteena oli muodostaa ja esittää kokonaiskuva kategorioista

sekä niiden suhteesta tutkittavaan ilmiöön. Kuva esittää tutkimuksen pääasiallisen tuloksen abstrahoidulla tavalla.

2.10 Tutkimusprosessi vaiheet ja eteneminen

Tutkimusaihe valikoitui kyberturvallisuuden maisteriopintojen aikana suoritetun kurssin tutkimusraportin kirjoittamisen aikana. Tutkija kiinnostui tällöin ihmisten tavoista kokea ilmiö sekä kontekstin ja siihen vaikuttavien tekijöiden merkityksestä tutkimuksen ja ihmisten käsitysten kannalta. Tutkimusprosessi toteutettiin iteratiivisesti, jossa eri vaiheet tuottivat tarkennuksia edellisiin tai vaatimuksia seuraaville vaiheille. Iteratiivisen työskentelyotteen avulla tutkija kykeni hyödyntämään tutkimusprosessin aikana ilmiöstä, tutkimusmenetelmästä tai tutkimusprosessista lisääntynyttä ymmärrystä.

Tutkimus toteutettiin fenomenografisen tutkimuksen vaiheiden mukaan: tutkija perehtyi ensin tutkittavaan teemaan tutkimustehtävän määrittelemiseksi ja ongelmanasettelun tarkentamiseksi (Ahonen, 1994). Tämän jälkeen selvitettiin aihealueesta aiemmin tehty tutkimus, jotta kyettiin tunnistamaan tarve uudelle tutkimukselle sekä tutkimusaihetta tukevan tiedon olemassaolo tai puuttuminen. Tavoitteena oli myös selvittää, miten, milloin, miten ja missä kontekstissa tutkimuksen keskeistä ilmiötä on tutkittu, koska ne vaikuttivat tutkimusongelman asetteluun ja sen näkökulman valintaan. Tämän perusteella tutkimuksen määrittelyvaiheessa tuotettiin alustavat tutkimuskysymykset. Tässä vaiheessa tunnistettiin tarve rajata tutkimusongelmaa, jotta kokonaisuus on hallittavissa pro gradu -työssä ja valitut kokonaisuudet kyetään käsittelemään riittävällä tasolla.

Kirjallisuuskatsaus toteutettiin systemoidusti rajaamalla aihepiiri tunnistamalla tutkimuksen kannalta keskeiset käsitteet, laatimalla hyväksymis- ja poissulkukriteerit, toteuttamalla kirjallisuushaku Jyväskylän yliopiston kautta saatavilla oleviin tietokantoihin ja kirjallisuuteen sekä hakemalla hakukoneilla aihepiiriä koskevaa tietoa ja valitsemalla alkuperäistutkimukset hyväksymis- ja hylkäämiskriteerien perusteella. Systemaattisen kirjallisuuskatsauksen avulla pyrittiin takaamaan lähteiden laatu, huomioimaan kaikki aiheen kannalta olennaiset lähteet ja säilyttämään lähteiden keskinäinen yhteys (Metsämuuronen, 2011). Haasteeksi muodostui materiaalin runsas määrä, mikä johtui etenkin kulttuuria ja yksilöä koskevan tutkimuksen runsaudesta ja toteutuksesta eri näkökulmista, esimerkiksi tietotekniikan, tietojärjestelmätieteiden, tietoturvan, organisaatiopsykologian, sosiologian ja käyttäytymistieteiden tutkimusaloilla.

Kirjallisuuskatsauksen aikana määriteltiin tutkimuksen kannalta keskeiset käsitteet. Katsauksen jälkeen toteutettiin käsiteanalyysi, jonka tavoitteena oli käsitteiden ja niiden välisten suhteiden määrittely valitussa viitekehyksessä. Käsiteanalyysissa ilmeni, että tutkimus käsitteli pääasiassa teoreettisia käsitteitä, jotka koostuvat lukuisista toiminnoista ja havainnoista (Hirsjärvi ym., 2007). Teoreettisten taustalukujen kirjoittamisen aikana tarkennettiin alustavia tutkimuskysymyksiä ja tutkimuksen luotiin viitekehys. Tutkimuskysymyksiä tarkennettiin tutkimusprosessin edetessä.

Tutkimusmenetelmän hahmottelu toteutettiin kirjallisuuskatsauksen aikana. Laadullisten ja hypoteesittomien tutkimusten määrä havaittiin olevan pieni verrattuna määrällisiin tutkimuksiin. Suurin osa tietoturva- ja kyberturvallisuuskulttuuria koskevista tutkimuksista havaittiin olevan toteutettu määrällisellä tutkimusotteella ja kyselylomakkeilla, jossa tavoitteena oli todistaa ennalta asetettujen hypoteesien tai teorian paikkaansa pitävyys. Tähän mennessä toteutetut tietoturvakulttuuria koskevat laadulliset tutkimukset käsittelivät ainoastaan itse ilmiötä, eivätkä ihmisten käsityksiä ja kokemuksia ilmiöstä. Kyberturvallisuuskulttuuria koskevia laadullisia tutkimuksia löytyi vain vähän. Laadullisen tutkimusotteen valinnan jälkeen tutkija perehtyi erilaisiin tutkimusmenetelmiin. Tutkijalla oli esikäsitys fenomenografisen tutkimusotteen käyttämisestä, mutta sen hyötyjä ja toteuttamista verrattiin muihin potentiaalisiin.

Toisena vaihtoehtona oli grounded theory -tutkimusmenetelmä, joka jakaa fenomenografisen tutkimusmenetelmän kanssa muun muassa aineistolähtöisyyden ja tutkijan ajattelun merkityksen. Grounded theoryn on todettu soveltuvan tutkimusaiheeseen, josta on olemassa vain vähän tutkimusta. (Eskola & Suoranta, 1998; Strauss & Corbin, 2008). Fenomenografia valittiin tutkimusmenetelmäksi, koska tutkittava ilmiönä oleva kyberturvallisuuskulttuuri on subjektiivinen ilmiö. Tutkija halusi antaa painoarvoa erilaisille tavoille kokea ja käsittää ilmiö.

Tutkimusmenetelmään perehtyessä haastattelututkimus valikoitui tiedonkeruumenetelmäksi, koska se soveltuu erinomaisesti haastateltavien käsitysten ja kokemusten tutkimiseen. Puolistrukturoitu lomaketutkimus päädyttiin sulkemaan pois, koska yksilöt kokevat ja ymmärtävät kulttuuriin liittyvät tekijät eri tavoin ja tutkimusaiheen käsittely vaatii vuorovaikutusta haastattelutilanteessa (Ahonen, 1994). Teemahaastattelun valinta aineistonkeruumenetelmäksi vaikutti mahdollistavan parhaiten haastateltavien todellisten kokemusten ja ajatusten sekä tutkittavien ilmiöiden vivahteiden esiin tuomisen (Hirsjärvi & Hurme, 2008). Haastattelut päätettiin nauhoittaa, jotta materiaali voitiin käydä useasti läpi eri näkökulmista ja tarkistaa tutkijan ymmärrys ilmaisujen sisällöstä ja merkityksistä.

Ennen tiedonkeruuta tutkija perehtyi haastattelujen toteuttamiseen useiden teosten ja artikkelien avulla. Haastatteluvaiheen suunnittelussa tunnistettiin tärkeäksi mahdollisimman samanlaisen haastatteluolosuhteiden muodostamiselle, jotta ajankohta, paikka tai motiivi haastatteluun osallistumiseen ei vaihtelisi merkittävästi haastateltavien välillä. Aikataulusyistä haastattelut jouduttiin toteuttamaan työpäivän eri aikoina, mikä saattoi vaikuttaa haastateltavien vireystilaan ja reflektioon.

Analyysivaiheessa materiaalin purkamisen jälkeen materiaali käytiin läpi useaan kertaan ja sitä verrattiin ensimmäisellä kerralla muodostettuun kategorisointiin. Tämän jälkeen alatason kategorioita yhdisteltiin ylemmän tason kategorioiksi ja kuvauskategorioiksi. Analyysivaiheen kirjoitusvaiheessa tunnistettiin tarve yhdistellä alatason kategorioita, koska ilmauksissa oli päällekkäisyyksiä sekä pyrittiin välttämään toistoa ja parantamaan luettavuutta. Analyysivaiheen kappaleissa käytettiin runsaasti yksittäisiä ilmauksia havainnollistamaan ja

konkretisoimaan niiden merkitystä tutkimukselle. Tutkimuskysymyksiin vastattiin hyödyntämällä kuvauskategorioita ja tukemalla niitä alakategorioilla.

Viimeistelyvaiheessa tarkennettiin prosessin aikana syntyneitä kappaleita tutkimuksen luotettavuudesta ja jatkotutkimusaiheista. Ulkopuoliset henkilöt lukivat tutkimuksen ja kommentoivat sen ymmärrettävyyttä, kieliasua, selkeyttä ja ajattelun loogisuutta. Tutkija pyysi tutkimuksen ohjaajaa havainnoimaan puutteita ja ehdottamaan muutoksia tutkimuksen sisältöön ja rakenteeseen. Lopussa tutkija hioi sisältöä palautteiden sekä havaintojensa perusteella ja teki tekstille oikoluvun. Tutkimusprosessin ja -vaiheiden eteneminen on esitetty kuvassa 1.

Tutkimusprosessin eteneminen

Tutkimuksen vaiheiden eteneminen

I. Tutkimuksen määrittely	II. Teoreettinen tarkastelu	III. Menetelmä-osuus	IV. Tiedonkeruu	V. Analyysi	VI. Raportointi	VII. Viimeistely
1. Aiempaan tutkimukseen perehtyminen	1. Kirjallisuus-katsauksen toteuttaminen	1. Tutkimus-menetelmiin perehtyminen	1. Haastattelujen järjestelyjen sopiminen	1. Haastattelu-materiaalin purkaminen ilmaisuiksi	1. Tutkimus-kysymyksiin vastaaminen	1. Pohdinnan kirjoittaminen
2. Aiheen ja näkökulman valinta	2. Keskeisten käsitteiden määrittely	2. Tutkimus-menetelmän valinta	2. Haastattelu-tekniikkaan perehtyminen	2. Ilmaisujen ryhmittely	2. Johto-päätösten kirjoittaminen	2. Tutkimuksen luetuttaminen ulkopuolisilla ja ohjaajalla
3. Keskeisten käsitteiden tunnistaminen	3. Teoriataustan kirjoittaminen	3. Valittuun menetelmään perehtyminen	3. Haastattelujen toteuttamisen suunnittelu ja kuvaaminen	3. Kategorioiden muodostaminen		3. Korjaukset palautteen perusteella
4. Tutkimuksen rajaaminen	4. Haastattelun teemojen valinta	4. Menetelmän soveltamiseen liittyvät valinnat	4. Haastattelujen valmistelu	4. Analyysin kirjoittaminen		4. Tutkimuksen hiominen ja oikoluku
5. Alustavien tutkimus-kysymysten muodostaminen	5. Tutkimus-kysymysten tarkentaminen	5. Kohde-organisaation valinta ja sopiminen	5. Haastattelujen toteuttaminen			5. Tutkimuksen lähettäminen arviointiin

Kuva 1. Kuvaus tutkimusprosessin vaiheista ja etenemisestä

3 Kulttuurin vaikutus kyberturvallisuutta koskeviin asenteisiin, tapoihin ja käsityksiin

Tutkittaessa käyttäjien toimintaa tietoturvan tai kyberturvallisuuden näkökulmasta on kulttuuri yksi keskeisistä tekijöistä. Yksilö toimii aina tietyssä kontekstissa, jossa hänen käsityksiensä syntyyn ja toimintaan on vaikuttanut ja kohdistuu usean kulttuurin ja alakulttuurin vaikutuksia. Edgar Scheinin ja Peter Schneierin (2017) mukaan kulttuuri on ryhmän oppima ilmiö vastaavalla tavalla kuin luonne ja persoona ovat yksilölle. Kulttuuri on jotain mikä erottaa ihmisryhmän toisesta, mikä tarkoittaa arvojen, merkitysten ja normien jakamista (Hofstede, 1991). Edward Hall (1981) painottaa, että yksilö oppii ja omaksuu osia kulttuurista vuorovaikutuksen kautta ilman että kulttuuria voi erikseen opettaa. Vuorovaikutus on suurimmilta osin muuta kuin puheen sisältöä eli käytösmalleja ja käyttäytymistä ohjaavia eleitä, jotka tapahtuvat tiedostetusti tai tiedostamattomasti. Kulttuuri muodostuu ihmisryhmän keskuudessa, vaikka sitä ei erikseen yritettäisi muodostaa. Kulttuuri vaikuttaa yksilön käsitykseen ja kokemuksiin ajasta, aikasykleistä, tilasta ja rajoista sekä oppimisesta ja opettamisesta. (Hall, 1981).

Kulttuurista omaksuttavat asiat voidaan jakaa arvoihin ja käytänteisiin. Arvot liittyvät yksilön kykyyn vertailla sisäsyntyisesti eri vaihtoehtoja ja valita niistä henkilökohtaisesti tai sosiaalisesti sopivin vaihtoehto. Arvojärjestelmä kertoo hyväksyttävät käyttäytymismallit ja halutut lopputilanteet. (Rokeach, 1973). Arvot omaksutaan kasvu- ja elinympäristön, koulutuksen ja vuorovaikutuksen kautta. Ne integroituvat osaksi persoonaa, mutta voivat muuttua kulttuurinmuutoksen ja elämänkokemusten myötä. (Karahanna ym., 2005).

Arvot liittyvät kulttuuristamme omaksumiin tiedostamattomiin käsityksiin ja tapoihin, miten toimia eri tilanteissa suhteessa esimerkiksi vastuun ottamiseen, asioiden kiireellisyyteen, aloitteellisuuteen, ennakkoluuloihin ja työkalujen käyttöön. Kaikista näistä on löydettävissä kolmen eri tason asioita: muodollisella tasolla yksilöllä on tiedostamaton käsitys siitä, miten asioiden kuuluu olla. Epämuodollisella tasolla yksilöllä on tiedostettu käsitys siitä, miten asioiden tulee ilmetä käytännössä. Teknisellä tasolla, miten asia tulee toteuttaa käytännön sovellutuksissa, esimerkiksi tekniikoissa, työkaluissa ja järjestelmissä. (Hall, 1981). Keskeistä on ymmärtää kulttuurin jakautuminen näkyvään ja tiedostettuun sekä tiedostamattomaan ja salattuun tasoon. Tämän vuoksi näkyvä asia, esimerkiksi ele, voi saada täysin päinvastaisen merkityksen kahden eri kulttuurin kontekstissa. Kulttuurin salatut osat puolestaan paljastavat asioita kulttuurin arvoista. Kulttuuri määrittää sen mihin asioihin kiinnitämme huomiota ensiksi, mille annamme arvoa ja esimerkiksi yleisesti hyväksyttyjä tapoja ilmaista statusta ulkoisten merkkien tai käytöksen avulla. Yksilö hyödyntää kulttuurien tiedostamattomia osia toimiessaan intuitiolla, kun näkyvät osat ilmenevät esimerkiksi tiedostettujen käytösmallien kautta. (Hall, 1976).

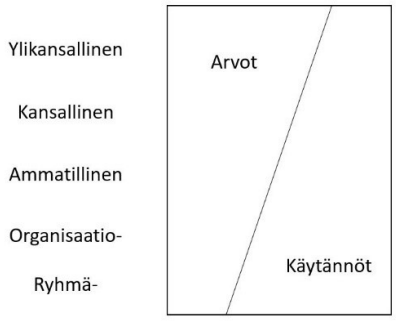
Schein ja Schneier (2017) esittävät kulttuurin jaon neljään tasoon: makrokulttuurit, jotka sisältävät kansat ja monikansalliset yritykset, organisaatiot,

organisaatioiden sisällä toimivien ryhmien alakulttuurit ja organisaatioiden kanssa tai sisällä toimivat mikrokulttuurit. Sen vuoksi tässä tutkimuksessa yksilön toimintaan vaikuttavat asiat on jaettu seuraaviin kokonaisuuksiin: kansalliseen ja organisaatiokulttuuriin, ammatillisiin alakulttuureihin ja henkilökohtaisiin ominaisuuksiin, jotka vaikuttavat toisiinsa yksilön ja ihmisryhmien asenteen, aikomusten ja toiminnan kautta.

Tässä kappaleessa käsitellään eri kulttuurien vaikutusta yksilöiden tietoturvaa ja kyberturvallisuutta koskevien käsitysten muodostumiseen. Tutkimuksessa on tarkoituksella rajattu kulttuuri kattamaan ainoastaan edellä mainitut kokonaisuudet siksi, että aiheiden käsittelyä oli tarve rajata tutkimuksen laajuuden vuoksi. Luvun lopussa esitellään Suomen kansallisen kulttuurin piirteitä ja eroavaisuudet verrattuna muihin pohjoismaihin.

3.1 Kulttuurin vaikutus yksilön arvoihin ja toimintaan

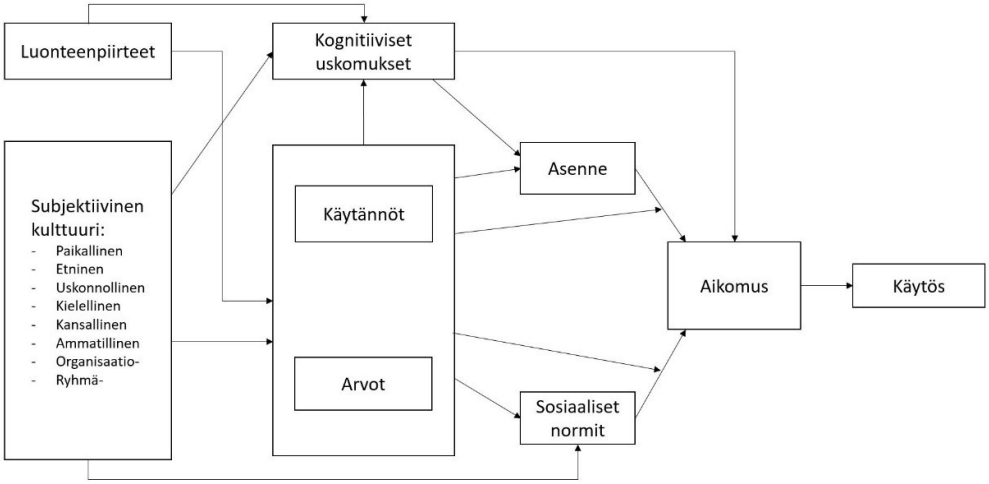
Koska tutkimuksen kohteena ovat käyttäjät, on olennaista ymmärtää se, miten yksilöt omaksuvat arvoja ja käytänteitä niistä viiteryhmistä, joissa hän toimii. Geert Hofstede (1991) jakaa kulttuurit korkeampiin ja matalampiin tasoihin riippuen siitä vaikuttavatko ne enemmän arvoihin vai käytäntöihin (kuva 2). Kulttuurin korkeammat tasot, esimerkiksi etniset, uskonnolliset ja muiden viiteryhmien kulttuurit, vaikuttavat enemmän yksilön arvoihin. Matalamman tason kulttuurit, esimerkiksi ammatilliset ja organisaatiokulttuurit sekä organisaation sisällä toimivien ryhmien kulttuurit, vaikuttavat enemmän käytäntöihin. (Hofstede, 1991).



Kuva 2. Eri tasojen kulttuurien vaikutus yksilön arvoihin ja käytäntöihin (Hofstede, 1991)

Eri kulttuurien vaikutuksen yksilöön tietyssä tilanteessa on todettu riippuvan tilanteen luonteesta ja kontekstista, painottuuko siinä sosiaalinen kanssakäyminen vai toiminta. Korkeamman tason kulttuureilla on enemmän vaikutusta toimintaan, jossa yksilön täytyy tehdä valintoja arvojensa perusteella. Mikäli tilanteessa toimintaan vaikuttavat käytännöt arvoja enemmän, on ammatillisella ja organisaatiokulttuurilla enemmän vaikutusta. (Karahanna ym., 2005).

Kulttuurin vaikutus yksilön asenteeseen tietoturvaa kohtaan on tunnistettu merkittäväksi (Mishra & Dhillon, 2006; Rocha Flores ym., 2014; Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville, 2013), minkä vuoksi käyttäytymistieteiden, sosiologian ja psykologian kulttuuria koskevissa tutkimuksissa ihmistä koskevat havainnot on todettu soveltuvan esimerkiksi tietoturvaohjeiden noudattamisen tutkimiseen. Vallitseva kulttuuri voi tukea tai heikentää yksilön asennetta tietoturvaa kohtaan. Asenteen puolestaan on tunnistettu olevan suoraan sidoksissa aikomukseen toimia, jonka puolestaan on todettu ennustavan käytöstä eli turvallisuuteen liittyvien toimenpiteiden toteuttamista tai toteuttamatta jättämistä. (Crossler ym., 2013; Lebek, Uffen, Neumann, Hohler, & Breitner, 2014; Siponen, Mahmood & Pahnila, 2014). Kulttuuri vaikuttaa myös välillisesti yksilöön, sillä sosiaalisen kognitiivisen teorian mukaan sosiaalinen ympäristö vaikuttaa yksilön käyttäytymisen muodostumiseen. Käyttäytymiseen vaikuttavia tekijöitä ovat muun muassa muiden ihmisten suunnalta tuleva rohkaisu, tietoturvaan liittyvä osaaminen (*eng.* self-efficacy), odotukset lopputuloksesta, välineellinen tuki ja toisten ihmisten tietoturvakäytännöt (Galvez, 2015; Johnston, Warkentin & Siponen, 2015; Paternoster, Bachman, Bushway, Kerrison & O'Connell, 2015). Kuvassa 3 on hahmotettu eri kulttuurien vaikutusta yksilön käytökseen.



Kuva 3. Yksilön käytökseen vaikuttavat tekijät (Karahanna ym., 2005)

3.2 Kansallinen kulttuuri ja sen vaikutus yksilöön

Kansallisen kulttuurin muodostumiseen ovat vaikuttaneet kansakunnan historia, taloudellinen kehitys, uskonto ja filosofia. Ihmisten ja yhteiskuntien arvot linkittyvät tapoihin tuottaa ravintoa ja hankkia vaurautta. Filosofia ja uskonto ovat muovanneet ihmisten käsityksiä vuorovaikutuksesta ja yhteistyöstä sekä myös tuottaneet selviytymismalleja. Näin teoria ja käytäntö ovat luoneet perustan, jonka perusteella yhteiskuntien ja kulttuurien käyttäytymisnormit ja jaetut arvot

ovat kehittyneet. (Barry, Child & Bacon, 1959; Ross, Nisbett & Gladwell, 2011). Robert Bartels (1967) oli ensimmäisiä, joka tutkimuksessaan tunnisti kulttuurin merkityksen ja löysi kulttuurierojen kuvaamiseen muutamia kriteerejä: lainsäädännön, yksilöllisyyden kunnioittamisen, vallan ja auktoriteetin luonteen, omistusoikeuden, jumalakäsityksen, yksilön suhteen valtioon, kansallisen identiteetin ja uskollisuuden sekä arvot ja tavat.

Kulttuuri on arvojen ja sosiaalisten normien perusta, minkä kautta useat eri kulttuurit vaikuttavat myös yksilöiden aikeisiin ja käyttäytymiseen. Kansallinen kulttuuri vaikuttaa oppilaitosten kautta yksilöiden maailmankuvaan heidän rakentaessaan kognitiivisia malleja ja selviytymisstrategioita (Sagiv & Schwartz, 2007). Yksilöiden omaksumilla kulttuurin osilla on korkea kyky vastustaa muutosta, mikä korostaa erilaisten kulttuurien merkitystä (Hall, 1981; Fukuyama, 1985; Hofstede, 1999). Tämän vuoksi kulttuurien vaikutuksen tunnistaminen on merkittävää erityisesti toimittaessa globaalissa ympäristössä (Rocha Flores ym., 2014).

Francis Fukuyaman (1985) mukaan yhteiskunnat voidaan jakaa matalan ja korkean luottamuksen kategorioihin, jotka kuvaavat kuinka helppoa ihmisten on luottaa toisiinsa sekä luoda erilaisia ryhmiä ja suhteita. Etenkin matalan luottamuksen kulttuureissa luottamuksen rakentamisen prosessi on keskeinen, koska luottamus toimii innovatiivisuutta ja talouskasvua tukevana katalyyttina. Luottamus vaikuttaa ihmisten tapaa kokea uhkia sekä asenteeseen riskejä ja yksityisyyttä kohtaan. Myös sosiaalisella pääomalla on tärkeä rooli kansallisessa kulttuurissa. (Fukuyama, 1985).

Kansallisista kulttuureista voidaan tunnistaa alueellisia eroja. Eurooppalaisten sivilisaatioiden arvot perustuvat Aristoteleen ja muiden suurten filosofien ajatuksiin ja näkemyksiin. Muinainen kreikkalainen filosofia korosti vapautta, yksilöllisyyttä, optimismia, vastuuta ja aloitteellisuutta. Huolimatta myöhempää, useissa Euroopan maissa ilmennyttä, kollektivismin merkityksen korostamista, kreikkalaisen filosofian arvot nähtiin ennen ja nähdään edelleen hyveinä eurooppalaisissa ja pohjoisamerikkalaisissa kulttuureissa. Aasiassa puolestaan kulttuurien perusta on lähtökohtaisesti buddhalaisuudessa, taolaisuudessa ja kungfutselaisuudessa. Niissä korostetaan harmoniaa, itsesäätelyä ja -kontrollia, harmoniaa muiden kanssa sekä toisten tukemista. (Nisbett & Masuda, 2003; Chen & Zahedi, 2016). Aasialaisten ja läntisten kulttuurien erot vaikuttavat myös käyttäjien asenteisiin, aikomuksiin ja käytökseen liittyen tietoturvauhkiin sekä tapoihin toimia havaittaessa tietoturvauhkia ja jaettaessa tietoa organisaation sisällä. Dinev, Goo, Hu & Nam (2009) havaitsivat tutkimuksessaan, että yksilön vastuuta, aloitteellisuuta ja tiedonjakoa korostavissa läntisissä kulttuureissa tietoisuuden lisääminen uhkista näyttelee suurempaa roolia kuin aasialaisissa kulttuureissa, joissa puolestaan yksilöt pitäytyvät enemmän normien ja ohjesääntöjen noudattamisessa.

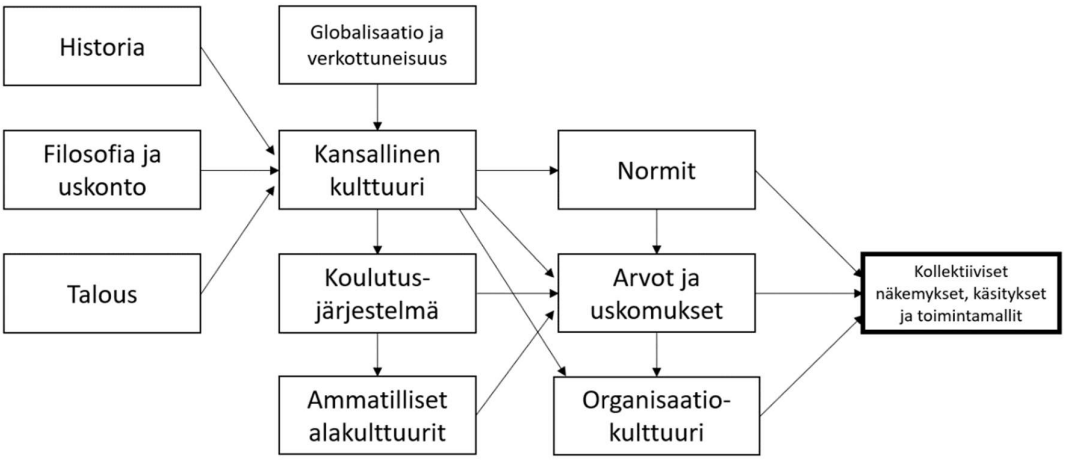
Kansallinen kulttuuri luo olosuhteet esimerkiksi paikallisille ja organisaatiokulttuureille. Kansallinen kulttuuri vaikuttaa organisaatiokulttuuriin asettamalla joukon lakeja ja normeja, joiden mukaan organisaatioiden on toimittava. Lisäksi kansallisen kulttuurin ominaispiirteet asettavat näkymättömiä ja

kirjoittamattomia toimintamalleja, jotka vaikuttavat organisaatiorakenteiden suunnitteluun, prosessien luomiseen ja turvallisuustiedon jakamiseen (Rocha Flores ym., 2014).

Kansallisen kulttuurin ominaisuuksia on myös ihmisjoukon ja yksilöiden teknologian käytön taso ja historia, minkä on tunnistettu vaikuttavan ihmisten käsityksiin. Kansojen ja ihmisjoukkojen välillä on demografisia eroja esimerkiksi kokemuksissa internet-palvelujen käytöstä, mikä täytyy ottaa huomioon heidän näkemyksiinsä arvioitaessa ja eri kulttuurikonteksteissa toteutettujen tutkimusten tuloksia verrattaessa. Tietoturvaa koskevien tutkimustulosten yleistettävyyttä rajoittaa havainto siitä, että myös kansojen ja kulttuurien sisällä on havaittu ilmenevän vaihtelua asenteissa luottamusta ja yksityisyyttä kohtaan. Alueellisten kulttuurierojen vaikutus vaihtelee kansallisten kulttuurien välillä, joten erot täytyy tarkastella aina tapauskohtaisesti. (Dinev, Bellotto, Hart, Russo, Serra & Colautti, 2006).

Globalisaatio ja globaalit kommunikaatiojärjestelmät, kuten internet, ovat tuoneet peruuttamattomia muutoksia edistämällä keskinäisriippuvuuksia, monikulttuurisuutta ja kulttuurillista vaihtelua kulttuurien sisällä. On syntynyt globaali ideoiden foorumi, josta ihmiset voivat valita ideoita ja näkökulmia yhdistääkseen niitä käsityksiin itsestään sen sijaan, että he voisivat tukea vain ympäröivän kulttuurin ajatuksia ja perinteitä (Berry, 2008). Kulttuurit ovat jatkuvassa muutoksen tilassa. Niihin vaikuttavia tekijöitä ovat muun muassa matkustamisen lisääntyminen, maahanmuutto ja lähes kaikille elämänalueille tunkeutunut tietokoneiden käyttö. Edellä mainitut tekijät tekevät yksilön kulttuurillisesta identiteetistä lisääntyvissä määrin dynaamisen ja yksilöiden kulttuurilliseen identiteettiin voi kuulua usean eri kansallisen kulttuurin piirteitä. (Krumov & Larsen, 2013).

Globalisaatio on aiheuttanut kulttuurillista rapautumista ja kulttuurierojen vähenemistä. Mark Clevelandin (2016) tutkimuksessa havaittiin kuitenkin, että globaalin kulutuskulttuurin omaksumiseen ei ole vaikuttanut ainoastaan hinta ja laatu, vaan myös sosiologiset tekijät, jotka heijastivat paikallisen kulttuurin arvoja ja mieltymyksiä. Välitön yhteys yhteiskuntien yhdistymisen ja globaalin yhdenmukaisuuden välillä ei ole todellisuutta tietoturva-alalla, vaikka kulttuurit ja yksilöt omaksuvat trendejä ja tapoja globaalista yhteydestä. Globaalin viestintäteknologian omaksuminen kuitenkin altistaa yksilöitä globaaleille massa- ja sosiaalisille medioille, mikä lisää yksilöiden tietoisuutta tietoturvaa kohtaan olemassa olevista riskeistä ja uhkista. (Walsham, 2002). Kuvassa 4 on esitetty yhteenveto erilaisiin ryhmiin vaikuttavista tekijöistä.



Kuva 4. Kollektiivisiin näkemyksiin, käsityksiin ja toimintamalleihin vaikuttavia tekijöitä

Geert Hofstede (2010) näkee kulttuurin kollektiivisena ilmiönä, jota määrittävät kirjoittamattomat säännöt. Hänen hypoteesinsa mukaan kulttuuri on kollektiivista mielen ohjelmointia, joka erottaa yhden ihmisryhmän muista. Hän erottaa kuusi ulottuvuutta, joita voidaan käyttää määrittämään demografisen alueen kulttuurillisia ominaisuuksia vertailtaessa eri kulttuurien samankaltaisuuksia ja eroavaisuuksia (taulukko 1). (Hofstede ym., 2010).

Ulottuvuus	**Kulttuurillisen ulottuvuuden merkitys**
Individualismi (Individualism)	Yksilön mahdollisuus tehdä päätöksiä ja tuntea olonsa itsenäiseksi sen sijaan, että olisi riippuvainen muista (kollektivismi).
Valtaetäisyys (Power distance)	Tapa, jolla organisaatioiden ja instituutioiden vähemmän valtaa omaavat ihmiset kokevat vallanjaon tasapuolisuuden.
Maskuliinisuus (masculinity)	Kuinka avoimesti sukupuolittunut yhteiskunta on ja kuinka vahvat odotukset ovat tunteellisia sukupuolirooleja kohtaan. Maskuliinisemmissa yhteiskunnissa sukupuoliroolit ja rajat ovat vahvempia.
Epävarmuuden välttäminen (Uncertainty avoidance)	Kuinka yhteiskunnan jäsenet kokevat epävarmuuden: miten he pystyvät käsittelemään epävarmuutta ilman ahdistusta tai miten he yrittävät käsitellä sitä rutiinien tai rituaalien avulla.
Pitkän aikavälin orientaatio (Long-term orientation)	Pitkälle aikavälille orientoituneen yhteiskunnan asenne muutosta kohtaan on joustava ja muutos nähdään jatkuvana maailman kehityksenä. Kulttuuri lyhyelle aikavälille orientoituneessa yhteiskunnassa nähdään muuttumattomana.
Suopeus (Indulgence)	Suopeassa kulttuurissa vapaus nähdään hyvänä ja suvaitsevaisuus liittyy mahdollisuuteen toimia oman tahdon mukaan ja sen eteen, minkä näkee tärkeäksi. Rajoittuneessa

	kulttuurissa elämä on kovaa ja tuntuu enemmän velvollisuudelta.

Taulukko 1. Hofsteden hypoteesin kuusi ulottuvuutta (Hofstede ym., 2010)

Hofstede (2010) esittää hypoteesinsa perusteella muun muassa, että matalampi individualismin taso kansallisessa kulttuurissa tukee ihmisten uskollisuutta suurempaan joukkoon, esimerkiksi yritykseen, organisaatioon, yhteiskuntaan enemmän kuin vain itseensä ja perheeseensä. Matalamman individualismin tason on havaittu vaativan vähemmän virallista työntekijän käyttäytymisen säätelyä, koska uskollisuuden arvostaminen näkyy kollektiivisena käytöksenä ja esimerkiksi korkeampana tietoturvaohjeiden noudattamisena (Rocha Flores ym., 2014).

Geert Hofsteden luomaa kuuden kulttuurillisen dimension mallia on kritisoitu muun muassa siitä, että se kuvaa kansan yhtenäisenä eikä ota huomioon esimerkiksi alueellisia eroja. Suurin osa kansoista koostuu joka tapauksessa erilaisista etnisistä joukoista. Kansa ei ole sopiva yksikkö kulttuurintutkimuksessa, koska kulttuuria ei myöskään sido valtioiden rajat (McSweeney, 2000; Jones, 2007). Lisäksi Hofstede jättää huomiotta yhteisön merkityksen ja yhteisöjen yksilöön kohdistuvien vaikutusten erot. Hofsteden alkuperäisen tutkimuksen tiedonkeruu toteutettiin 1970-luvulla, minkä jälkeen globalisaatio, teknologian kehityksen ja laajan käyttöönoton vaikutukset yksilöiden jokapäiväiseen elämään sekä kansainvälistyminen ovat vaikuttaneet kansallisiin kulttuureihin. (Jones, 2007). Hofsteden tutkimus toteutettiin yhdessä monikansallisessa yrityksessä eli tietyssä kontekstissa, mutta toisaalta se rajasi pois eri yritysten ja toimialojen erityispiirteiden ja yritysten sääntöjen sekä toimintaohjeiden vaikutuksen (Hofstede, 1980).

Hofsteden tutkimukseen kohdistuva kritiikki tukee ajatusta siitä, että kansallista kulttuuria koskeva tutkimus on vain suuntaa antavaa eikä se tuota absoluuttisia totuuksia. Huolimatta tutkimuksen saamasta kritiikistä, Hofsteden tutkimus soveltuu käytettäväksi tässä tutkimuksessa yhtenä kansallisen kulttuurin perustutkimuksena, jota vasten peilataan empiirisen osuuden aikana kerättyä materiaalia.

3.3 Organisaatiokulttuuri sekä sen vaikutus organisaation tietoturvaan ja kyberturvallisuuteen

Organisaatiokulttuurin voi lyhyesti tiivistää määritelmään ”miten asiat organisaatiossa tehdään”. Organisaatiokulttuuri kattaa sekä näkyvän sääntelyn että vakiintuneet käytännöt ja toimintamallit. Smircich (1983) määrittelee organisaatiokulttuurin jaetuiksi keskeisiksi arvoiksi ja uskomuksiksi, mikä sisältää myös prosessit ja käytösmallit. Organisaatiokulttuurilla on organisaatiolle neljä päätoimintoa: rakentaa organisaation jäsenten identiteettiä, luoda sitoutuneisuutta laajempaan kokonaisuuteen, lisätä sosiaalisen järjestelmän vakautta ja ohjata organisaation jäsenten käytöstä. Organisaatiokulttuuri luodaan ja se on olemassa siitä

huolimatta, onko se luotu tarkoituksella vai muotoutunut ilman johdon ohjausta. (Smircich, 1983). Richard Lewis (2006) painottaa kuitenkin johtamisen ja organisaatiokulttuurin olevan hyvin kulttuurisidonnaista, koska eri kulttuureissa arvostetaan sekä odotetaan eri asioita ja erilaisia toimintatapoja. Koko johtamisen käsite sekä auktoriteetin lähtökohdat ja tarve vaihtelevat kansallisen kulttuurin mukaan (Lewis, 2006).

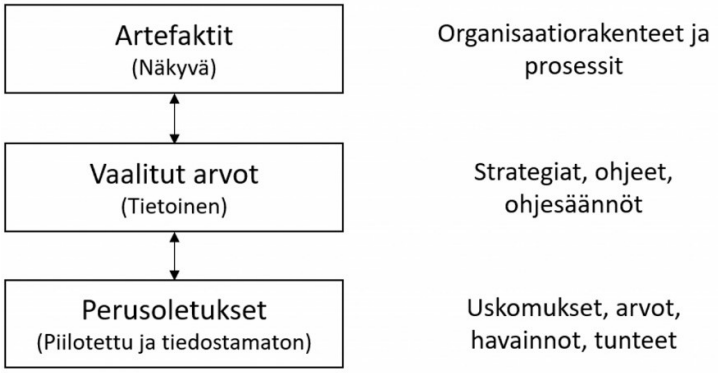
Organisaatiokulttuuri matalamman tason kulttuurina vaikuttaa enemmän yksilöiden käytäntöihin kuin arvoihin (Hofstede, 1991). Kansallisen kulttuurin ja organisaatiokulttuurin suhteesta ei ole täysin yksimielistä käsitystä: kansallisen kulttuurin on havaittu vaikuttavan vahvasti organisaatioiden arvoihin ja organisaatiokulttuuriin (Hofstede ym., 1990). Kansallisen kulttuurin vaikutus heijastuu koulutusjärjestelmän ja yksilöiden kautta. Organisaatiokulttuuri voi myös ylittää kansallisen kulttuurin vaikutukset (Nelson & Gopalan, 2003; Selmer & De Leon, 1996). Edellä mainitut johtopäätöksiltään eroavat tutkimukset oli kuitenkin toteutettu eri maissa ja kulttuurikonteksteissa, joten on mahdollista, että kansallisen ja organisaatiokulttuurin välinen suhde ja vaikutukset yksilöihin riippuvat tutkimuksen kontekstista. Suomen kulttuurikontekstissa asiaa ei ole tutkittu.

Edgar Schein (1985; 1999) jakaa organisaatiokulttuurin kolmeen eri kerrokseen: artefakteihin ja luomuksiin, arvoihin ja uskomuksiin sekä perusoletuksiin (kuva 5). Nämä kerrokset sisältävät näkyviä ja näkymättömiä elementtejä, jotka vaikuttavat organisaation toimintaan. Ensimmäinen kerros on näkyvä, ja se koostuu artefakteista ja luomuksista, jotka tieto- ja kyberturvallisuuden kontekstissa voidaan ymmärtää organisaation rakenteiksi ja prosesseiksi. Artefakteihin kuuluvat kaikki organisaation näkyvät ja julkaistut asiat, esimerkiksi pukeutumiskoodi, organisaatiossa noudatettu käyttäytymis- ja puhuttelutapa sekä kieli. Artefaktit ovat kaikki se, minkä tietyn kulttuurin edustajan kohdatessaan voi nähdä, kuulla tai tuntea. (Schein, 1985; 1999).

Toinen kerros on tiedostettu ja osittain näkyvä. Se koostuu strategioista, tavoitteista, uskomuksista ja filosofioista. Strategioihin sisältyvillä organisaation arvoilla tulee olla kiinteä suhde ohjausasiakirjoihin ja ohjeisiin, jotta ne voivat olla tehokkaita ja hyödyllisiä organisaation toiminnan kannalta. Tietyt arvot voidaan vahvistaa ryhmän tai organisaation jaetun kokemuksen kautta, jolloin niistä voi tulla ensin uskomuksia ja kehittyä sen jälkeen perusoletuksiksi. Mikäli vaalitut arvot ja uskomukset ovat yhteneviä vallitsevien perusoletusten kanssa, niiden ilmaiseminen toiminnan filosofiana voi yhdistää organisaatiota sekä toimia sen identiteetin perustana ja ydintehtävänä. (Schein, 1999). Organisaation arvoja pohdittaessa tulee huomioida yhdenmukaisuus siihen vaikuttavien kansallisten kulttuurien arvojen kanssa. Esimerkiksi tietoturvallisuusohjeet ja -ohjesäännöt täytyy suunnitella vastaamaan organisaation edustamia arvoja, mikäli niillä halutaan saavuttaa positiivisia vaikutuksia (Kolkowska, 2011; Hsu, 2009).

Kolmas kerros kostuu tiedostamattomista asioista: perusoletuksista ja tunteista. Kerros on näkymätön ja abstrakti. Sitä ei voi kuvata tarkasti, vaikka sillä on perustavanlaatuisia vaikutuksia ihmisten toimintaan. Kolmas kerros on ymmärryksen ja hyväksynnän syvin taso. Perusoletukset ovat niin yleisesti hyväksyttyjä asioita, että niissä on organisaation sisällä ainoastaan vähän vaihtelua.

Tälle yhteisymmärryksen tasolle päästään ainoastaan toistamalla ja toteuttamalla organisaation arvoja ja uskomuksia. Perusoletuksia on niiden omaksumisen jälkeen äärimmäisen vaikea muuttaa, koska ne ovat organisaation identiteetin perusta. Niiden muuttaminen heikentää organisaation vakautta ja yksilöiden kognitiivisia malleja ja järkyttää sitä kognitiivista vakautta, jota ihminen tarvitsee. Tiedostamattomat mallit ohjaavat ihmisten jokapäiväistä käytöstä tavalla, joka eroaa heidän tiedostetuista käsityksistään (Schein, 1999). Tiedostamattomat mallit koskevat koskee myös turvallisuuden kannalta haluttua ja hyväksyttyä käytöstä.



Kuva 5. Organisaatiokulttuurin rakenne Scheinin (1999) tutkimuksen perusteella

Organisaatiokulttuuria ei tule arvioida tutkimalla pelkästään yhtä tasoa, vaan sitä tulee tutkia kokonaisuutena. Esimerkiksi artefaktien kautta organisaation toimintaa on helppo havainnoida, mutta vaikea selittää. Organisaation ulkopuolinen voi kertoa, mitä hän havaitsee ja tuntee, mutta ei voi arvioida mitä merkityksiä artefakteilla on organisaation jäsenille tai heijastavatko ne jotain tiedostamattomia perusoletuksia. Organisaation arviointi artefaktien perusteella on erityisen vaarallista, koska arvioijan tulkinta on väistämättä heijastus hänen tunteistaan ja reaktioistaan. (Schein, 1999).

Scheinin kolmikerroksinen organisaatiokulttuurin malli nähdään hyödyllisenä työkaluna analysoitaessa työntekijöiden arvoja turvallisuuskulttuurin kontekstissa (Kolkowska, 2011). Organisaatio voi tietoturvan ja kyberturvallisuuden lisäämiseksi esimerkiksi pyrkiä vaikuttamaan työntekijöihin tiedostamattomiin tasolla ylläpitämällä turvallisuuskulttuuria. Arvoihin vaikutettaessa täytyy kuitenkin analysoida työntekijöiden sanoja ja käytöstä (Kluckhohn, 1951). Tarve tähän perustuu mahdollisiin ristiriitoihin työntekijöiden ja organisaation esitettyjen sekä todellisten arvojen välillä.

Kun työntekijät valitsevat erilaisia ratkaisumalleja, organisaation toimintamallit ja kulttuuri ohjaavat työntekijöiden käyttäytymistä ja toimintaa. Tietoturva-alalla on tehty laajasti tutkimusta esimerkiksi tietoturvaohjeista ja niiden noudattamisen tai noudattamatta jättämisen syistä. Aiemmat mallit tietoturvaohjeiden noudattamien ja tietoturvallisen käytöksen lisäämisestä ovat perustuneet pääasiassa käyttäjien valvontaan, ohjaamiseen tai rankaisemiseen. Niin sanottuja pehmeitä asioita, esimerkiksi normeja tai tunteita edustavien muuttujien

on kuitenkin todettu ennustavan tietoturvaohjeiden noudattamista tai järjestelmien väärinkäyttöä paremmin kuin kovia asioita, kuten rangaistuksia tai aineellisia palkkioita, edustavien muuttujien (Sommestadt, Hallberg, Lundholm, & Bengtsson, 2012). Tämän vuoksi pehmeitä asioita edustaviin muuttujiin vaikuttaminen voidaan nähdä tehokkaampana tapana ylläpitää tietoturvaa ja kyberturvallisuutta kuin rangaistusten ja aineellisten palkkioiden korostaminen. Hedström, Kolkowska, Karlsson ja Allen (2011) esittävätkin arvoihin perustuvan mallin olevan tehokkaampi ja parempi tapa sitouttaa työntekijöitä edistämään organisaation turvallisuuskulttuuria. Turvallisuuskulttuurilla on havaittu olevan yhteys siihen, miten loppukäyttäjät noudattavat turvallisuusohjeita sekä tietyssä määritetyssä tehtävässä että yleisesti (Greene & D'Arcy, 2010), mikä tukee näkemystä turvallisuuskulttuurin vaikutuksesta sekä tarkemmin ennalta määritettyihin että määrittelemättömiin turvallisuuteen liittyviin valintatilanteisiin.

Turvallisuuskulttuurin luomisen ja ylläpitämisen tulisi Kearneyn (2010) tutkimuksen mukaan sisältää toimia, jotka lisäävät työntekijöiden ymmärrystä tietoturvallisuutta uhkaavista tekijöistä sekä organisaation tiedon ja tietojärjestelmien suojaamisen vastuun jakamista. Loppukäyttäjä voidaan näin sitouttaa loppukäyttäjiä tietoturvalliseen toimintaan, ja tehdä turvallisuudesta yksi organisaation keskeisistä arvoista. Mikäli erillinen turvallisuushenkilöstö vastaa turvallisuuteen liittyvistä toimenpiteistä ja loppukäyttäjät saavat vahvaa tukea kaikkiin tietotekniikkaan ja -järjestelmiin liittyviin ongelmiin, heille voi muodostua valheellinen kuva turvallisuuskontrollien runsaudesta. Tällöin loppukäyttäjät eivät välttämättä näe heidän omaa tietoturvaohjeiden noudattamistaan yhtä tärkeänä kuin tilanteessa, jossa koko organisaatio on sitoutettu turvallisuuden ylläpitämiseen. (Greene & D'Arcy, 2010).

Myös se, miten tietoturvallisuuskontrollit näkyvät käyttäjille ja miten käyttäjiä tiedotetaan kontrollisen olemassaolosta, vaikuttaa tietoturvallisuuden kannalta positiiviseen käytökseen (Choi ym., 2013). Ollakseen tehokkaista tulee tietoturvaohjeiden olla työntekijöiden saatavilla ja ymmärrettäviä. Eri henkilöiden ja käyttäjäryhmien roolien sekä vastuiden tulee myös olla selkeästi ilmaistu. (Metalidou ym., 2014).

Organisaatiokulttuurin ominaispiirteiden tunnistamisella on kiinteä yhteys toiminnan tehokkuuteen. Käytännössä tämä näkyy esimerkiksi siinä, miten koulutusohjelmien räätälöinti organisaation ominaisuuksien ja organisaatiokulttuurin perusteella lisää koulutusten tehokkuutta (Wilson & Hash, 2003).

Teoreettisen tarkastelu perusteella voidaan sanoa, että organisaation arvot, toiminnan perusoletukset ja tuntemukset vaikuttavat organisaation toiminta-, turvallisuus-, tietoturva- ja kyberturvallisuuskulttuuriin. Luodakseen turvallisuutta tukevan organisaatiokulttuurin tulisi organisaation tunnistaa millaisia arvoja se näkyvästi ja näkymättömästi ylläpitää sekä räätälöidä ohjeet, toimintamallit ja koulutukset vastaamaan niitä.

3.4 Organisaatioiden ala- ja mikrokulttuurit

Vaikka organisaatiokulttuuri voi vaikuttaa homogeeniseltä, lähes poikkeuksetta se koostuu ja siihen vaikuttaa useampi ammatillinen, paikallinen ja yksittäisen ryhmän tai osaston alakulttuuri. Martin Parker (2000) näkee organisaatioiden olevan samanaikaisesti yhteisöllisiä ja hajautuneita. Organisaatiot toimivat yhteisen päämäärän eteen, mutta organisaatio koostuu esimerkiksi rakenteiden, sukupuolen tai samanhenkisyyden perusteella muodostuneista useista erilaisista kulttuureista. Paikallisten kulttuurien muodostumiseen voivat vaikuttaa vuorovaikutuksen määrä, työskentelyolosuhteet ja ryhmään kuuluvat vahvat persoonat (Parker, 2000). Parker (2000) tunnistaa kolme eri syytä organisaatioiden hajautuneisuudelle:

1. Spatiaalinen ja toiminnallinen jako johtuu maantieteellisestä tai esimerkiksi osastojen välisestä jaosta liittyen ihmisten väliseen vuorovaikutukseen ja toimintojen vaikutukseen organisaatiokulttuuria kohtaan.
2. Sukupolvista johtuva jako, jonka perusteella eroavaisuuksia ihmisten välille syntyy heidän kuulumisestaan tietyn sukupolven edustajiin.
3. Ammatillisista syistä johtuva jako, jossa yhteneväisyydet ja eroavaisuudet selittyvät kuulumisella tietyn koulutuksen tai ammattikunnan edustajin.

Yksilön kuuluminen ryhmään ei riipu niinkään hänen identiteetistään, vaan siitä mihin hän itse identifioituu. Yksilön identifioitumisessa on kyse enemmän prosessista kuin pysyvästä asiantilasta. (Parker, 2000). Ammatilliset alakulttuurit organisaatioiden ja yhteiskuntien sisällä rakentuvat yhteisistä koulutukseen, työtehtäviin tai yhteisöihin liittyvistä kokemuksista. Sellaisilla ammateilla, joilla on pitkä historia, ainutlaatuiset koulutusvaatimukset tai korkea ammatillinen status, voi olla suurempia vaikutuksia ammattia edustavien työntekijöiden arvoihin ja uskomuksiin kuin organisaatiokulttuurilla. (Trice & Beyer, 1993; Guzman ym., 2008).

Tietoteknisen alan henkilöstöllä on tunnistettu olevan erillisiä, tunnistettavia ammatillisia alakulttuureja. Tämän takia tietotekniikka-alalla ammatilliset alakulttuurit voivat jopa luoda konflikteja tietotekniikka-ammattilaisten ja loppukäyttäjien välille. (Guzman ym., 2008). Tähän voi osaltaan vaikuttaa tietotekniikka-alan henkilöstön ja loppukäyttäjien välillä vallitseva ero ymmärryksessä ja tavoissa käyttää tietotekniikkaa.

Samankaltainen koulutustausta ei kuitenkaan aina takaa yhteisymmärrystä, vaan organisaation pienempiin kokonaisuuksiin syntyy paikallisia kulttuureja. Niiden merkitystä kuvaa Kolkowskan (2011) havainto siitä, että saman koulutuksen tai ammatin edustajien välillä voi olla merkittäviäkin kulttuurieroja, jos he työskentelevät eri osastoilla tai tehtävissä.

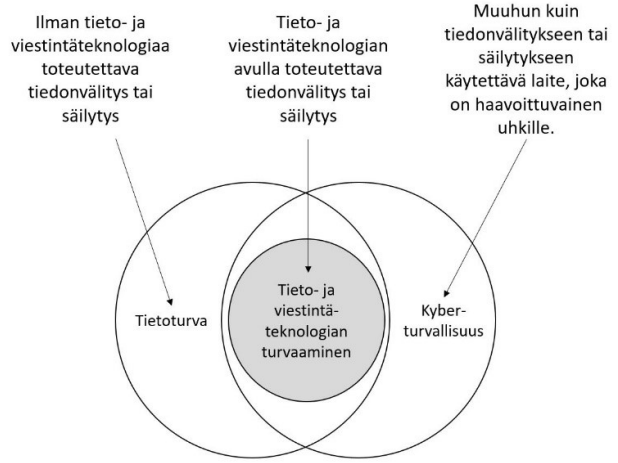
3.5 Kyberturvallisuuskulttuuri osana organisaatiokulttuuria

Organisaatiokulttuurin määritelmää mukaillen voidaan sanoa, että kyberturvallisuuskulttuuri on kokoelma niitä arvoja ja tapoja, joilla kyberturvallisuutta toteutetaan ja ylläpidetään organisaatiossa. Kyberturvallisuuskulttuuri limittyy käsitteenä tietoturvakulttuurin (*eng.* information security culture) käsitteen kanssa, minkä vuoksi tietoturvakulttuurin mallia voidaan hyödyntää hahmoteltaessa kyberturvallisuuskulttuurin rakennetta (Da Veiga & Eloff, 2010; Von Solms & Van Niekerk, 2013). Tietoturvakulttuurin tutkimuksessa Edgar Scheinin (1999) organisaatiokulttuurin malli on todettu soveltuvaksi, kun siihen lisätään neljänneksi kerrokseksi tieto (Van Niekerk & Von Solms, 2006; 2010). Edgar Schein (1999) argumentoi, että mikäli halutaan ymmärtää artefaktien ja vaalittujen arvojen todellista merkitystä organisaatiolle, täytyy kyetä tutkimaan organisaation tiedostamattomia ja jaettuja perusoletuksia. Kuvassa 6 on esitetty Scheinin (1999) organisaatiokulttuurin sekä Van Niekerkin ja Von Solmsin (2013) tietoturvakulttuurin mallien vertailu.

Kuva 6. Organisaatiokulttuurin (Schein, 1999) ja tietoturvakulttuurin (Van Niekerk & Von Solms, 2006) tasot ja niiden esiintyminen käytännössä

Keskeinen tietoturva- ja kyberturvallisuuskulttuureita yhdistävä tekijä on tieto- ja viestintäteknologian (ICT, *eng.* information and communication technology) käyttö. Kyberturvallisuus limittyy tietoturvan niiden osien kanssa, joilla tieto- ja viestintäteknologiaa hyödyntäen välitetään, hyödynnetään tai säilytetään tietoa (kuva 7). Von Solms & Van Niekerk, 2013). Kyberturvallisuuskulttuuri kattaa edellä mainitun lisäksi myös laitteet ja verkkoinfrastruktuurin sekä protokollat, joita tarvitaan tieto- ja viestintäteknologian käyttöön, mutta joiden avulla ei suoranaisesti välitetä tai säilytetä tietoa. Kyberturvallisuuskulttuurin käsitettä määritettäessä täytyy tietoturvakulttuurin malliin lisätä käyttäjä- ja asiakastiedon suojaaminen ja sosiaalisen median käyttö (Da Veiga, 2016).

Keskeisenä tavoitteena kyberturvallisuuden integroimisessa organisaatiokulttuuriin ja sitä kautta organisaation jokapäiväiseen toimintaan on asenteellinen muutos, jossa yksilö ja yksilön toiminta nähdään turvallisuusriskin sijaan turvallisuutta edistävänä tekijänä (Von Solms, 2000). Tällöin yksilön osaaminen, toiminta, ymmärrys ja asenne ovat keskeisiä organisaation kyberturvallisuuskulttuuria edistäviä tekijöitä. Tietoturvaan liittyvä koulutus edistää yksilön positiivista suhtautumista tietoturvakulttuurin (Da Veiga & Martins, 2015).



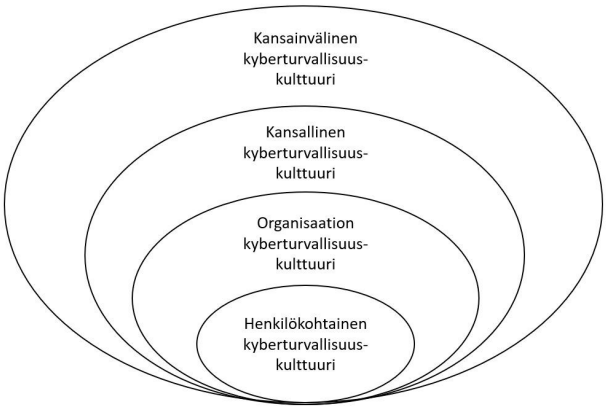
Kuva 7. Tietoturvan, tieto- ja viestintäteknologian turvaamisen ja kyberturvallisuuden suhde (Von Solms & Van Niekerk, 2013)

Tietoturvakulttuurin tutkimus on keskittynyt organisaation toimintaympäristöön tai vastaaviin samankokoisiin eristettyihin ympäristöihin, jotka ovat hyvin hallittavissa ja käyttäjien toiminta on laajalti ennalta-arvattavaa. Kyberturvallisuuskulttuurin kontekstissa erilaisia käyttäjäprofiileja ja käyttötapauksia on huomattavasti enemmän, etenkin kansallisella ja globaalilla tasolla. Käyttäjäprofiileissa on runsaammin muuttujia, esimerkiksi ikä ja osaaminen sekä laitteiden ja ohjelmistojen käyttökohteet ja -tarve. Lisäksi käyttäjien toiminta on vähemmän säänneltynä ja säädeltynä ennalta-arvaamattomampaa. Tietoturvakulttuurin tutkimus ei myöskään ota huomioon esimerkiksi ympäröiviä yhteiskuntia eli yksilön useita ja vaihtelevia rooleja sekä toimintaa erilaisissa toimintaympäristöissä. (HLEG, 2008; Reid & Van Niekerk, 2014). Kyberturvallisuuskulttuurin rakenteet ja painotukset vaihtelevat organisaatiotasolla kontekstin mukaan.

Von Solmsin ja Van Niekerkin (2013) tavoin myös Adele Da Veigan (2016) mukaan kyberturvallisuuskulttuuri on tietoturva- tai turvallisuuskulttuurien määritelmiä huomattavasti laajempi kokonaisuus. Von Solmsin ja Van Niekerkin (2013) mukaan kyberturvallisuuskulttuurissa täytyy huomioida kokonaisuus yksittäisestä henkilöstä ja yksittäisen talouden laitteesta kansalliseen kriittiseen infrastruktuuriin, jonka kautta voi kohdistua välillisiä vaikutuksia kokonaisuuden eri osiin. Kokonaisuuden hallitsemiseksi kyberturvallisuuskulttuuri täytyy jakaa eri tasoihin ja tunnistaa eri tasoihin kuuluvat sekä vaikuttavat asiat. Yksittäisen organisaation toimintaympäristöön vaikuttaa käyttäjien lisäksi kansallisen ja

kansainvälisen konteksti, koska organisaatio hyödyntää internetissä toimivia eri toimijoiden ylläpitämiä palveluja, globaaleja tietoliikenneyhteyksiä ja lukuisia eri tason teknologisia ratkaisuja (Da Veiga, 2016). Da Veiga (2016) näkee eri tasojen merkitykset seuraavasti (kuva 8):

- Kansainvälinen taso sisältää globaalisti kaikki internetiin kytketyt ja kytkeytyneet laitteet sekä ihmiset.
- Kansallisella tasolla kriittisen infrastruktuurin turvallisuus ja resilienssi vaikuttavat kybertoimintaympäristöön.
- Organisaatiotasolla organisaation kannalta kriittistä infrastruktuuria ja tietoa täytyy hallita ja suojella niin, että tietoverkkojen ja -järjestelmien kautta ilmenevät riskit kyetään minimoimaan ja hyödyt maksimoimaan.
- Yksilötasolla tietoverkkoja ja -järjestelmiä hyödyntävän henkilön kaikkia internetiin kytkettyjä välineitä ja informaatiota, niin työ- kuin henkilökohtaista, sekä siellä jaettua tietoa täytyy suojella.



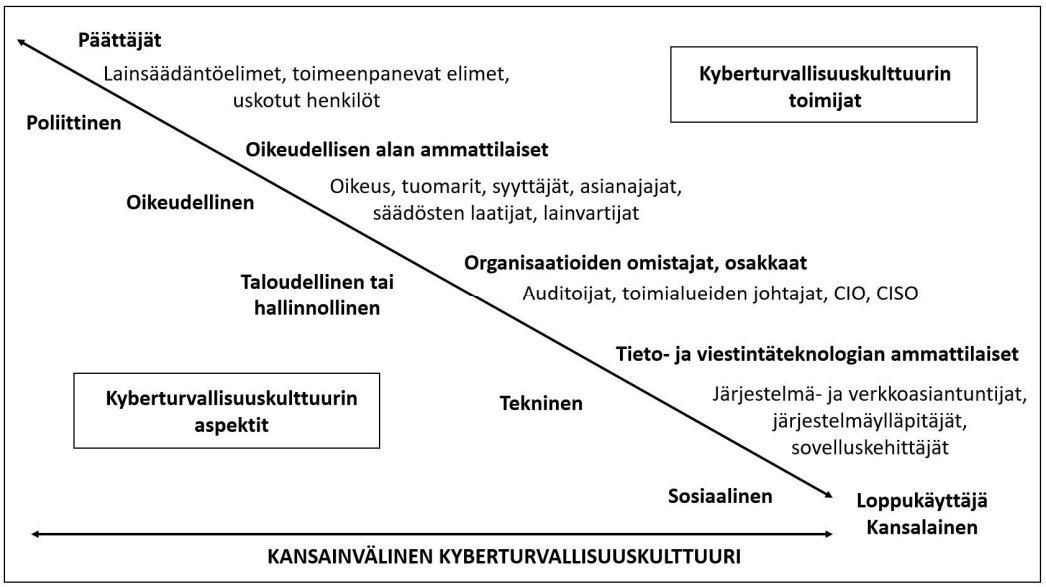
Kuva 8. Kyberturvallisuuskulttuurin tasot (Da Veiga, 2016)

Adele da Veiga (2016) määrittelee kyberturvallisuuskulttuurin tarkoituksellisiksi ja tahattomiksi toimenpiteiksi, joissa kyberulottuvuutta hyödynnetään kansainvälisestä, kansallisesta, organisaation tai yksilön näkökulmasta asenteiden, olettamusten, uskomusten, arvojen ja käyttäjän tietojen kontekstissa. Käytännössä kyberturvallisuuskulttuuri esiintyy kyberulottuvuuden hyödyntämisen toimintatapoina. Kyberturvallisuuskulttuuri voi joko lisätä tai vähentää turvallisuutta, yksityisyyttä tai kansalaisten, organisaatioiden tai valtiovallan oikeuksia. Kyberturvallisuuskulttuuri ilmenee tietyssä ihmisjoukossa, ryhmässä tai organisaatiossa. Kyberturvallisuuskulttuurin tavoite ylläpitää eettisiä, turvallisuuden ja yksityisyyden periaatteita. (Da Veiga, 2016).

Tietoturvakulttuuri sisältää organisaation ainoastaan tiedon turvaamiseen liittyvät asiat (Reid & Van Niekerk, 2014; Von Solms & Van Niekerk, 2013). Kyberturvallisuuskulttuurin määritelmä on puolestaan sekoitus teknologiaa eli laitteita, ohjelmistoja ja telekommunikaatiojärjestelmiä sekä psykologiaa eli organisaatiokulttuurin ja ihmisen käyttäytymisen ymmärtämistä (Da Veiga, 2016).

Kansainvälisen telekommunikaatiounionin (ITU) asiantuntijatyöryhmän (HLEG) raportissa (2008) on tunnistettu kyberturvallisuuskulttuurin jatkumo

yksittäisestä henkilöstä ja paikallisesta kulttuurista kansainväliselle tasolle (kuva 9). Kansainvälinen kyberturvallisuuskulttuuri koostuu sosiaalisesta, teknisestä, taloudellisesta, lainopillisesta ja poliittisesta ulottuvuudesta. Eri ulottuvuuksien huomioimiseksi tulee erilaista osaamista edustavien asiantuntijoiden osallistua kyberturvallisuuskulttuurin kehittämiseen sekä kyetä yhteistoimintaan eri tasoilla. Yksilön osalta keskeistä on tietous loppukäyttäjiin kohdistuvista uhkista, ymmärrys tietoturvallisesta tieto- ja viestintäteknologian käytöstä sekä valppaus uhkien havaitsemiseksi. (HLEG, 2008). Yksilön tietouden ja ymmärryksen lisääminen palvelee tällöin kyberturvallisuuskulttuurin muita tasoja ja ulottuvuuksia.



Kuva 9. Kansainvälisen kyberturvallisuuskulttuurin aspektit ja toimijat (HLEG, 2008)

Tämän tutkimuksen näkökulmasta voidaan tiivistää, että kyberturvallisuuskulttuuri on useita eri tasoja ja ulottuvuuksia sisältävä sosio-tekninen kokonaisuus. Sen keskiössä on käyttäjät, tietojen käsittely tieto- ja viestintätekniikan avulla sekä siihen tarvittavat laitteet, välineet ja infrastruktuuri. Vaikka kyberturvallisuuskulttuuri kattaa kaikki tasot yksilöstä kansainväliseen ja sisältää myös kriittisen infrastruktuurin, tässä tutkimuksessa kyberturvallisuuskulttuurin tarkastelu rajataan koskemaan yksilö- ja organisaatiotasoja.

3.6 Ihmisen ominaisuuksien, käyttäytymismallien ja osaamisen vaikutus suhtautumisessa tietoturvaan ja kyberturvallisuuteen

Ihmisen voidaan sanoa olevan kulttuurinsa tuotos, koska yksilön kasvuympäristöön ja kasvatukseen vaikuttavat kansallinen, paikallinen ja muut kulttuurit.

Lapsuudesta lähtien yksilö oppii malleja yleisesti hyväksytystä käytöksestä ja oppii säätelemään toimintaansa sekä tekemään valintoja erilaisissa tilanteissa. Kun yksilö muodostaa sosiaalista identiteettiään, käsitystä itsestään ja ajattelunsa vinoumia, hän omaksuu asioita jatkuvasta sosiaalisesta vuorovaikutuksesta. Kansallinen kulttuuri, olosuhteet ja alakulttuurit vaikuttavat suorasti tai epäsuorasti minäkuvan muodostumiseen (Markus & Kitayama, 1991). Kuitenkin yksilöiden välillä ilmenee henkilökohtaisia eroja siinä, minkä verran he samaistuvat ryhmään, omaksuvat ryhmän arvoja ja toteuttavat ryhmän tapoja (Berry, 2008). Tämän vuoksi ei ole mahdollista tehdä täysin pitäviä yleistyksiä kansallisen, alueellisen tai ammatillisen alakulttuurin vaikutuksesta yksilöiden asenteisiin, tapoihin ja toimintamalleihin. Kulttuurillisten piirteiden perusteella tehtyjen yleistysten paikkaansa pitävyyteen vaikuttaa myös kansallisen homogeenisyyden taso (Nishimura, Nevgi & Tella, 2008).

Eri sukupuolten välillä on havaittu eroja suhtautumisessa turvallisuuteen sekä turvallisuutta edistävässä käyttäytymisessä. Miehet kokevat itsensä naisia varmemmiksi teknologian käytössä ja yksityisyytensä suhteen internetissä. (Halevi, Lewis, Memon, Kumaraguru, Arora, Dagar & Aloul, 2016). Sukupuolen vaikutus henkilön tietoturvaa koskeviin arvoihin ja asenteisiin riippuu kansallisesta kulttuurista ja niissä esiintyvistä eroista koskien sukupuolirooleja. Koska ympäröivä kulttuuri vaikuttaa minäkuvan kehittymiseen, on liberaalimmissa maissa sukupuolen vaikutus muuttumassa hitaasti ahtaiden sukupuoliroolien, asenteiden, odotusten, normien ja sukupuolisidonnaisten käyttäytymismallien häviämisen tai vaikutusten vähenemisen myötä. (Cross & Madson, 1997; Markus & Kitayama, 1991; Hofstede, 1999). Suomessa ja muissa länsimaissa sukupuolten väliset erot tietotekniikan ja kyberturvallisuuden osaamisessa ovat kavenneet naisten lisääntyvän teknisten alojen opiskelun kautta.

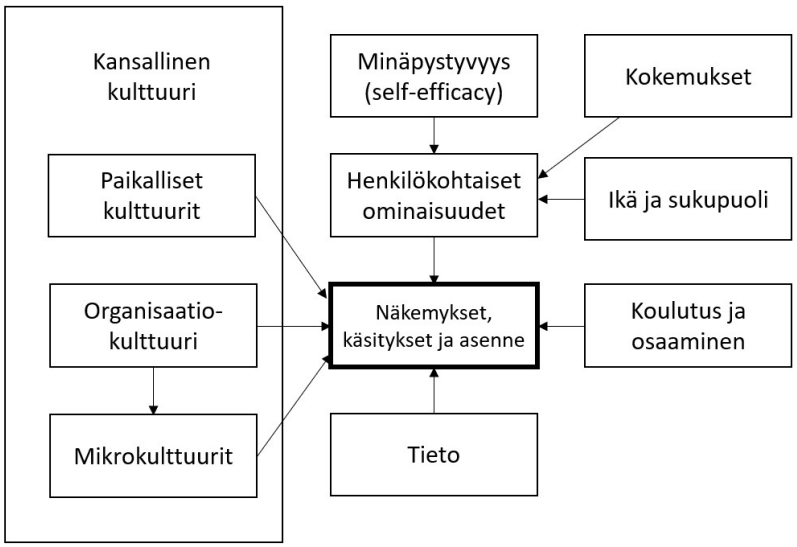
Yksilön iän on todettu tietoturvatutkimuksissa vaikuttavan tietotekniikan käyttöön liittyvien taitojen oppimisnopeuteen. Nuorten on havaittu tekevän vähemmän virheitä ja oppivan tietotekniikan käyttöön liittyviä taitoja nopeammin. (Echt ym., 1998). Tämä saattaa johtua tottuneisuudesta tieto- ja viestintätekniikan käyttöön. Toisaalta nuoren iän on myös todettu lisäävän tietotekniikan väärinkäyttöä (D'Arcy ym., 2009; Hovav & D'Arcy 2012).

Yksilön osaaminen ja käsitys omasta osaamisestaan ennustaa hänen käytöstään tietotekniikan ja myös kyberturvallisuuden suhteen, koska käsitys henkilökohtaisesta osaamisesta vaikuttaa stressin ja ahdistuksen tunteisiin sekä suorituskykyyn ja kykyyn selvitä erilaisista tilanteista (Bandura, 1982; 1986; 1997). Käsitys omasta heikosta tietoteknisestä osaamisesta vähentää proaktiivista kyberturvallisuutta tukevaa käytöstä, koska yksilö voi kokea kyberturvallisuuteen liittyvät tapahtumat ahdistaviksi ja haluta välttää ahdistusta lisääviä tilanteita (Conetta, 2019). Kyberturvallisuuden ja tietotekniikan käytön osaamisen taso myös vaikuttaa käyttäjien käsityksiin tietoturvasta (Torkzadeh & Lee, 2003; Choi ym., 2013), vaikkakin kyky hyödyntää tieto- ja viestintätekniikkaa ei välttämättä lisää kyberturvallisuuden osaamista ja voi itse asiassa johtaa väärinkäytön lisääntymiseen (Cronan ym., 2006). Taidot ja ymmärrys eivät myöskään välttämättä riipu koulutuksesta. Vuorovaikutustaidot ja hyväksyvä luonne vaikuttavat henkilön

kykyyn saada kyberuhkia koskevaa tietoa sosiaalisten verkostojen kautta. Hyväksyvän luonteen havaittu yhdistyvän luottamuksen, suorasukaisuuden ja ohjeiden noudattamisen kanssa. (Costa & MacCrae, 1992; Conetta, 2019).

Henkilökohtaisten kokemusten vaikutus kyberturvallisuuteen liittyvään toimintaan riippuu niiden positiivisesta tai negatiivisesta luonteesta. Tutkiessaan kohdehenkilöiden vastauksia koskien negatiivista asennetta, tietämättömyyttä, laiminlyöntejä, ilkivallan tekoa ja tietoturvakontrollien vastustusta suhteessa havaittuihin tietoturvariskeihin Safa, von Solms ja Furnell (2016) havaitsivat niiden esiintymisen vastauksissa olevan vahvasti sidoksissa tietoturvariskien lisääntymiseen. Myös henkilökohtaisten ominaisuuksien, esimerkiksi matalan riskinottohalukkuuden ja tunne-elämän tasaisuuden, on huomattu vaikuttavan yksilöiden tietoturvaa koskevaan ymmärrykseen, asenteeseen ja sitä kautta käytökseen niin että näiden ominaisuuksien vaikutus on jopa suurempi kuin iän tai sukupuolen (McCormac, Zwaans, Parsons, Calic, Butavicius & Pattinson, 2017).

Tietoisuus tietoturvaan ja kyberturvallisuuteen liittyvistä uhkista voi olla ympäröivän kulttuurin vaikutuksen, koulutuksen tai työnantajan toiminnan tulosta. Arvioidakseen organisaatioon kohdistuvia kyberuhkia, täytyy yksilöiden ymmärtää organisaation tai yksilön käyttämien tietojärjestelmien ja käsittelemän tiedon tyypit ja arvo sekä millainen riski kohdistuu erilaisiin järjestelmiin ja tietoon (Metalidou ym., 2014). Kuvaan 10 on koostettu yksilöön vaikuttavia tekijöitä.



Kuva 10. Yksilön näkemyksiin, käsityksiin ja toimintamalleihin vaikuttavia tekijöitä

Tutkiessaan tietoturvakulttuuria Greene ja D'Arcy (2010) havaitsivat, että korkea tyytyväisyys työhön vaikutti positiivisesti turvallisuusmääräysten noudattamiseen. Havainto linkittyy sosiaalisen transition teoriaan, jonka mukaan motivoituneet ja tyytyväiset työntekijät noudattavat organisaation asettamia sääntöjä ja ohjeita paremmin. Hetkellinen motivaatio tietoturvaohjeiden noudattamisessa on altis nopeille muutoksille, mutta hetkellisen tason on havaittu vaihtelevan

ainoastaan vähän työntekijän tunnistetusta perustasosta. (Greene & D'Arcy, 2010). D'Arcy ja Lowry (2019) havaitsivat työntekijöiden mielentilan vaikuttavan tietoturvaohjeiden noudattamiseen, minkä perusteella tutkijat korostivat positiivisen työilmapiirin vaalimista ja hyvien työolojen tarjoamista yhtenä ratkaisuna tietoturvaohjeiden noudattamisen kehittämiselle. He myös suosittelivat moraalisia vastuita koskevan osuuden lisäämistä tietoturvakoulutukseen, yksittäisen työntekijän tietoturvaohjeiden noudattamisen vaikutusta sekä onnistuneen tietoturvakäyttäytymisen tunnustamista koko organisaatiossa (D'Arcy ja Lowry, 2019). Edellä mainitun toiminnan tavoitteena on ryhmän toiminnan eli organisaatiokulttuurin osien ohjattu muuttaminen (Schein & Schneier, 2017), jossa tavoitteena on organisaation yleisen suhtautumisen muuttaminen tietoturvaohjeiden noudattamiseen ja tietoturvan kehittämiseen.

Ihmiselle ominaisen käyttäytymisen tunteminen edes auttaa käyttäjien kyberturvallisuutta koskevan asennoitumisen ja toiminnan ennustamista. Pfleeger ja Caputo (2012) tutkivat kognitiivisen kuormituksen ja vinoumien (bias) merkitystä ihmisen kyberturvallisuutta koskevaan käytökseen. Kognitiivisen kuormituksen havaittiin vaikuttavan muistiin ja tarkkaavaisuuden vähenemiseen. Useista eri lähteistä saadun tiedon perusteella havaitun riskin luonteen ja kokoluokan hahmottamisessa havaittiin ongelmia. Yksilöitä voidaan kannustaa kyberturvallisuutta tukevaan käytökseen ottamalla huomioon toimintamallien tai järjestelmien suunnittelussa muistin, kognition ja vinoumien luonnollinen vaikutus. Esimerkiksi organisaatioon kohdistuvan kyberuhkan torjunta voidaan kuvata sen kautta mitä sillä saavutetaan, eikä sen kautta mitä sillä voidaan menettää. (Pfleeger & Caputo, 2012).

Tutkimuksen kannalta olennaisimmiksi yksilön ominaisuuksiksi tunnistettiin aiemman tutkimuksen perusteella ymmärrys ja tieto kyberturvallisuuden kokonaisuudesta yleisesti sekä organisaation kontekstissa, asenne kyberturvallisuutta kohtaan, tyytyväisyys työhön, henkilökohtainen osaaminen ja käsitys omasta osaamisesta. Tämän lisäksi kyberturvallisuutta parantavia toimintamalleja suunniteltaessa täytyy ottaa huomioon ihmisen käyttäytymiselle ominaiset tekijät ja vinoumat. Kaikki edellä mainitut tekijät ovat sellaisia, johon organisaatio pystyy toiminnallaan vaikuttamaan.

3.7 Suomalaiselle kulttuurille ominaisia piirteitä sekä niiden vaikutus tietoturvaan ja kyberturvallisuuteen

Koska kansallisen kulttuurin on tunnistettu vaikuttavan yksilö- ja organisaatiotasojen kyberturvallisuuskulttuuriin, on kriittistä tunnistaa tutkimuskontekstin kansalliset erityispiirteet. Suomen kansallinen kulttuuri kuuluu pohjoismaisiin kulttuureihin, jotka voidaan yleistää kuuluvan matalan kontekstin individualistisiin kulttuureihin. Matalan kontekstin kulttuurit nähdään loogisina, suoraviivaisina sekä yksilö- ja toimintakeskeisinä. Kontekstilla ei ole niin suurta merkitystä, vaan informaatio välitetään puheen sisällössä sanattoman

kommunikaation keinojen sijaan. Tällainen kansallinen kulttuuri myös muuttuu nopeammin, eikä historialla tai asemalla ole niin suurta merkitystä kuin enemmän perinteisiin nojaavissa kulttuureissa. Yksilöllisyyttä arvostetaan enemmän kuin kollektiivisuuden ja ryhmän harmoniaa, mikä edistää innovointia ja uusien ideoiden esittämistä. (Hall, 1976; Hall & Hall, 1990; Hall, 2000).

Geert Hofstede (1999) on tutkimuksensa kautta määritellyt Suomen kansallisen kulttuurin ominaisuudet kuuden dimension kautta (taulukko 2):

Ulottuvuus:	Piste-määrä:	Merkitys:
Individualismi (Individualism)	63 / 100	Suomalainen kulttuuri katsotaan individualistiseksi. Yksilön odotetaan huolehtivan itsestään ja läheisistään. Työsuhde perustuu kahdensuuntaiseen hyötyyn. Palkkaamisen ja ylentämisen odotetaan perustuvan ansioihin. Johtaminen keskittyy enemmän yksilöihin kuin ryhmään.
Valtaetäisyys (Power distance)	33 / 100	Hierarkian merkitys on pieni. Kulttuuri arvostaa tasa-arvoa vallanjaossa. Johtajuus on luoteeltaan valmentavaa ja mahdollistavaa. Johtajat ovat saatavilla ja tukevat työntekijöitä. Päätösvaltaa hajautetaan ja itsenäisyyttä arvostetaan. Kommunikaatio on suoraa ja osallistavaa.
Maskuliinisuus (masculinity)	26 / 100	Suomalainen kulttuuri katsotaan feminiiniseksi, jossa vaalittavia arvoja ovat toisista välittäminen, nöyryys ja elämänlaatu. Päätöksissä pyritään löytämään konsensus, tasa-arvoa, solidaarisuutta ja laatua arvostetaan työelämässä. Vapaa-aika ja joustavuus nähdään kannustimina. Statusta ei näytetä julkisesti. Sukupuoliroolit eivät ole täysin erillään ja sekoittuvat.
Epävarmuuden välttäminen (Uncertainty avoidance)	59 / 100	Suomalaisessa kulttuurissa pyritään välttämään epävarmuutta ja arvostetaan tietoa sekä selkeyttä. Säännöille on henkinen tarve, aika on arvokasta ja ihmisillä on sisäinen halu olla kiireisiä ja työskennellä kovaa. Tarkkuutta ja täsmällisyyttä arvostetaan. Muutosvastarintaa esiintyy ja turvallisuus on tärkeä elementti yksilön motivaation suhteen.

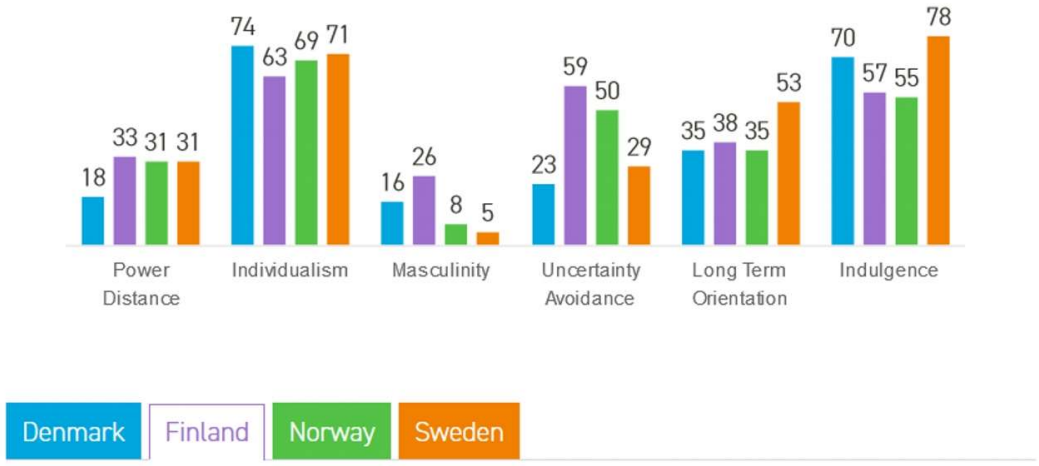
Pitkän aikavälin orientaatio (Long-term orientation)	38 / 100	Suomalainen kulttuuri on normatiivinen, jonka vuoksi ihmiset arvostavat absoluuttisia totuuksia. Ihmiset arvostavat perinteitä. Tulosten nopea saavuttaminen on keskiössä.
Suopeus (Indulgence)	57 / 100	Suomalainen kulttuuri on suopea. Ihmisillä on positiivinen asenne ja heillä on taipumus optimismiin. He arvostavat vapaa-aikaa sekä käyttäytyvät ja käyttävät rahaa kuten haluavat.

Taulukko 2. Suomen kansallisen kulttuurin määritelmä Geert Hofsteden kuuden kulttuurillisen ulottuvuuden mukaan (https://www.hofstede-insights.com/country/finland/).

Suomalaiset kokevat henkistä erillisyyttä muista, myös skandinaavisista kulttuureista muun muassa maantieteellisistä, historiallisista ja kielellisistä syistä. Hofsteden (1999) tutkimuksen perusteella Suomen kansallinen kulttuuri eroaa muiden pohjoismaiden kulttuureista merkittävimmin maskuliinisuuden ja epävarmuuden välttämisen osalta (kuva 11). Suomi on myös hieman hierarkkisempi kuin muut pohjoismaat.

Suomen kulttuurillisiin eroavaisuuksiin mahdollisesti vaikuttavat Venäjän vallan aika, itsenäistymisen vaiheet ja asema toisessa maailmansodassa. Kieli ja kommunikaatio on yksi merkittävä kulttuureja yhdistävä tekijä, mikä voi osaltaan selittää suomalaisten erillisyyden tunnetta skandinaavisista kulttuureista (Lewis, 2005; Nishimura, Nevgi & Tella, 2008). Yhtenevyyttä puolestaan selittävät osittain maantiede, demokratia, luterilaisuus, yhteiskunnallinen vakaus, taloudellinen tilanne, muut Ruotsin vallan aikana omaksutut kulttuurilliset vaikutteet ja tiiviit yhteydet muihin pohjoismaihin. Pohjoismaisten kulttuurien samankaltaisuutta selittävät myös suomalaisten muuttoliikkeet Ruotsiin ja sitä kautta sukulaisuussuhteet sekä Suomessa asuva suomenruotsalainen vähemmistö. (Lewis, 2005).

Kansallisen ylpeyden tason on havaittu olevan suomalaisessa kansallisessa kulttuurissa lähtökohtaisesti korkea (Lewis, 2005). Myös kansallisen kulttuurin homogeenisyyden taso on Suomessa keskimäärin korkea, mikä esimerkiksi parantaa Suomen kansallisen kulttuurin kontekstissa toteutettujen tutkimustulosten yleistettävyyttä (Nishimura, Nevgi & Tella, 2008). Suomalaiselle kulttuurille ominainen lyhyt ja suora ilmaisutapa sekä asiakeskeisyys vähentävät väärinymmärryksen mahdollisuutta haastattelututkimuksissa, koska ilmaisujen merkitys eri konteksteissa vaihtelee vähemmän.



Kuva 11. Neljän pohjoismaan kansallisten kulttuurien vertailu Hofsteden kuuden dimension mukaan. (https://www.hofstede-insights.com/country-comparison/denmark,finland,norway,sweden/)

Suomalaiset arvostavat totuutta huolimatta sen epämieluisuudesta, mikä voi ilmetä muiden kulttuurien näkökulmasta suorapuheisuutena (Lewis, 2005; Nishimura, Nevgi & Tella 2008). Täsmällisyyttä arvostetaan ja odotetaan noudatettavan. Suomalainen kulttuuri on lähtökohtaisesti suvaitsevainen: yksilöllisyyttä arvostetaan, mutta yhteisten sääntöjen puitteissa. Luotettavuus on arvo, jolla mitataan henkilön nauttimaa arvostusta. Suomalainen kulttuuri on työkeskeinen, minkä vuoksi työn tekeminen ja viimeistely voidaan katsoa arvoksi. Koulutusta ja osaamista arvostetaan. Suomessa yksilö määrittelee itsensä usein enemmän sen perusteella mitä hän tekee kuin mitä hän on tai sanoo. Suomalaiset mielletään käytännönläheisiksi sekä faktoja ja läpinäkyvyyttä arvostaviksi. Suomalaisessa kulttuurissa uskotaan lyhyeen ja yksinkertaiseen kommunikaatioon, jossa yksi henkilö puhuu kerrallaan ja vastaus on reaktio edelliselle puhujalle. Suomen kansallista kulttuuria voi myös kuvailla uhkalähtöiseksi tai pessimistiseksi. (Lewis, 2005; Lewis, 2006; Minkov, 2011).

Suomalaisten on tunnistettu arvostavan vapaa-aikaa ja itsensä toteuttamista, mikä on tutkimuksissa yhdistetty suopeuden kulttuurilliseen ulottuvuuteen. Korkeaan suopeuteen on yhdistetty myös kevyemmät rangaistukset yhteisten sääntöjen rikkomisesta, korkea tyytyväisyys elämään, tunne yksilön mahdollisuudesta hallita elämäänsä ja sananvapaus. (Minkov, 2011; Lewis, 2005). Suopeuteen liittyvä universalismi on Suomessa korkealla tasolla, mikä näkyy kaikkia ihmisiä kohtaan toteutettuna tasavertaisen suhtautumisen tavoitteluna. Tasavertaisuus on tärkeää, eikä kukaan ole lähtökohtaisesti etuoikeutetussa asemassa suhteessa muihin esimerkiksi ryhmän jäsenyyden perusteella vaan kohtelu perustuu ansioihin tai osaamiseen. (Minkov, 2011).

Johtamisen näkökulmasta suomalaisessa arvostetaan maalaisjärkeä ja tehokkuutta, mutta työntekijöiden ja eri näkökulmien kuuntelemista sekä yhteisymmärryksen saavuttamista. Suomalaisessa kulttuurissa päätöksentekovaltaa on annettu alempien hierarkiatasojen johtajille. Johtajat toimivat osana tiimejä menettämättä auktoriteettiaan. Suomalaista johtamiskulttuuria on luonnehdittu

autoritäärisemmäksi kuin ruotsalaista, mutta demokraattisemmaksi kuin ranskalaista. Suomalaisten johtajien arvostettuja ominaisuuksia ovat muun muassa yhteisten tavoitteiden asettaminen, kyky tiimien luomiseen ja johtamiseen, asiantuntijoiden kunnioittaminen sekä kykyyn mukauttaa johtamistyyliään eri tilanteisiin. Motivaation näkökulmasta tärkeimpiä asioita ovat johdonmukaisuus, yhteisten tavoitteiden asettaminen ja saavuttaminen, tehokkuus sekä sanojen ja tekojen kohtaaminen. Reaktiiviselle kulttuurille ominaisella tavalla, muutos täytyy toteuttaa hitaasti ja sen kohteena olevia henkilöitä osallistaen. Muutoksille tulee olla selkeä peruste, koska toimivia malleja arvostetaan. Innovaatiot syntyvät kollektiivisen ajattelun perusteella. (Lewis, 2005; Lewis, 2006).

Tämän tutkimuksen näkökulmasta ja Hofsteden (1999) sekä Lewisin (2005) julkaisuihin perustuen suomalaisen voidaan luonnehtia hoitavan hänelle annetut tehtävät loppuun asti ja selvittää asian, ellei hänellä ole asiaan valmista vastausta tai tietoa. Suomalaiseen kulttuuriin kuuluu nopea sopeutuminen tilanteeseen ja toiminta tilanteen vaatimalla tavalla. Perusteet työtehtävän toteuttamisen aikana tehtäville valinnoille perustuvat faktoihin reaktiivisuuteen. Asioista keskustellaan avoimesti ja suoraan, mikä mahdollistaa asioiden tarkastelun yhdessä useasta eri näkökulmasta. Vuorovaikutus on suoraa ja asiapitoista. Päätökset tehdään faktoihin perustuen. Päätösvalta on matalalla ja johtajat toimivat osana tiimejä. Keskustelevuudesta ja osallistamisesta huolimatta nopeaa päätöksentekokykyä arvostetaan. Asiantuntijoilla on valta tehdä päätöksiä heille määritetyissä rajoissa. Vaatimattomuutta arvostetaan, mikä voi näkyä siten, ettei suomalainen tuo osaamistaan mutta toisaalta ei myöskään puutteitaan esiin. Suomalainen osaa toimia ryhmässä, mutta arvostaa yksinäisyyttä ja henkilökohtaista tilaa. Luottamalla toiseen henkilöön suomalainen osoittaa myös arvostusta hänen ammattitaidolleen.

Kyberturvallisuuskulttuurin muodostumisen näkökulmasta suomalaisessa kulttuurikontekstissa annetaan painoarvoa yksilön toiminnalle sekä painottaa koulutusta ja osaamista. Ohjeiden ja vastuujaon tulee olla selkeitä ja yksinkertaisia. Vastuut ja päätösvalta kulkevat käsi kädessä, ja ne tulee jakaa osa-alueisiin yksilötasolta lähtien. Vastuut tulee yksilöidä henkilölle enemmän kuin ryhmälle. Yksilöiden osaamiseen perustuva toiminta voi tuottaa eroavaisuuksia kyberturvallisuuden tasossa organisaatioiden eri osien välillä. Turvallisuuteen liittyvien ratkaisujen ja ohjeiden tulee perustua faktoihin ja tietoon, tavoitteena yksilön ymmärryksen lisääminen ja organisaation osaamisen kasvattaminen toimintaohjeiden sijaan.

4 Reaktorin kyberturvallisuuskulttuuri ja sen vaikutus organisaation kyberturvallisuuteen

Tässä luvussa esitetään haastatteluissa esiin tulleiden ilmausten perusteella muodostetut ja nimetyt merkityskategoriat, jotka sidotaan haastatteluissa esiin tulleisiin yksittäisiin ilmauksiin. Havaintoja peilataan muuhun tutkimustietoon suhteessa organisaation kyberturvallisuuskulttuurin rakentumisesta. Tulokset esitetään haastattelussa käytettyjen teemojen kautta. Haastateltavien taustoja koskevia tietoja on hyödynnetty ilmaisujen ja erojen selittämisessä.

Esimerkkeinä käytettäviä haastateltavien ilmaisuja on muokattu siten, ettei niistä pysty tunnistamaan yksittäistä henkilöä, ohjelmistoa tai laitetta. Luvussa esitetään runsaasti sitaatteja, jotta analyysista välittyy sen aineistolähtöisyys. Sitaattien valinnassa kiinnitettiin huomiota siihen, miten ne kuvaavat esitettyä ajatusta. Esitetyt sitaatit on hyväksytetty Reaktorin edustajalla.

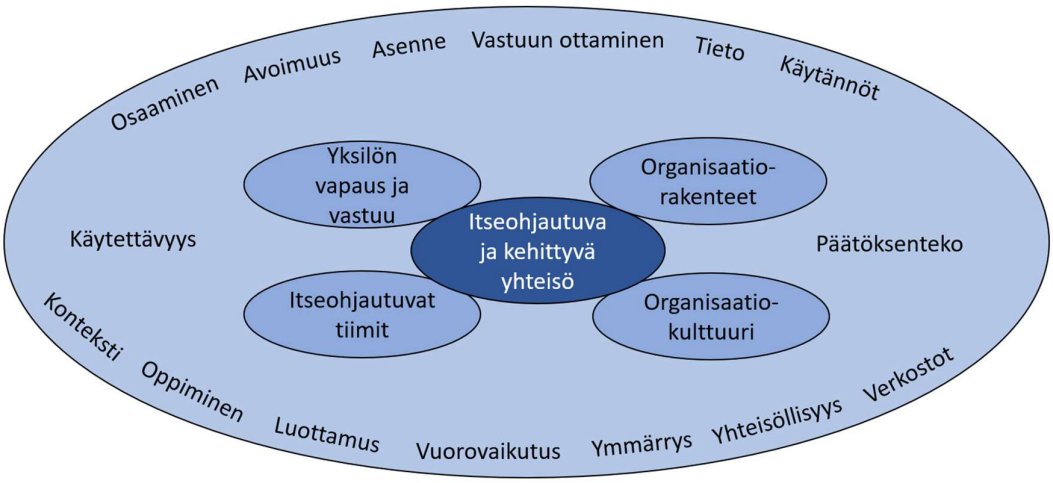
Haastateltavat jaoteltiin karkeasti kolmeen ryhmään työtehtävien perusteella. Jako ei ole täysin yksiselitteinen, koska Reaktorilla yksittäisen henkilön työtehtävät eivät ole tiukasti määritelty. Hän voi kuulua kiinnostuksensa ja osaamisensa perusteella tiettyä toiminnallisuudesta vastaavaan ryhmään. Ryhmät on esitetty taulukossa 3. Yksittäistä haastateltavaa kuvataan tässä luvussa ryhmää kuvaavalla tunnisteella, johon on lisätty järjestysnumero (esimerkiksi KON 1, KEH 3).

Ryhmä	Haastateltavien määrä	Kuvaus työtehtävien sisällöstä	Tunniste
Konsultointi	4	Asiakasprojektit, asiakkaiden konsultointi	KON
Tukitoiminnot	3	Markkinointi, tilojen käytön suunnittelu, järjestelmien ylläpito	TUK
Sovelluskehitys	3	Ohjelmointi, graafinen suunnittelu ja käyttöliittymäsuunnittelu	KEH

Taulukko 3. Haastateltavien jaottelu työtehtävien mukaan ja käytetyt tunnisteet

4.1 Reaktorin kyberturvallisuuskulttuuri – itseohjautuva ja kehittyvä yhteisö

Tutkimuksen empiirisen osuuden aikana toteutettujen teemahaastattelujen aineisto käsiteltiin käyttäen fenomenografista analyysia. Haastateltavien käsityksistä muodostettiin aineistolähtöinen teoria Reaktorin kyberturvallisuuskulttuurista (kuva 12). Kokonaisuus koostuu kolmen eri tason kategorioista. Ylintä kategoriaa määrittää neljä toisen tason kuvauskategoriaa. Ne jakoivat runsaasti kolmannen tason teemoja, jotka esitetään yhteisinä vaikuttajina.



Kuva 12. Reaktorin kyberturvallisuuskulttuurista fenomenografisen analyysin perusteella muodostetut eri tason kategoriat

Tulevissa alaluvuissa edetään yksilötasolta tiimeihin, josta siirrytään organisaatiokulttuurin ja organisaation rakenteiden kautta itse ilmiön kuvailemiseen. Tämä tapa valittiin kategorioiden esittämiseksi, koska havaittiin pienempien kokonaisuuksien sisältyvän suurempiin. Näin on myös helpompi ymmärtää mistä tutkimuksen keskeinen ilmiö rakentuu.

Kappaleen tavoitteena on tuoda esille aineiston perusteella ilmauksista muodostettuja kategorioita ja harvinaisuuksia, jotka on muodostettu ilmauksista aineiston perusteella. Kategorioita kuvataan yksittäisen haastateltavan kategoriaa edustavalla tai siitä poikkeavalla ilmauksella, jotka on litteroitu suoraan haastattelusta.

4.2 Yksilön vapaus ja vastuu – henkilökohtainen kyberturvallisuuskulttuuri

Adele Da Veigan (2016) kyberturvallisuuskulttuurin määritelmän mukaan organisaation kyberturvallisuuskulttuuriin vaikuttaa organisaatiossa toimivien työntekijöiden henkilökohtainen kyberturvallisuuskulttuuri eli näkemykset ja toimintatavat. Kyberturvallisuuden henkilökohtainen taso ulottuu sekä työ- että henkilökohtaiseen elämään.

Tässä tutkimuksessa yksittäisten työntekijöiden kyberturvallisuuskulttuuriin sisällytettiin henkilön taustoihin, arvoihin ja arvojen vaikutuksiin liittyviä kysymyksiä, joita peilattiin tutkimuksessa käytettävään teoriaan suomalaisesta kansallisesta kulttuurista. Taustoihin liittyvät kysymykset auttoivat myös tutkijaa ymmärtämään haastateltavan näkemyksiä ja ilmauksia. Tämän jälkeen kartoitettiin haastateltavien henkilökohtaisia käsityksiä kyberturvallisuudesta

ilmiönä ja siihen liittyvistä uhkista sekä heidän asennettaan kyberturvallisuutta kohtaan ja kyberturvallisuutta koskevia käytäntöjään. Kyberturvallisuus ulotettiin koskemaan haastateltavan kaikkea toimintaa. Tavoitteena oli selvittää myös käsitysten ja asenteiden taustalla olevia tekijöitä: koulutuksen, henkilökohtaisten kokemusten sekä median ja työpaikan vaikutusta käsitysten muodostumiseen. Keskiössä oli löytää mahdollisia yhteisiä tai erottavia tekijöitä, jotka vaikuttavat haastateltavien ilmauksiin tutkimuksen kontekstissa.

Haastateltavien ilmausten perusteella henkilökohtaisesta kyberturvallisuuskulttuurista on kyberturvallisuus kaikkialla läsnä oleva arkipäiväinen ilmiö. Ilmaisujen perusteella kyettiin tunnistamaan kuusi eri kategoriaa:

- asenne kyberturvallisuutta kohtaan,
- ymmärrys kyberturvallisuudesta ja siihen liittyvistä ilmiöistä,
- henkilökohtaisen kyberturvallisuuden ylläpitämistä tukevat käytännöt,
- kokemukset kyberturvallisuutta uhkaavista tilanteista,
- sosiaalinen media ja tietosuoja sekä
- kyberturvallisuutta ja ICT-välineitä koskeva osaaminen.

Käsitys ja ymmärrys kyberturvallisuudesta sekä siihen kuuluvista ilmiöistä

Käsitykset kyberturvallisuudesta sekä siihen kuuluvista osa-alueista ja ilmiöistä vaihtelivat vastaajien välillä. Kyberturvallisuuden määrittelyn yhteydessä tietoturvan, tietosuojan ja sosiaalisen median käsitteet nousivat useasti esiin. Osalla haastateltavista kyberturvallisuus limittyi tai sekoittui tietosuojan kanssa. Yksittäiset haastateltavat painottivat joko tietoturvaa tai sosiaalista mediaa. Kyberturvallisuuden ja tietoturvan suhde tai rajapinnat eivät olleet selkeitä. Kyberturvallisuuden jakautuminen kahteen keskeiseen elementtiin, käyttäjien toimintaan ja teknisiin ratkaisuihin, tuli esille käytännössä jokaisessa haastattelussa joko suoraan tai välillisesti esimerkkien kautta.

Yksittäinen haastateltava ilmaisi, ettei tarkalleen tiedä mitä kyberturvallisuus tarkoittaa. Hän epäili, että moni muu ajattelee samalla tavalla, mutta kukaan uskalla myöntää tietämättömyyttään tai ymmärtämättömyyttään.

”Mä en itse asiassa osaa eritellä tietoturvaa ja kyberturvallisuutta” (KEH 2)

”Et kaikki puhuu siitä, mut must tuntuu siltä et kukaan ei ikinä uskalla sanoa hei et mä en itse asiassa ymmärrä helvettiäkään tosta et mitä toi tarkottaa.” (TUK 1)

Muutama haastateltava mainitsi kyberturvallisuuden roolin korostuvan nykypäivän ihmisen elämässä. Kyberturvallisuuden nähtiin ulottuvan kaikille elämän osa-alueille ja siinä olevan runsaasti erilaisia näkökulmia.

”Mä nään sen sillei niin kuin hyvin niinku laajasti sellasena niinku eettisenä, poliittisena teknisenä, niinku kenttänä, joka vaikuttaa nykypäivänä niinku kaikkeen ihmisen toimintaan.” (KON 3)

Muutaman haastateltavan kertomuksissa mainittiin maailmanpolitiikan tapahtumien vaikutukset kyberturvallisuutta ja uhkien lisääntymistä kohtaan. Ilmauksissa mainittiin informaatiovaikuttaminen ja valheellisen informaation levittäminen internetissä. Eri valtioiden harjoittama käyttäjien seuranta ja tiedonkerääminen käyttäjistä myös nähtiin uhkana yksityisyyttä kohtaan. Yksilöä kohtaan kohdistuvat uhkat nähtiin kohdistuvan älypuhelimeen, kodin älylaitteisiin, henkilötietoihin tai luottokortteihin.

"Tai miten niin kuin nään mitä niin kuin vois sattua on just joku, sekin on siis aika epätodennäköistä, mut voihan se olla mahdollista, identiteettivarkaus. Mut todennäköisempää on, että joku joskus kopioi mun luottokortin. Se mun mielestä vois jopa olla aika todennäköistä. Mä uskon et joku jonain päivänä voi ottaa etähallintaan, käydä käsiks mun puhelimeen." (KEH 2)

Käsitykseen kyberturvallisuudesta vaikutti haastateltavien suhtautuminen ja ymmärrys kyberuhkista. Teknisesti koulutut, esimerkiksi sovelluskehittäjät ja järjestelmäarkkitehdit, kertoivat järjestelmien rakennetta ja rakentamista sekä rakentamiseen käytettävistä menetelmistä koskevasta osaamisestaan. Sen avulla he näkivät haavoittuvuuksien läsnäolon jatkuvaksi ja haavoittuvuuksien olemassaololle erilaisia syitä. Heidän vastauksistaan tuli esille kattava näkemys tietoverkoista ja -järjestelmistä laitteiden, verkkoinfrastruktuurin, protokollien ja tiedon kokonaisuutena. Kyberturvallisuuden ylläpitämiseen ja haavoittuvuuksien vähentämiseen tähdättiin suunnittelemalla ja valitsemalla toimivia ratkaisuja sekä keskittymällä tekemään perusasiat hyvin. Inhimillisen virheen mahdollisuus mainittiin useassa haastattelussa.

"Jos aattelee vielä nimenomaan täst niin kuin duunin puolesta, niin siin on niinku sitä et millä niin kuin et millä perusteella valitaan ensinnäkin ohjelmointikieliä johonkin tarkotukseen, sit sellasia niin kuin kirjastoja tai alustoja, mitä käytetään. Ja sit sitä sellasta designia silleen et ennen kuin ruvetaan miettimään jotain uutta järjestelmää tai jotain uutta ominaisuutta olemassa olevaan järjestelmään. Samalla kun miettii niin kuin sitä pihviä et mikä on niin kuin se päämäärä millä saadaan jotain hyötyä jollekin ihmiselle siitä järjestelmästä niin samalla pitää mielessä ne uhkat ja sellaset et mitkä kaikki asiat voi mennä niinku pieleen ja et millä tavalla niitä sit vois käyttää joko hyväkseen joku pahantahtoinen hyökkääjä tai sitten ne voi jonkun inhimillisen mokan takia sitten aiheuttaa sitä, että tulee vaikka julkisuuteen jotain tietoa mitä ei sais tulla." (KON 2)

Muutama vastaaja näki kyberturvallisuuden laajempana ilmiönä, joka kattaa teknisen ulottuvuuden ja sen eri tasoilla tehtävien toimintojen lisäksi myös organisaation toiminnan muita osia. Tämän perusteella kyberturvallisuuden eri näkökulmien huomioiminen vaatii huomioita organisaation eri osilta ja monipuolista osaamista.

"Siin pitää muistaa sit näiden teknisten asiantuntijoiden lisäksi sitten myös sellaiset domain- tai liiketoiminnan asiantuntijat, jotka tuntee paremmin vaikka näihin riskeihin liittyvät juridiset tai muut tollaset tekijät." (KON 2)

Kyberturvallisuutta ja kyberuhkia koskeva tieto ja osaaminen vaati haastateltavien mukaan jatkuvaa opiskelua ja tietämyksen pitämistä ajan tasalla. Moni muuten kuin teknisesti suuntautunut haastateltava mainitsi, että kyberturvallisuutta koskevat asiat ovat tulleet tutuksi työelämän kautta. Useampi edellä mainittu haasteltava oli siirtänyt työssä oppimiaan käytäntöjä ja hyödyntänyt kyberturvallisuutta koskevaa tietämystään myös henkilökohtaisessa elämässään. Yksittäinen haastateltava ilmaisi, että ilman teknistä koulutusta kyberturvallisuutta koskevat asiat ovat haastavia ymmärtää eikä siitä ole aina saatavissa tietoa ymmärrettävästi.

"En mä esimerkiksi ymmärrä miksi vaikka Chromessa on joku haavoittuvuus tai aukko, mutta jos sen pystyisi jotenkin maallikolle selittämään niin kuuntelisin." (KEH 2)

Lähes jokainen haastateltava oli kiinnostunut lisäämään tietämystään ja ymmärtämystään kyberturvallisuudesta. Esimerkiksi uutisista saatava tieto ja henkilökohtaisten laitteiden suojaamista koskevien ohjeiden kerrottiin johtavan toimenpiteisiin. Ongelmalliseksi nähtiin myös kyberturvallisuutta koskevan tiedon vanheneminen ja käytäntöjen muuttuminen.

"Olispa niin että sulla olis tavallaan joissain jutuissa tiettyjä käytäntöjä, että kun oot tehny tietyllä tavalla niin se on niinku hyvä. Niin se ei, niinku tämmösiä käytäntöjä ei vaan ihan hirveen helposti tunnu niinku löytyvän, moniinkaan asioihin. Se nimenomaan just sillei muuttuu ajassa ja se mitä joskus on sillei tehty, niin se ei sit oo enää niinku 2019." (KEH 1)

Henkilökohtaisen kiinnostuksen ja asenteen merkitys järjestelmien ja tietojen suojaamisessa korostui vastauksissa. Vaikka haastateltava ei ollut suorittanut teknisesti painottunutta koulutusta esimerkiksi korkeakoulussa tai hänellä ei ollut tietotekniikkaan liittyvää harrastuneisuutta, hän kykeni ymmärtämään uhkien kohdistumista ja luonnetta, koska hänellä oli henkilökohtaista kiinnostusta tietojen suojaamiseen.

"Tietoisuus uhkista jo jeesaa siinä." (TUK 2)

Asenne kyberturvallisuutta kohtaan

Huolimatta eroavaisuuksissa kyberturvallisuutta ja siihen sisältyviä asioita kohtaan, oli haastateltavien asenne kyberturvallisuutta kohtaan pääpiirteittäin melko yhtenevä. Kaikki haastateltavat tiedostivat kyberturvallisuuden ja tietosuojan merkityksen myös henkilökohtaisessa elämässään, joka ilmeni arkisina toimenpiteinä. Eroja ilmeni teknisesti koulutettujen tai osaavien ja muiden välillä, mitkä näkyivät käsityksissä omasta osaamisesta ja tieto- ja viestintätekniikan

käytön varmuudessa suhteessa kyberuhkiin. Osa teknisesti koulutetuista kuvaili asennettaan viitaten humoristisesti ”foliohattuun”, kun taas osa kertoi pyrkivänsä välttämään ”foliohattuilua” eli suhtautumaan kyberuhkiin realistisesti ja mitoittamaan turvallisuustoimenpiteet uhkia vastaan realistisesti.

Haastateltavien ilmausten perusteella täydellistä kyberturvallisuutta ei ole ja uhkien läsnäolo ei tule katoamaan. Kaikki tekniset ratkaisut ovat murrettavissa, mikäli hyökkääjällä on riittävästi aikaa, osaamista ja rahaa. Tästä huolimatta tästä tietty kyberturvallisuuden taso tulee saavuttaa, ettei organisaatio tai yksilöt sorru yksinkertaisiin virheisiin. Kyberturvallisuutta koskevien valintojen tulee olla tietoisia, ja ratkaisut tulee perustaa tutkittuun tietoon tai tunnettuihin hyviin käytäntöihin. Kontekstilla oli myös vaikutusta tietoturvan ja kyberturvallisuuden tasoon. Sen takaamiseksi esitettiin tilanteen arvioimista jokaisessa tilanteessa erikseen sekä tilanteeseen sopivien työkalujen ja ratkaisujen valitsemista.

Kyberturvallisuus nähtiin arkipäiväisenä ja luonnollisena asiana, joka täytyy ottaa huomioon vastaavalla tavalla kuin fyysinen turvallisuus. Kyberturvallisuuteen liittyvien kontrollien käyttämistä verrattiin esimerkiksi kodin ulko-oven lukitukseen ja kotiavaimeen. Tietoturva-asioissa mainittiin myös käytettävyyden arvostaminen suhteessa tietoturvaan niin että tietoturvaratkaisut ovat vaadittavalla tasolla, mutta käytettävyys ei kärsi liikaa.

”Kyberturvallisuus on kulttuuria, se on tapa toimia. Se on vähän niinku, kun me lähdetään kotoa niin me katotaan, onko kahvinkeitin jäänyt päälle.” (TUK 3)

”Se on vähä, vähän niinku hygienia tavallaan, et se ei oo niinku mun elämää ohjaava tekijä vaan semmonen mikä pitää ottaa huomioon.” (KEH 3)

Epäileväisyys ja valppaus korostuivat haastateltavien vastauksissa, koska uhkien läsnäolo tiedettiin ja koettiin jatkuvaksi. Uhkien koettiin lisääntyneen suhteessa nuoruuteen tai kouluaikoihin.

”Eihän sitä voi mennä enää ihan avoimena kekkosena nettiin.” (KEH 2)

Henkilökohtainen kyberturvallisuus, tietoturva ja tietosuoja koettiin tärkeiksi asioiksi. Haastateltavat ilmaisivat näkevänsä vaivaa tietojensa turvaamiseen, vaikka syyt siihen vaihtelevatkin. Osa mainitsi suojaavansa tietojaan ja laitteitaan periaatteen vuoksi. Moni ei kokenut itseään merkittäväksi henkilöksi tai että hänellä ei ole hallussaan mitään merkittävää tietoa. Henkilökohtaisessa elämässä identiteetti tunnistettiin turvattavaksi asiaksi, jonka kautta voisi realisoitua erilaisia uhkia rikollisten suunnasta. Työnantajan laitteet ja tieto koettiin tärkeämmäksi kuin henkilökohtaisessa käytössä tai hallinnassa olevat. Etenkin muun kuin teknisen koulutuksen omaavien ilmauksista tuli esille ero työ- ja vapaa-ajalla käsiteltävien tietojen tärkeydestä.

Perusymmärrys tietoturvasta ja kyberturvallisuudesta nähtiin kuuluvan jokaisen yksilön yleissivistykseen, erityisesti teknisellä alalla työskennellessä. Kyberturvallisuuden osaaminen ja ymmärrys sisällytettiin vastauksissa ammattitaitoon sekä osaamisen jatkuva ylläpito tiedon hankkimisen ja keskusteluun kautta.

"Se on yks osa sitä osaamispalettia, jota tarvitaan nykypäivänä ihan missä vain töissä." (TUK 2)

Tietoturva nähtiin erottamattomaksi osaksi ohjelmointia ja ohjelmistosuunnittelua. Tietoturva on yksi laadukkaan tuotteen sisäänrakennetuista ominaisuuksista, joka tulee ottaa huomioon heti alusta alkaen tuotteen suunnittelussa ja rakentamisessa. Tietoturva pystytään ottamaan huomioon ohjelmistojen ja laitteiden suunnittelussa, mikäli siihen kiinnitetään jatkuvasti huomiota.

"On nykyihmisen ammattitaitoa muistaa se tietoturva." (TUK 2)

Muutama haastateltava mainitsi, etteivät tunne itseään varmoiksi tieto- ja viestintätekniikan käytössä suhteessa uhkiin. Haastateltavat tunnistivat, että ilman teknistä suuntautuneisuutta oleva henkilö ei voi ymmärtää kaikkea uhkiin liittyvää. Uhkien vaikutusta voi kuitenkin vähentää kiinnittämällä huomiota toimintatapoihin sekä tiedostamalla eri välineiden ominaisuudet käsiteltäessä ja välitettäessä niillä tietoa.

"En [tunne itseäni varmaksi], mä uskon, että aina on joku fiksumpi kuin minä." (KON 4)

"Mietin, että mitä tietoa voi laittaa ja millä välineellä se kannattaa laittaa." (KON 4)

Yksittäinen haastateltavista ilmaisi suoraan olevansa tieto- ja viestintätekniikan käytön suhteen laiska, vastustavansa teknologian käyttöä ja kertoi, ettei hän jaksa paneutua asiaan liikaa. Hän sanoi käyttävänsä vanhoja toimintatapoja, vaikka uusien toimintatapojen opettelu helpottaisi hänen työtään. Hän myös mainitsi, että tunnistaa itsensä potentiaaliseksi tietoturvariskiksi. Hänen mielestään organisaation tulisi asettaa enemmän tietoturvakontrolleja hänen kaltaisiaan ihmisiä varten, jotta perusasioiden toteutuminen tietoturvassa tulisi huomioitua riittävällä tasolla.

"Mä tiedän! Mä oon tietoturvariski!" (TUK 1)

Henkilökohtaiset kyberturvallisuuteen liittyvät käytännöt

Moni haastateltava painotti perustoimenpiteiden tekemistä eli laitteiden asetusten tarkistamista ja säätämistä aina ennen laitteiden käyttöönottoa. Asetukset ilmaistiin säädettävän aluksi liian tiukalle ja löysennettävän tarpeen mukaan. Haastateltavien mainitsemat käytännöt jakautuivat teknisiin ja toiminnallisiin keinoihin. Yksityiskohtaisimmat käytännöt on tarkoituksella kuvattu yleisemmällä tasolla tässä tutkimuksessa. Näistä tekniset käytännöt sisälsivät esimerkiksi yksittäisen käyttäjän tietoturvaa helpottavien ja tietojen hallintaan tarkoitettujen sovellusten käyttöä. Verkkoliikenteen salaaminen, kovalevyn

kryptaaminen, VPN-sovellusten käyttö, monivaiheinen tunnistautuminen ja tietojen kryptaaminen tulivat haastatteluissa myös useasti esille.

Haastateltavat korostivat turvallisuuden huomioonottamista myös työkalujen ja menetelmien valitsemisessa. Tietojen arkaluonteisuuden ja vakavuuden kerrottiin määrittävän käytettävät menetelmät. Turvallinen toiminta esitettiin lähtökohtana, etenkin jos turvallisempi vaihtoehto ratkaisusta tai menetelmästä on olemassa.

"Miksi niinku käytettäis tyyliin telnettiä yleensäkään yhtään mihinkään, kun SSH on ollu olemassa jo 90-luvun puolesta välistä lähtien jo?" (KEH 1)

Haastateltavien esittämät toiminnalliset käytännöt koostuivat yleisistä ja yksittäisiä tilanteita olevista toimintamalleista. Valppaus ja epäileväisyys tulivat esille. Linkkien ja sähköpostin liitteiden avaamisessa painotettiin harkintaa ja tarkastelua. Tarvittaessa haastateltavat ottivat aikaa ja miettivät rauhassa tilannetta, mikäli jotain epäilyttävää tai epänormaalia havaittiin. Tietojen jakamisen tilanteissa korostettiin harkintaa sekä tarpeen ja tietojen pyytäjän motiivin ja todellisen tarpeen miettimistä ennen toimintaa. Sensitiivisen tiedon tunnistaminen oli ehtona tiedon jakamiseen liittyvälle harkinnalle.

Luottokorttien käyttöön niin internetissä kuin fyysisessä maailmassa tunnistettiin sisältyvän uhkia. Yksi haastateltava kertoi käyttävänsä tiettyä luottokorttia ainoastaan verkossa tapahtuviin ostoksiin. Toinen haastateltava mainitsi miettineensä etälukemisen estävää suojaa lompakossaan oleville luottokorteille.

Henkilökohtainen tiedonhallinta tuli esiin varmuuskopioiden ottamisen ja digitaalisen jalanjäljen yhteydessä. Yksittäinen haastateltava toi esille tapansa tehdä säännöllisesti henkilökohtaisten tietojen jakamisen seuraamista ja rajoittamista. Tämä koski hänen rekisteröitymistään palveluihin ja aiemmin internetissä jakamaansa tietoa.

"Konmaritan niin kuin digitaalisen jalanjäljen." (KEH 2)

Sosiaalinen media ja digitaalinen jalanjälki

Tietosuojaa pyrittiin huomioimaan ja digitaalisen jalanjäljen muodostumista pyrittiin estämään kiinnittämällä huomiota henkilökohtaisten tietojen jakamiseen. Moni haastateltava kertoi pyrkivänsä minimoimaan tietoja, mitä jakavat itsestään sosiaaliseen mediaan tai verkkopalveluihin. Osa haastateltavista kertoi tiedostaneensa sosiaalisen median kautta tapahtuvan tiedonkeruun ja uhkat vasta myöhemmin, mikä on johtanut toimintamallien muuttamiseen heidän saatuaan lisää tietoa aiheesta.

"Facebookkiin on tullut aika paljon tietoa tuutattua, mutta ei enää." (KEH 2)

Haastateltavat suhtautuivat Facebookiin, sen omistamiin palveluihin ja sovelluksiin yleisesti epäilevästi, koska he tiedostivat yrityksen palveluihin kautta yksityisyyteen kohdistuvat uhkat. Yksittäinen haastateltavat tarkensi, ettei käytä

älypuhelimeen asennettua Facebook-sovellusta, vaan erillisellä selaimella ja tarkemmin määritetyillä asetuksilla.

Yksittäinen haastateltava kertoi, että on kuullut kollegoiden ilmoittavan vaihtelevia ja vääriä tietoja verkkopalveluiden rekisteröitymisvaiheissa. Hän ilmaisi tämän toiminnan käytännön tavoitteeksi käyttäjän profiloinnin vaikeuttamisen ja sitä kautta epämieluisten kohdennettujen mainosten välttämisen.

Osaaminen ja varmuus tieto- ja viestintätekniikan käytössä suhteessa kyberturvallisuuteen

Harvan haastatellun koulutus oli sisältänyt mitään koulutusta kyberturvallisuuteen liittyen, vaan tietoa oli omaksuttu uutisista, koulutuksista ja yrityksen sisäisistä tiedotuskanavista. Kysyttäessä suurin osa haastateltavista koki itsensä varmoiksi tieto- ja viestintätekniikan käytössä. Osa haastateltavista perusteli tuntemustaan varmuudesta kyvyllä ymmärtää kyberuhkia tietoverkkotekniikan tai vastaavan osaamisen kautta. Epävarmuutta aiheutti kuitenkin tieto- ja viestintätekniikan läsnäolo kaikilla elämän osa-alueilla.

"Epävarmuus tulee epätoivosta, kun mitään ei voi oikein tehdä ilman verkkoyhteyksiä ja laitteita." (KON 1)

Kaikki haastateltavat kertoivat kokevansa itsensä valistuneiksi tai osaaviksi kyberturvallisuuteen liittyvissä tiedoissa ja taidoissa. Joka tapauksessa eri työtehtävissä työskentelevien välillä ilmeni luonnollisesti eroavaisuuksia. Muuten kuin teknisesti suuntautuneet haastateltavat lähtökohtaisesti arvioivat osaamisensa perustasolle tai vähän sen yläpuolelle.

"Mä oon ehkä jollain perustaso plussalla." (KON 4)

Henkilökohtaiset kokemukset kyberturvallisuudesta ja -uhkista

Lähes jokaisella vastaajalla oli henkilökohtaisia kokemuksia kyberturvallisuuteen liittyvistä tapahtumista, joilla oli ollut vaikutuksia usean haastateltavan asenteeseen tai toimintaan. Kokemukset liittyivät työtehtäviin, henkilökohtaiseen elämään ja kyberuhkia koskevaan uutisointiin. Kokemukset ovat liittyneet joko haastateltavaan itseensä tai hänen lähipiiriinsä. Osassa tapahtumista uhka oli kyetty tunnistamaan selkeäksi ja tarkoituksella toteutetuksi hyökkäykseksi. Tämän lisäksi haastateltavat mainitsivat myös epäselvistä tapauksista, jossa kynnys epäilyyn oli ylittynyt mutta tapahtuma oli jäänyt epäselväksi tai uhka ei ollut tunnistettavissa suoranaisesti hyökkäykseksi.

"On tullut tilanteita, jossa on joutunut admineilta kysymään miksi selaimessa tapahtui jotain." (KEH 2)

Henkilökohtaisia kokemuksia koskevissa ilmauksissa tuli useasti esille myös kokemukseen liittyvän tapahtuman henkilökohtaisuus ja sen aiheuttama

tunnereaktio. Paras esimerkki on haastateltavan kuvailema kokemus organisaation toteutusta red teaming -harjoituksesta, joka on tässä tapauksessa jaettu kahteen osioon:

"Meillehän tehtiin tänne semmonen niinku, en tiedä mikskä sitä nyt sanotaan, red team -harjoitus. Se järjestelmä, jonka päällä mä istun, niin tavallaan, niinku ikään kuin sen osana yritettiin kräkkää. Ja se on niinku sellanen kokemus, että jos on ikinä saanu sellasen kokemuksen, niin sitäpä ei ihan hevillä unohda." (KEH 1)

"Onhan se niinku se äärimmäisen niinku emotionaalinen se response. Et niinku tavallaan, ku monesti niinku asioihin voi suhtautua niinku semmosina, et tää on niinku tämmönen resursointikysymys, mut kun jotain tollasta tapahtuu niin se ei oo enää resursointikysymys." (KEH 1)

Yhdellä haastateltavalla oli henkilökohtainen kokemus varusmiespalveluksen aikaisesta tietojenkalastelusta sähköpostitse, jonka hän oli suoraan tunnistanut epäilyttäväksi. Toisella oli kokemus lähipiirissä tapahtuneesta tietomurrosta, jossa sähköpostiin tullut linkki oli ohjannut sivustolle ja mahdollistanut henkilön tilin kaappaamisen. Haastateltava kertoi tiedostavansa läheisen henkilön tilille murtautumisen mahdollistavan hyökkääjälle toiminnan jatkamisen lähettämällä linkkejä edelleen tilin omistajan kontaktiverkossa ja esiintymisen luotettuna toimijana.

"Oli menny klikkaamaan jotain linkkii, kun oli tullu, että saa jonkun ilmasen jutun. Sit se tili korkattiin ja sithän se meni niinku häkkerille. Toki sit rupes, pääs, spämmäämään linkkejä myös muualle." (KON 3)

4.3 "Kaukopartioryhmät" – itseohjautuvat tiimit

Reaktorin toiminnan keskiössä ovat tiimit, joiden tehtävänä on hoitaa tiettyä toimintoa tai asiakasprojektia. Tiimien rakentamiseen kiinnitetään huomiota niin että tiimeihin saadaan riittävä osaaminen ja kyky tehdä päätöksiä sekä sen toimivuus pystytään kaikilla tavoin takaamaan. Projektin luonne vaikuttaa tiimiin tarvittavaan osaamiseen. Rekrytoitaessa organisaatioon kiinnitetään huomiota työntekijän kykyyn toimia osana itseohjautuvaa tiimiä. Haastateltavat näkivät organisaation tiimirakenteen toimivaksi.

"Yksilön ei tarvii aina olla itseohjautuvia, kun kaikki ei oo. Mut tiimien pitää olla." (KON 1)

Asiakasprojekteissa toimivien tiimien tehtävänä on muodostaa käsitys asiakkaan tarpeesta, muodostaa siitä näkemys ja vastata tarpeeseen. Käytännön yksityiskohdat sovitaan asiakkaan kanssa, vaikka asiakkaan kanssa sopimuksen tekemisestä ja noudattamisesta tiimi ei täysin vastaakaan. Koska tiimit toimivat erillään

muista tiimeistä ja pääkonttorin henkilöstöstä, yleensä asiakkaan tiloissa, vastaa asiakasprojektin tiimi kaikesta projektin toiminnasta. Tiimeillä ei ole kiinteää rakennetta tai selkeitä rooleja, vaan ne organisoituvat ja jakavat työtehtävät sisäisesti. Tiimien toimintaa selkeytetään käyttämällä erilaisia projektinhallintaan tarkoitettuja malleja, joiden käyttötavan määrittelee tarve.

"Mä nään niinku sellasta kaukopartio-, niinkun analogiaa. et kun sä oot rajan toisella puolen, niin sä et voi, se on sen jengin ite hoidettava se homma ja se on kaikkien vastuulla. Jollain voi olla jotain spesifejä vastuita, et se ainakin katsoo sen perään, mut se on se porukka." (KON 1)

"Se et se ois selkeetä, vaatis että meillä olis jotkut tietynlaiset roolit. Ei meillä oo, vaan me tehdään sitä mitä tarvii." (KON 4)

Reaktorin vahvassa organisaatiokulttuurista tiimeillä on runsaasti vapautta tiimin toiminnan organisoimisessa, päätöksenteossa ja projektin hoitamisessa. Tiimit organisoituvat sisäisesti ja asettavat itselleen tavoitteita. Tiimeillä on vapaus sopia sisäiset toimintatavat ja käytettävät menetelmät.

"Jokaisen tiimin tulee itse keksiä tapansa olla Reaktor." (KON 2)

"Porukalla sovitaan tiimin tavoitteet ja toimintatavat millä niitä edistetään." (KEH 3)

Tiimien toiminta perustuu organisaatiokulttuurin mukaisesti keskinäiseen luottamukseen. Luottamus yksilöiden ja yksittäisen tiimin toimintaa nähtiin ääritapauksissa myös riskinä tai heikkoutena.

"Kun kaikis tavois organisoitua on joku semmonen tietty heikkous, niin meidän niinku tavassa, se niinku se ihmisten keskinäinen luottamus, mikä on hiton iso vahvuus, niin se on myös tämmönen niinku reikä ja uhka. Et sit, jos jokin niinku feilaa eikä hommia ookaan hoidettu kunnolla, niin mitäköhän sitten tapahtuu." (KEH 1)

"Et esimieshierarkiassa on yleensä silleen helppoo et, jos joku yksilö alkaa voida huonosti niin sillä on itsestään selvä taho mihin se voi ottaa yhteyttä. Meil se on vähän hankalampaa, koska se on se eka selvä taho olis tavallaan se tiimi, mut jos se koko tiimi on vähän niinku tavallaan sellasessa projektissa, jossa asiat alkaa mennä vähän hullusti ja ne on vähän niinku kaikki samassa kattilas kiehumas. Niin se ei ookaan enää mitenkään selvä et sä saat sieltä [tiimistä] tukea ja ymmärrystä, ja mihin sä sitten meet ja mitä sä sitten osaat tehdä." (KEH 1)

Tiimien toimivuus ja niiden sisällä oleva joukkuehenki vaihtelee. Haastateltavien ilmausten perusteella siihen vaikuttavat henkilöt, toimintatavat, henkilösuhteet ja tiimeihin muodostuva mikro-organisaatiokulttuuri.

"Mä en oo ite havainnu siinä mitään säännönmukaisuutta. Yhtä hyvin voi olla täällä pääkonttorilla joku tiimi, vaikka markkistiimi, tai asiakkaan luona oleva tiimi. Se voi olla

iso tai pieni. En oo huomannu mitään säännönmukaisuutta. Jossain menee hyvin ja jossain ei mene niin hyvin." (TUK 3)

Siinä toimintatavassa, että tiimi vastaa itse niin projektissa ilmenneiden kuin tiimin henkilöstön välisestä ongelmien ratkaisemisesta, nähtiin myöskin etuja. Tiimin yhteinen, jakamaton vastuu ja velvollisuus ratkaista ongelmat sisäisesti kehittävät tiimien kiinteyttä ja parantavat niiden toimintaa. Tukea erilaisten käytännön ongelmien ratkaisemiseksi, osaamisen lisäämiseksi tai vastauksia avoimeksi jääviin kysymyksiin tiimi voi hakea organisaation sosiaalisten verkostojen tai virtuaalisten työtilojen kautta.

"Se on tosi kasvattavaa, et ne tiimit ite hoitaa niitä asioita, kun esimies puuttuu. Et niitä sitä ei vaan voi lakasta jollekin toiselle, tehtäväks. Ja koska sekään ei tunnu kovin hyvältä, et se esimies tulee sieltä et "anteeks". Et tavallaan niin vaikee, kun se onkin sanoo kasvotusten niin mun mielestä se on tosi opettavaista. Ja kyllähän kun meillä on intohimoist jengii, niin konflikteja tulee." (KON 4)

Myös tietoturvaa ja kyberturvallisuutta koskevat päätökset ja ratkaisut kuuluvat tiimien ratkaisuvaltaan. Tietoturva ja kyberturvallisuus huomioidaan osana tiimin jokapäiväistä toimintaa ja tiimi pitää huolen henkilöstönsä turvallisista toimintatavoista ja -ratkaisuista. Mikäli tiimi näkee päätöksen olevan laajempi, se voidaan viedä johtoryhmälle päätettäväksi.

Asiakastiimit huomioivat työsään projektikohtaiset vaatimukset, jotka vaihtelevat asiakkaan mukaan ja keskustellaan asiakkaan kanssa. Tekniseen tietoturvaan ja fyysiseen turvallisuuteen keskittyvät erilliset tiimit, jotka huolehtivat myös pääkonttorin turvallisuudesta, järjestävät koulutuksia ja tiedottavat.

"Niin silloin se on niinku hyvin selkeesti just niinku siellä tiimillä. Eikä siihen niin kuin ole, hyvin vähän meillä on mitään sellasta mekanismia, jolla niinkuin olis joku meidän oma tämmönen tietoturvapoliisi tai auditoija, joka niinku kulkis kyselemäsä jonkun tällasen, vaikka jos [yritykselle] tehtäis hommia niin mites ootte hoitanut tähän [palveluun] kirjatuvan ihmisen tietoturvan. Vaan kyl se on niinku sillei, että de facto luotetaan siihen niin kuin kaikissa muissakin hommissa luotetaan työntekijöiden arvostelukykyyn ja vastuunkantoon." (KON 2)

4.4 Organisaation rakenteet

Reaktor on matalan hierarkian organisaatio eli niin kutsuttu flat-organisaatio. Matalan hierarkian organisaatio ei tarkoita täydellistä rakenteettomuutta, vaan muodollisten rakenteiden vähäisyyttä verrattuna perinteisiin hierarkkisiin organisaatioihin. Organisaatiossa ei jokaiselle ole suoranaisia esimiehiä, selkeää tiimien välistä hierarkiaa sekä eri osien sijoittumista organisaatiokaavioon.

Tiimeillä ei ole nimettyä johtajaa, vaan tiimit organisoituvat itse osaamisen ja kiinnostuksen mukaan.

Useissa ilmaisuissa korostettiin näkymättömien rakenteiden merkitystä, koska muodollisia rakenteita on vähemmän. Näkymättömät rakenteet ovat ilmausten perusteella epämuodollisia toimintatapoja ja käytänteitä, joiden merkitys korostuu muodollisten rakenteiden puuttumisen myötä. Rakenteita oli enemmän organisaation toiminnan ja osa-alueiden, esimerkiksi asiakkuuksien, asiakastiimien kokoamisen tai tieto- ja viestintätekniikan hoitamisessa ja johtamisessa. Osa ”säännöistä” mainittiin olevan niin itsestään selviä, että työntekijöiden luotetaan ymmärtävän noudattaa niitä ilman niiden selittämistä. Päätöksenteossa sovellettiin tiettyjä tapauskohtaisesti sovellettavia reunaehtoja.

”Meillä ne näkymättömät rakenteet on, mä koen et ne on, vahvemmat kun monessa muussa paikassa. Ja mä luulen, et se menee niin, et kun ei ole niin muodollisia rakenteita niin paljon, niit on jonkin verran mut ei merkittävissä määrin, se johtaa ehkä siihen, että tota ne epämuodolliset rakenteet on ehkä vahvempia kuin jossain muualla.” (TUK 3)

”Mut nyt kun tota firma on kasvanut sekä määrällisesti että laadullisesti että maantieteellisesti, niin sit ollaan myös havahduttu siihen, että kun ei ole virallisia, kaikille näkyviä rakenteita niin sitten tota mitä isommaks kuviot menee, sitä isommaks sit tulee sellaset näkymättömät rakenteet.” (KON 2)

Esille tuotu rakenteettomuus ei kuitenkaan tarkoita sitä, että organisaatio toimii täysin organisoimattomasti tai vapaasti. Muodolliset ja staattiset rakenteet laajasti puuttuvat, mutta yhteisiä pelisääntöjä ja toimintatapoja on luotu tiimien ja organisaation sisälle. Suuriman osan työstä nähtiin tapahtuvan muodollisten rakenteiden ulkopuolella.

”On näitä paljon näitä tämmösiä säännöllisiä, ei tää mikään semmonen. Tää ei oo mitään hippeilyä, sen vois sanoo sillä tavalla.” (KON 1)

Kertoessaan organisaationsa kulttuurista ja toimintatavoista haastateltavat toivat esille eroavaisuuksia työskentelyssä matalan hierarkian organisaatiossa verrattuna perinteisiin hierarkkisiin tai esimiesjohtoisiin organisaatioihin. Kaikki haastateltavat olivat tyytyväisiä niin työtehtäviinsä kuin työskentelyynsä Reaktorilla. Matala hierarkia haastateltavien mukaan ole kuitenkaan täysin ongelmaton, vaan ongelmien luonne on erilainen.

”Tosi monet, jotka meil on töissä, niin nimenomaan tykkää siitä, että on matala ja olematon hierarkia. Sit joittenkin lieveilmiöiden kanssa sit vaan, ne on sit ehkä kivempia ongelmia ratkoa kuin mitkä vois tulla siitä hierarkiasta.” (KON 2)

Monella haastateltavalla oli mielikuva hierarkkisten organisaatioiden vallankäyttömallin tuomista ongelmista. He osasivat arvostaa niiden puuttumista matalan hierarkian organisaatiomallista.

”Aina kun on hierarkiaa, niin voi olla valtataisteluita. Ne puuttuu meiltä, kun ollaan flätti organisaatio.” (TUK 2)

Organisaation liiketoiminnan kannalta keskeiset konsultti- tai kehitystiimit toimivat pääasiassa työn alla olevan projektin asiakkaan tiloissa. Projektien sisältö ja luonne ohjaavat yksittäisen työntekijän tai tiimin näkemyksiä, koska näkymä organisaation toimintaan on erilainen ja tiimit toimivat eri tavoin.

”Jossain tiimeissä on jotku omat, on niinku tuolla asiakastiimeissä on varmasti omia juttujaan riippuen paljon siitä asiakkaasta. Asiakkaan tilat aiheuttaa aina tietynlaisia rajoituksia ja tietynlaisia juttuja. Mut sit kuitenkin ne pääperiaatteet, että käytetään samanlaisia metodeja, niinku Kanbania, tai niinku proaktiivista asennetta yritetään pitää niinku samana.” (KEH 2)

Useat haastateltavat kertoivat organisaatiorakenteiden puuttumisesta, mutta toivat esille työn organisointia koskevia toimintamalleja ja menetelmiä. Näiden yhteydessä useasti ilmaistiin, että ne ovat tavallaan rakenteita, mutta rakenteiden luominen ja ylläpitäminen on enemmän tiimin valinta.

”Mut on meillä enemmän rakenteita, meil on niinku semmosia patterneja. Esimerkiks meidän tiimit niin, siel on, nää on ihan sellasia rakenteita tai prosesseja, mitkä ei oo pakollisia. Tiimit voi ottaa ne halutessaan käyttöön, ja tiimit usein ottaa ne käyttöön, kun ne haluu tehdä hyvää jälkeä.” (KEH 1)

Matalan hierarkian organisaation ongelmana nähtiin toisaalta hierarkkisen organisaation luonnollisten rakenteiden puute, mikä korostui ongelmatilanteissa. Esimerkkeinä mainittiin tiimien ajautuminen tilanteeseen, jossa ongelma ei koske yksittäistä henkilöä vaan koko tiimin toimintaa. Ei ole selkeää rakennetta tai henkilöä, jonka tehtävä on edellä mainitussa tilanteessa ratkaista ongelmatilanne.

Organisaation kasvu ja sen myötä ilmenneet muutokset tulivat esille useissa ilmauksissa. Organisaation kasvaessa on tunnistettu tarve kehittää johtamisrakenteita ja tukitehtäviä. Organisaatio on myös sopeutunut muutokseen. Strategian ja organisaation suuntaviivojen miettimiseen on perustettu työryhmiä. Organisaatiossa on tunnistettu, että laajemman organisaation toiminnan takaamiseksi täytyy olla tiettyjä uusia rakenteita, jotka kuitenkin luodaan yritykselle ominaisiksi. Strategiatyöhön osallistuu ”rivihenkilöitä” muun muassa halukkuuden perusteella.

”Kyl täs on niinku selvästi systemaattisempaa ja ammattimaisempaa johtamista meille kasvanut ja rakenteitakin siihen jonkun verran.” (KON 2)

Yksittäisissä ilmauksissa esiintyi pelkoa organisaation kasvamisesta ja rakenteettomuuden vähenemisestä. Organisaation ja toimintojen muuttamisen ja sitä kautta hierarkian lisääntymisen nähtiin olevan väistämätöntä kasvamisen mukana.

4.5 Organisaatiokulttuuri

Haastateltavien organisaatiokulttuuriin liittyvät käsitykset sekä kokemukset olivat hyvin yhteneviä ja toisiaan tukevia, mikä ilmaisee organisaatiokulttuurin vahvuutta. Haastateltavien ilmausten sisällössä vaihtelua toi heidän työskentelynsä organisaation eri osissa ja työtehtävissä, mikä painotti tiettyjä organisaatiokulttuurin elementtejä ja toiminnan osa-alueita. Yksittäiset haastateltavat mainitsivat lähiympäristön vaikutuksen yksilön ajatteluun ja kokonaisuutta koskevaan näkymään.

"Jokainen on oman lähiympäristönsä vanki." (KEH 1)

Organisaatiokulttuuria koskeviin näkemyksiin vaikutti myös työskentelyhistorian pituus. Osa pidempään organisaatiossa työskennelleistä avata paremmin sen taustalla olevaa filosofiaa ja organisaation historiaa. Osa haastateltavista oli ollut mukana luomassa ja kehittämässä sitä alusta asti.

Haastatteluissa tuli useasti esille, että organisaatiolla ja sen työntekijöillä on jaettuja arvoja, joita ei kuitenkaan ole kirjoitettu mihinkään. Arvojen vahvuudesta tai niiden esiintymisestä läpi organisaation oli eroavia käsityksiä.

"Kyllä joo, kyl mä näen, en mä oikein osaa sanoa miten vahvat ne arvot on, mut kyl meillä on sellanen tietynlainen arvopohja." (KEH 2)

Organisaation arvot koettiin samankaltaisiksi kuin yksilöiden henkilökohtaiset arvot. Rekrytoinnin yhteydessä kerrottiin kiinnittävän huomiota uuden työntekijän sopivuuteen organisaatiokulttuuriin, mikä todennäköisesti vaikuttaa arvoiltaan samankaltaisten henkilöiden valintaan.

"Reaktorin arvot on hyvin paljon samat kuin mitkä mulla on mun henkilökohtaiset arvot." (TUK 3)

Organisaation ja työntekijöiden jakamista yksittäisistä arvoista esiintyi vaihtelevia käsityksiä. Arvoja yhtenäisempi oli jaettu asenne toisia ihmisiä ja organisaation etua kohtaan. Tämän asenteen koettiin esiintyvän läpi koko organisaation.

"Lähtökohtasesti kaikki ihmiset kohtaa toisensa niinku positiivisesti ja avoimesti sillä ajatuksella, että toi toinen ihminen on niinku hyvä, toi toinen ihminen haluaa hyvää mulle, toi toinen ihminen haluaa hyvää tälle firmalle. Toi toinen ihminen ei niinku osaoptimoi, hän ei niin kuin toiminnassaan pyri edistämään vain jotain omaa niinku lähtökohtaansa, vaan hän näkee tämän yhteisen hyvän. Ja mä oon ton, toi on niin kuin mielenkiintonen, koska ton saman asenteen mä oon huomannu huolimatta onko toi toinen ihminen, vaikka koodaaja, tai visuaalinen suunnittelija, tai jossain tukitoimessa, tai onko hän vaikka meidän hallituksen jäsen." (TUK 3)

Tietynlaisen mentaliteetin nähtiin yhdistävän organisaation työntekijöitä. Mentaliteetti tiivistettiin useissa ilmauksissa kykyyn odottaa toisilta lähtökohtaisesti hyviä aikomuksia ja miettiä toisten toiminnan syitä positiivisten odotusten kautta. Tähän mentaliteettiin kuuluu myös toisten henkilöiden auttaminen suoraan osallistumalla tai ohjaamalla heidät eteenpäin.

"Vaikea kuvitella, että Reaktorilla olisi töissä ihmisiä, jotka eivät allekirjoita suopeuden periaatetta." (KON 2)

Yhteiset tavoitteet luovat yhteisöllisyyttä ja sitoutumista

Haastateltavat ilmaisivat kokevansa yhteisöllisyyttä monella eri tasolla: tiimeissä, fyysisesti samassa paikassa työskentelevien kesken ja kaikkien organisaatiossa työskentelevien. Yhteisöllisyyden nähtiin lisäävän sitoutumista organisaation tavoitteiden edistämiseen ja toiminnan kehittämiseen. Yritys koettiin yhteisöksi, joka huolehtii yksilöstä niin hyvässä ja pahassakin.

Organisaatiolla koettiin olevan yhteisiä tavoitteita, jotka eivät kuitenkaan olleet yksinkertaisia tai helposti selitettävissä. Tavoitteet koskettivat useita toiminnan eri osa-alueita ja olivat enemmän filosofisia kuin konkreettisia. Tavoitteita on eri tasolla, eivätkä konkreettisemman tason tavoitteet ole pysyviä. Tavoitteiden asettaminen ja niistä puhuminen liitettiin onnistumiseen ja tavoitteiden saavuttamiseen.

"Yritetään päästä siihen johonkin yhteiseen maaliin, joka on ehkä vähän hähmäinen." (TUK 2)

"Pyritään luottamukseen ja hyvään, niin silloin yleensä siinä tapahtuu hyviä asioita." (TUK 2)

Muutama haastateltava toi esille erot työntekijän kohtelussa ja organisaation arvoissa Reaktorin ja perinteisiä organisaatiomalleja noudattavien yritysten välillä. Suuryrityksiin, joihin viitattiin korporaatioina, nähtiin yksittäisen työntekijän aseman ja mahdollisuuden vaikuttaa häneen itseensä tai työtehtäviinsä huonommaksi. Korporaatioiden toiminta nähtiin joustamattomammaksi kuin Reaktorin.

"Ja täällähän ihmiset vihaa niinku prosessisanaa, koska niillä on korporaatiotrauma. Joku puhuu tavoitteista tai budjeteista tai prosesseista, niin jengille tulee näppyjä, koska ne on nähny ne huonot puolet." (KON 1)

Organisaation toteuttama huolenpito nähtiin kokonaisvaltaisena ja useat ilmaukset koskivat erilaisia toimintoja, jotka tukivat työntekijän jaksamista, työvälineitä tai työtehtävien hoitamista. Henkilöstöhallinnon rooli on asioiden hoitamista laajempi kattaen henkilöstön hyvinvoinnista huolehtimisen.

"Hyvin monia, hyvin useita. On niinku kollegat, ihmiset eli koko yhteisö, on erilaisia tukitoimintoja: on ATK-apua, on henkilöpuolen apua, kaikkee löytyy." (TUK 2)

Henkilöstö tunnistettiin organisaation toiminnan kannalta keskeisenä tekijänä. Henkilöstöä ja sen osaamista nähtiin tarvittavan kaiken muun toiminnan mahdollistamiseen. Haastateltavien ilmauksista ilmeni kokemukset henkilöstön arvostuksen vaihtelevuudesta eri yrityksissä. Korporaatioita käytettiin huonona esimerkkinä tästä, koska korporaatioiden nähtiin keskittyvän henkilöstöstä huolenpitämisen sijaan vain rahan hankkimiseen.

Yksittäinen haastateltava kertoi saaneensa organisaatiolta tukea henkilökohtaisiin asioihin liittyvässä ongelmassa. Hän oli kokenut, että organisaatio oli tilanteessa valmis tarjoamaan hänelle kaikkea mahdollista tukea.

"Meil on tiloja, meil on laitteita. Kaikki kumminkin vaatii aina sen ihmisen, että jotain tapahtuu." (TUK 2)

Huolenpitoa toisista ja sitä kautta organisaation toiminnasta tapahtuu kaikkien työntekijöiden kesken matalalla kynnyksellä. Se nähtiin olevan olennainen osa organisaatiokulttuuria.

"Jokainen on niinku niin sanotusti veljensä vartija ja jokainen pitää huolen toisistaan. Ja siihen huolenpito kuuluu myös se, että jos huomataan jotain mikä ei oo menny putkeen tai mihin liittyy riskiä niin siitä huomautetaan. Ja sitä tapahtuu niinku hyvin matalalla kynnyksellä eikä siitä kukaan ota nokkiinsa." (KON 1)

Osaamista kehitetään jatkuvasti, ja epäonnistuakin saa

Oppimiseen ja osaamisen kehittämiseen kannustettiin. Luottamukseen perustuvassa organisaatiokulttuurissa yksittäisen ihmisen harkintakykyyn luotettiin, että hän hankkii itselleen tarvittavaa osaamista toiminnan kehittämiseksi. Epävarmoissa tilanteissa koulutuksen hankkimisesta tai tarpeellisuudesta voi kysyä työkavereilta. Yksittäiset osaavat tai asioista kiinnostuneet työntekijät järjestivät koulutusta sisäisesti tai hankkivat kouluttajia muualta verkostojaan hyödyntäen.

"Jos haluaa oppia, niin tämä organisaatio on kuin taivas." (KON 1)

Haastateltavien ilmaisuissa tuli esille, että onnistumiseen vaaditaan uusien asioiden kokeilemista. Organisaation työntekijöitä yhdistää uteliaisuus ja halu kehittyä. Tietoa ja osaamista jaetaan ja levitetään muun muassa sillä, että paras osaaja ei aina suorita tai vastaa osaamisalueeseensa sisältyvistä tehtävistä vaan opastaa toista työntekijää tehtävän suorittamisessa.

Epäonnistumista pyritään luonnollisesti välttämään, mutta se nähdään joskus onnistumisen edellytyksenä ja luonnollisena osana oppimisprosessia. Onnistumisen todennäköisyyttä nostetaan organisaatiossa olevan osaamisen ja verkostojen hyödyntämisenä, kysymällä neuvoa muilta ja hankkimalla tietoa myös muualta.

"Vahinkoi sattuu, sit korjataan niitä ja mennään eteenpäin." (TUK 2)

"Kyllä saa epäonnistuu, se on mun mielestä oppimisen reitti. Harvoin epäonnistumisesta ei jää niinku silleen mitään käteen. Niissä aina on jotain, jos sitä käydään läpi. Jos siihen niinku annetaan aikaan, puretaan tavalla tai toisella." (TUK 2)

Epäonnistumiseen nähtiin liittyvän avoimuus, koska se mahdollistaa muille työntekijöille tai tiimeille saman virheen välttämisen ja sitä kautta organisaation kehittymisen. Kynnys kertoa epäonnistumisesta vaihteli ilmauksissa työntekijän luonteen mukaan.

"Avoimuutta ja rehellisyyttä, että uskaltaa myöntää itselleen, että nyt tuli mokattua." (TUK 2)

Virheiden tunnustaminen ja niistä kertominen nähtiin toivottavana, mutta ilman että siihen ei ketään kuitenkaan pakoteta. Tämä johtuu työntekijöiden vaihtelevista käsityksistä epäonnistumisista, ja tarpeesta kertoa niistä muille vaihtelevat. Yksittäinen haastateltava näki epäonnistumisesta kertomisen luottamuksenosoituksena muita työntekijöitä kohtaan. Henkilökohtaisesta epäonnistumisesta kertomisen nähtiin laskevan kynnystä kertomiseen muille.

"Mä epäonnistun päivittäin jossain asioissa ja mä kerron niistä." (TUK 2)

Epäonnistumiset pyritään käymään aina läpi. Epäonnistumisessa nähtiin keskeisenä tapahtuman ja tilanteen läpikäyminen riittävällä tasolla tai tavalla, ilman että virheillä tai epäonnistumisilla kuitenkaan "mässäiltäisiin". Epäonnistumisessa tunnistettiin myös tarve ongelman ratkaisun lisäksi kohdata yksittäinen ihminen. Vaikka organisaatiolla on sääntöjä, ei niitä käytetä yksittäisen henkilön rankaisemiseen tai tuomitsemiseen, koska uskotaan hänen hyviin tarkoitusperiinsä.

"Meil puhutaan kyl kipeistä asioista ja mokista, asiat kyl käsitellään." (KON 4)

Päätöksenteko ja vastuun ottaminen kuuluvat kaikille

Päätöksentekovaltaa on Reaktorilla jaettu yksilöille ja tiimeille vastuiden mukaan. Yksilöitä kannustetaan ottamaan vastuuta ja tekemään päätöksiä heidän päätösvallassaan olevista asioista. Tavoitteena useiden ilmausten perusteella on välttää välikäsiä ja edistää organisaation toimintaa mahdollisimman nopeasti ja joustavasti, kun muodollista hyväksyntää ei tarvitse erikseen hakea vaan päätöksien perusteet tarkastellaan paikallisesti työtehtävän ja osaamisen perusteella.

"Ne ihmiset, jotka on lähimpänä käytännön työtä tietää työhön liittyvät asiat parhaiten. Heidän kannattaa päättää." (KON 2)

Organisaatiossa on olemassa tietyt päätöksentekoa koskevat yhteiset, osin kirjoittamattomat, säännöt, jotka takaavat sen, että päätöksiä syntyy ja kaikki

toimivat yhdessä sovitulla tavalla. Haastateltavien ilmaisuista ilmeni, etteivät kaikki osanneet selittää selkeästi päätöksentekoon vaikuttavia perusteita tai päätöksenteko ei ole täysin ongelmatonta vaihtelevissa tilanteissa. Mutta ilmauksista nousi esiin esimerkkejä yksilön tekemistä päätöksistä ja kyvystä tehdä niitä. Lähtökohtaisesti kukaan ei tee itse yhtään merkittävämpiä päätöksiä, mikäli niillä on yhtään vaikutusta muihin henkilöihin. Päätösten vaikuttavuus ja hankinnan arvo määrittelevät sitä, voiko tiimi tai yksilö tehdä päätöksen itsenäisesti vai täytyykö valtuutus päätöksentekoon hakea esimerkiksi asiakkaalta vastaavalta tiimiltä tai johtoryhmältä.

"Pakkohan siinä jotain rakennetta on olla, koska muuten siinä vain ovi käy eikä mitään saada päätettyä." (KEH 2)

Yksilön toteuttamassa päätöksenteossa hyödynnetään niin kutsuttua Advice-prosessia. Siinä työntekijä kysyy neuvoa vähintään kahden ulkopuolisen henkilön kanssa ja hakee tarpeeksi monelta mielipidettä ratkaistavaan ongelmaan tai päätöksentekotilanteeseen. Keskeistä prosessissa ei ole ainoastaan ulkopuolisen mielipiteen ilmaisu, vaan myös kriittinen tarkastelu.

"Ja sit meil on ihan formaali menetelmäkin siihen käyttöön kuin Advice-prosessi eli sellanen et sä voit kysyy parilta kolmelta ihmiseltä, tai useemmalta, jotka tietää siitä asiasta eniten. Jos haluut vaikka laittaa rokkikonsertin pystyyn, niin kannattaa kysyä useemmalta ihmiseltä advicea et mulla olis tällanen idea, mä haluisin tehdä tätä juttua, mä haluisin saavuttaa tätä. Jos sit sä haluut tehdä sen vimpan päälle, niin sit sä otat sinne jonkun paholaisen asianajajaksi eli yhdelle ihmiselle et se saa ampuu sen idean alas. Ja sit sä teet kuitenkin sen päätöksen itse." (KON 1)

Yksilöitä kannustetaan ottamaan vastuuta. Huolimatta päätöksentekoa edeltävästä keskustelusta sekä organisaation sisäisen osaamisen ja ulkoisten kontaktien hyödyntämisestä tekee vastaa yksilö tai tiimi päätöksen sisällöstä itse. Haastateltavat ilmaisivat myös arvostavansa päätöksentekoon liittyvää autonomiaa ja toiminnanvapautta. Sen nähtiin olevan kytköksissä yksilön arvostukseen, luottamukseen, itseohjautuvuuteen ja mahdollisuuteen kokeilla uusia asioita.

"Se kaunein juttu on se et mä teen just niin kun on mun mielestä järkevää." (KON 4)

"Yksilön arvostaminen, tiimityö ennen kaikkea muuta, edestä johtaminen, autonomia, erityisesti tiimien autonomia, vapaus tehdä, yrittää kokeilla, vapaus epäonnistua ja tehdä virheitä, oppia." (TUK 3)

Aloitteellisuutta tuetaan ja itseohjautuvuutta vaaditaan

Olennaisena osana Reaktorin kulttuuria on yksilöiden aloitteellisuuden tukeminen. Henkilöiden työtehtäviä tai vastuita ei ole määritelty liian tarkasti, vaan vastuut limittyvät ja malli antaa vapautta toimia päätösvaltansa puitteissa organisaation toiminnan edistämiseksi. Tiimin tehtävä ja organisaation tavoitteet

määrittelevät toiminnan suuntaan korkeammalla tasolla, mutta kokonaisuuteen tai organisaation toiminnan kehittämiseen liittyvät yksittäiset ratkaisut tulee kyetä tekemään itse. Organisaation, tiimin tai yksilön toimintamallien tarkastelu on säännöllistä, niin niitä voidaan muuttaa tarvittaessa paremman mallin tai perusteiden kautta.

"Reaktorilla ei aktiivisesti tueta mitään, mutta kukaan ei laita hanttiin." (KEH 1)

"Iso osa työstä tapahtuu ihmisten omasta halusta ja itseohjautuvuudesta." (KON 1)

Haastateltavien ilmauksissa organisaatio nähtiin itseohjautuvaksi ja sitä kautta toimivaksi, kun ihmiset edistävät organisaation toimintaa myös erikseen pyytämättä.

"Jos on joku asia, joka vaatii hoitoa niin mulla on sellainen käsitys, että aika moni täällä tarttuu siihen." (KEH 2)

Yksilöitä kannustetaan viemään asioita eteenpäin ja sitä kautta edistämään organisaation toimintaa. Moni asia lähtee yksilön kiinnostuksesta tai ideasta, jonka eteenpäin vieminen tapahtuu muiden yksilöiden tietotaitoa ja osaamista hyödyntämällä. Moni idea tai instituutio henkilöityy yksittäisiin henkilöihin, jotka niitä ovat luoneet ja ylläpitäneet.

"Ei ole pelkokulttuuria vaan mahdollistamisen kulttuuri." (TUK 2)

Osa haastateltavista näki haasteelliseksi yksittäisen työntekijän palautteen saamisen tekemistään valinnoista sekä toiminnastaan. Koskaan kukaan ei välttämättä ole suoraan kertonut mitä yksilön täytyy tehdä, niin palaute toiminnasta ja sen onnistumisesta tulee osata lukea verkostojen kautta ja edistämiensä asioiden kautta.

"Mä nyt sit tartuin asioin ja ilmeisesti riittävän moni niistä oli hyvä asia yhteisön ja tiimin mielestä." (TUK 3)

Itseohjautuvuuden ja päätöksenteon mukana mainittiin vastuu omista päätöksistä sekä tehtävän loppuunsaattamisesta. Haasteeksi nimettiin yksilön jääminen yksin vastuuseen ongelmatilanteissa ja toiminnan epäonnistuessa, kun hänellä ei ole hierarkkiseen organisaatiomalliin kuuluvaa esimiehen tukea ja vastuuta alaisen toiminnasta.

"Meil ei oo sitä, meilt puuttuu sellainen esimiehen selkänoja ja se johtaa välillä tilanteisiin, joissa yksilöt vilpittömästi pyrkii tekemään oikein ja hyvin juttuja, mut sit, kun ne menee pieleen niin ne jää yksin välillä melko rajunkin kritiikin alle." (TUK 3)

Opitaan ajattelemaan ja asiat tehdään tarkoituksenmukaisesti

Ajattelu ja ajattelemaan oppiminen tuli esille keskeisenä niin työntekijöitä ja sitä kautta koko organisaatiota koskevana ilmiönä. Tämä näkyi toiminnan perusteiden selvittämisenä, miettimisenä ja tarvittaessa kyseenalaistamisena. Maalaisjärjen käyttö tuli useasti esille haastateltavien ilmauksissa. Asiakasprojekteissa toimivien tiimien tehtävänä on edustaa organisaatiota ja sen toimintatapoja sekä viedä ajattelun taitoa eteenpäin.

"Reaktor, ambassadors of common sense" (TUK 1)

Käytettävyys on organisaation keskeinen arvo ja toiminnan tavoitteena on aina tuottaa jotain lisäarvoa organisaatiolle tai asiakkaalle. Käytettävyys painottui myös erilaisissa teknisissä ratkaisuissa, pyritään tekemään yksinkertaisia ja toimivia malleja.

Konteksti määrittää ratkaisut

Kontekstisidonnaisuus ohjaa organisaation toimintaa. Eri ratkaisujen ja käytäntöjen hyödyntämisen on vahvasti kontekstisidonnaista ja tapauskohtaista. Työkalujen valitseminen riippuu täysin tarpeesta. Käytäntöjä tai prosesseja ei oteta käyttöön sellaisenaan, vaan hyödynnetään soveltuvia osia tai muokataan malleja organisaation käyttöön soveltuviksi.

"En mä oo koskaan tehny Scrumia niin kuin by-the-book. […] Me otetaan niitä hyviä juttuja, Scrumista hyviä juttuja, Kanbanista hyviä juttuja, systeemiajattelusta hyviä juttuja." (KON 1)

Haastateltavat mainitsivat useasti asiakkaan tyytyväisyyden mittarina asiakasprojekteissa työskentelevien tiimien onnistumiselle.

"Mulle tärkeetä on siis tosi tärkeetä asiakkaalta tuleva palaute. Se on se mikä loppuviimeks kertoo, että tehdäänks me oikein ja hyvin ja teenks mä oikein ja hyvin." (KON 4)

Luottamus, avoimuus ja arvostus ovat organisaation toiminnan perusta

Luottamuksen merkitys organisaatiossa tuli esille jokaisen haastateltavan ilmauksissa. Niissä luottamus nostettiin yhdeksi keskeisimmäksi tekijäksi organisaatiossa, jonka varaan organisaation toiminta ja työntekijöiden välinen vuorovaikutus perustuvat. Osissa ilmauksista luottamus ja arvostus limittyivät. Luottamuksen nähtiin myös liittyvän avoimuuteen ja siihen, että ihmiseen luottamalla hän myös luottaa muihin ja uskaltaa kertoa myös epävarmoista asioista tai suoranaista virheistä.

"Ihmisiin luotetaan, luotetaan ja siihen uskotaan, että kaikki pyrkii toimimaan tämän organisaation etujen mukaisesti." (KEH 3)

Luottamuksen nähtiin lisäävän työntekijöiden halua yrittää, kokeilla uusia asioita ja toimia organisaatiokulttuurin mukaisesti. Se on perusta rohkeudelle kokeilla uusia asioita ja ideoita käytännössä. Luottamusta ei tarvitse erikseen ansaita, vaan se on perusolettamus ja lähtökohta. Luottamuksen mukana tulee odotus toimia tietyllä tasolla, osata ja ymmärtää perusasiat sekä käyttäytyä yleisesti hyväksytyllä tavalla.

"Uskon, että kun luotetaan heti alussa, niin ihmiset haluaa olla luottamuksen arvoisia." (TUK 2)

Vuorovaikutustaitojen kehittäminen

Vuorovaikutustaitojen merkitys organisaation, tiimien ja yksilöiden toiminnassa tuli useasti esille. Vuorovaikutustaidot linkittyvät kiinteästi henkilön sopeutumiseen organisaatioon, yhteishenkeen, yhdessä tekemiseen ja myös asiakkaalle organisaatiosta välittyvään mielikuvaan.

Reaktor järjestää työntekijöilleen tai maksaa heidän itse hankkimaansa vuorovaikutuskoulusta. Vuorovaikutus nähdään työntekijän työkaluna ja osaamisena, minkä hallitseminen vähentää esteitä itse ongelman ratkaisemiselta.

"Pitäis olla sellaiset työkalut millä voidaan keskittyä olennaiseen ja vuorovaikutuksessa se ei ole itsestään selvää." (TUK 1)

Vuorovaikutus nähtiin myös mahdollistavana tekijänä, joka edesauttaa ongelmien ratkaisua, uusien ajatusten syntymistä ja ideoiden jalostamista käytännön toiminnaksi.

"Mitä paremmin ihmiset kommunikoi keskenään, sen vähemmän ongelmia on tai sit tulee yhä hullumpia ongelmia." (TUK 2)

Organisaation kasvun ja asiakaslähtöisen toiminnan vuoksi suuri osa kommunikaatiosta ja tiedonjaosta mainittiin tapahtuvan tietoverkkojen yli. Kaikki työntekijät eivät tunne tai ole tavanneet toisiaan. Richard Lewis (2006) korostaa vuorovaikutustaitojen merkitystä virtuaaliympäristöissä, koska sanoilla ja kirjoitustyylillä on enemmän merkitystä.

Verkostot mahdollistavat toiminnan ilman muodollisia rakenteita

Yksilön ja tiimien ulkopuolinen rakenne, organisaation sisäiset ja myös sen ulkopuolelle ulottuvat, verkostot koettiin merkitseviksi ongelmien ratkaisemisessa ja toiminnan suuntaamisessa. Verkostojen avulla saadaan tietoa tai apua. Verkostot perustuvat henkilösuhteisiin tai tietoon toisen henkilön kiinnostuksesta ja osaamisesta. Maantieteellisesti hajautuneessa organisaatiossa verkostojen muotoutumisen ja toimivuuden mahdollistavat sisäisten keskustelukanavien kautta laajempi saavutettavuus, tiimien väliset vierailut sekä yhteiset tapahtumat työajalla ja sen jälkeen.

”Mä en tiedä, mutta mä tiedän kuka vois tietää.” (TUK 2)

Verkostoissa henkilö todistaa ja saa tunnustusta osaamisestaan, minkä kautta hänelle voi muodostua auktoriteetti vaikuttaa osaamisaluettaan koskevaan päätöksentekoon. Verkostojen kautta, osaamisen ja kiinnostuksen perusteella, muodostuu kuin epämuodollisia tiimejä, jotka kehittävät tiettyjä toiminnan osa-alueita.

”Totta kai, että jos jollain on joku juttu, joku hattu päässä niin sanotusti, ja se sanoo siitä hattuun liittyvästä asiasta niin kyllä jengi kuuntelee.” (KON 4)

Jokaisen työntekijän sosiaalinen verkosto on henkilökohtainen ja ainutlaatuinen. Verkoston luominen organisaation sisällä alkaa heti uuden työntekijän aloitettua organisaatiossa henkilökohtaisen perehdyttämisen ja sisäisten koulutusten kautta, jolloin tietyt käytäntöihin liittyvät asiat henkilöityvät ja saavat ”kasvot” perehdyttäjien muodossa. Verkostojen vahvat henkilöiden väliset sidokset sitovat tiimit ja ydinhenkilöt yhteen, mutta heikot sidokset ovat olennaisia tiedon ja uusien ideoiden jakamisessa.

Matias Saarinen (2018) havaitsi vastaavanlaisen organisaation sosiaalisen verkoston analyysissa, että organisaation toiminnan perustuminen tiimeihin tuo hyötyjä ja luo riskejä. Jotta tiimit pystyvät toimimaan tehokkaasti, täytyy ne suunnitella niin, että ne kykenevät toimimaan itsenäisesti. Työntekijäkohtaisen, vahvoja ja heikkoja sidoksia sisältävän, sosiaalisen verkoston luominen on keskeistä. Verkosto tasaa osaamista ja tietoa, mahdollistaa tiedon ja uusien ideoiden jakamisen sekä ulottuu myös organisaation ulkopuolelle. (Saarinen, 2018). Verkostoja voidaan hyödyntää myös Advice-prosessissa, jossa vastuussa oleva tai ongelmaa ratkaiseva henkilö kysyy muiden työntekijöiden mielipiteitä ja osallistaa heitä ongelman ratkaisuun. Verkostot mahdollistavat oikean osaamisen löytämisen organisaation sisällä tai kontaktin hankkimisen organisaation ulkopuolelta.

Noin puolet haastateltavista toivat esille auttamisen kulttuurin ja merkityksen matalan hierarkian organisaation toimivuudessa. Auttamisen kulttuurilla ilmauksissa tarkoitettiin toisen työntekijän tukemista tai ohjaamista eteenpäin, jos ei itse kyetä auttamaan. Huolimatta siitä, että vastuu on toisella työntekijällä, pyritään aina edistämään toimintaa jollain tavalla.

” [Se, että joku sanoo] Öö, en tiedä, on vain itsellä niinku, että ei näin. Aina ohjataan eteenpäin, aina autetaan.”

Rekrytointiin, perehdyttämiseen ja kulttuuriin sopeutumiseen panostetaan

Lähes jokaisessa haastattelussa tuli esille ilmauksia, joiden perusteella organisaatio on tunnistanut rekrytoinnin keskeiseksi prosessiksi organisaation toimivuuden kannalta. Rekrytointiin osallistuu henkilöstötiimin lisäksi asiantuntijoita ja mahdollisesti rekrytoitavan kanssa työskenteleviä, jotta rekrytointiprosessissa pystytään huomioimaan erilaiset näkökulmat. Henkilöstötiimin ulkopuolinen

henkilöstö osallistuu rekrytointiin kiinnostuksen ja osaamisen mukaan. Organisaatiossa on tunnistettu tärkeäksi rekrytointiin osallistuvia ja soveltuvia asiantuntijoita.

"Se on tavallaan sellasta metarekrytointia, että me rekrytoidaan rekrytoijia." (KEH 3)

Moni haastateltava kertoi rekrytoinnissa merkitsevän osaamisen lisäksi persoonan, vuorovaikutustaitojen ja tavan tehdä töitä. Kulttuuriin sopeutuminen nähtiin jopa tärkeimmäksi ominaisuudeksi rekrytoinnissa, mikä johtuu organisaatiokulttuurin luonteesta ja sen vaatimuksista yksilön toiminnalle. Yksittäisenä ilmauksena mainittiin vaikeus rekrytoida täysin tuntemattomia henkilöitä, joilla ei ole suosittelijaa organisaation sisältä, koska rekrytoinnissa ei välttämättä pystytä arvioimaan kattavasti sopeutumista organisaation toimintatapoihin ja kulttuuriin. Organisaatio ei kuitenkaan pyri rekrytoimaan ainoastaan saman mielisiä henkilöitä, vaan se pyrkii ottamaan rekrytoinnissa huomioon erilaisen ajattelun ja näkökulmien tarpeen sekä niin kutsutut "diversiteettikulmat".

"Tänne otetaan töihin persoonia, joiden kanssa ihmiset haluavat tehdä töitä." (KON 1)

Haastateltavien ilmauksista tuli esille, että rekrytoinnissa olennaista on tunnistaa henkilön soveltuvuus ainakin seuraaviin toimintoihin:

- pystyy omaksumaan organisaation näkymättömät rakenteet ja toimimaan niiden mukaisesti
- on halukas oppimaan jatkuvasti uutta ja kehittämään itseään sekä organisaatiota
- kykenee itsenäisesti tekemään päätöksiä ja ottamaan vastuuta
- omaa hyvät vuorovaikutustaidot
- pystyy toimimaan itseohjautuvasti yksin ja osana tiimiä

Uuden työntekijän perehdyttämisessä nähtiin runsaasti haasteita. Osalla haastateltavista oli henkilökohtaisia kokemuksia ja muistoja sopeutumisen vaikeudesta organisaatiokulttuurin poikkeuksellisuuden ja toimintavapauden määrän vuoksi. Organisaation toimintamallien omaksumisen lisäksi perehdyttämisen aikana saatavan tiedon määrä koettiin valtavaksi.

Uuden henkilön sopeutumisessa organisaation toimintamalleihin keskeiseksi nähtiin yksilön henkilökohtainen aktiivisuus ja halu omaksua asiat. Uskallus kysyä kysymyksiä ilmaistiin tärkeäksi ominaisuudeksi, mutta tunnistettiin että se voi helposti ilmetä liiallisena tai liian vähäisenä.

"Se vapauden määrä mikä heille on annettu tekemään päätöksiä ihan päivittäisellä tasolla, lyö heitä kuin tsunamiaalto. He eivät käsitä sitä. Ja mä oon huomannu sellasen, mun käsitys on se, että siinä on sellanen hetki aikaa, useampi kuukausi, ennen kun henkilö tajuaa kuinka paljon vapautta ja vastuuta hänelle on annettu. Et se tulee aina yllätyksenä. Alkuun on sellaista jähmettymistä. Joko ei kysytä tai uskalleta tai sit kysytään ihan liikaa koko ajan kaikkee." (TUK 1)

Perehdyttämisen haasteisiin vastatakseen organisaatiolla on perehdyttämistä varten olemassa kattavat ja hyväksi havaitut rakenteet. Uusi työntekijä ei jää missään vaiheessa ”tyhjän päälle”, vaan vastuu uudesta työntekijästä on alussa henkilöstötiimillä, joka käy perusasiat ja -toimintamallit läpi.

”Meidän HR ottaa uudesta tyypistä aina otteen ensimmäiseksi viikoksi ja esittelee paikat ja talon tavat.” (KEH 2)

Perusasioiden selvittämisen jälkeen on muutamasta päivästä noin viikkoon kestävä tilaisuus, jossa käydään läpi lisää työntekoon ja organisaatiossa toimimiseen liittyviä toimintamalleja ja tapoja. Perehdyttämisen kautta uudelle työntekijälle alkaa syntyä sosiaalinen verkosto, kun hän yhdistää tietyt nimet ja kasvot eri toimintoihin.

Jokaiselle uudelle työntekijälle nimetään mentori, joka ohjaa häntä työnteon yhteydessä ilmenevissä kysymyksissä toimintavoista tai organisaatiokulttuurista. Asiakastiimiin sijoittuva henkilö saa mentorinsa tiimistään ja koko tiimin mainittiin toimivan tavallaan uuden henkilön mentoreina. Tavoitteena on uuden henkilön kasvaminen organisaation kulttuuriin ja toimintatapoihin työnteon ja projektien kautta. Työntekijän tiimi jatkaa perehdyttämistä työn ohessa.

”Meil on onboardaus, käytännössä se on ihan tilaisuus ja strukturoitu sisäänajo-ohjelma. Meil on mentori, tai joka, no mentori tai kummiko se on nykyään, joka auttaa ihan käytännön työssä.” (KON 3)

4.6 Organisaation kyberturvallisuuskulttuuri

Asenne ja mentaliteetti

Haastateltavat näkivät organisaationsa kyberturvallisuuskulttuurin ja siihen liittyvät käytänteet pääasiassa toimivina. Organisaation tavoite on nostaa organisaation tietoturvan ja kyberturvallisuuden taso korkeammaksi kuin mitä asiakkaat vaativat.

Haastateltavien ilmauksista kuitenkin ilmeni, että heillä oli ristiriitaisia käsityksiä joistain organisaation kyberturvallisuuskulttuurin yksityiskohdista. Osa haastateltavista näki, että nykyinen tapa tehdä tietoturvaa perustuu olettamukseen jokaisen työntekijän korkeasta kyvystä ymmärtää riittävästi tekniikkaa. Täten jokainen ymmärtää myös tietoturvaa ja tietoverkkojen kautta kohdistuvia uhkia. Etenkin teknisesti koulutetut ja teknisissä tehtävissä toimivista näkivät organisaation työntekijät keskimääräistä valistuneempina kyberturvallisuus- ja tietoturva-asioissa. Silti he tunnistivat eri käyttäjien väliset erot asenteissa ja käytänteissä liittyen organisaation tietojen käsittelyyn sekä hallinnointiin. Kaikkien työntekijöiden nähtiin kuitenkin olevan tietynlaisella perustasolla tietotekniikan osaamisessa.

"Meillä ei ole töissä täysin tietokonelukutaidottomia persoonia." (KON 1)

Suurin osa haastateltavista ilmaisi tietävänsä organisaation tietoturvakäytännöt ja roolinsa tietoturvan toteuttamisessa. Tietoturva-asioiden ohjeistaminen tunnistettiin sisältyvän perehdytykseen. Moni haastateltava kuitenkin kertoi, ettei täysin ymmärrä kaikkien eri henkilöiden roolia tietoturva-asioissa tai mitä uhkia juuri hänen kauttaan voisi kohdistua yrityksen liiketoimintaan.

Osa haastateltavista ilmaisi, ettei heitä ole henkilökohtaisesti ohjeistettu tarkemmin tietoturva-asioista ja aihealuetta koskevat kirjalliset ohjeistukset eivät olleet riittäviä. Myös täysin vastakkaisia näkemyksiä ohjeistamisesta tuotiin esiin, vaikka kukaan ei maininnut, että tietoturvaan koskeva ohjeistus olisi koottu perinteisen tapaiseksi dokumentiksi tai dokumenttikokoelmaksi.

"Ainakaan mä en tiedä, että meillä olis joku sellainen tietoturvapolitiikka mitä mun pitäis noudattaa." (KON 4)

Tietoturvan ymmärrys ja tietouden ylläpito nähtiin jokaisen työntekijän velvollisuudeksi. Yksittäinen haastateltava vertasi sitä muuhun ammatilliseen kouluttautumiseen. Tällöin työntekijällä on velvollisuus selvittää asia sekä kehittää ja ylläpitää osaamistaan, mikäli hänellä ei ole kaikkea tarvittavaa tietoa. Tässäkin asiassa mainittiin, että koulutuksen hankkiminen ja osaamisen kehittäminen on organisaation puolesta mahdollista.

"Ehkä mä oon ite kokenu, et mul on niinku velvollisuus ottaa selvää." (KEH 1)

Yksittäinen haastateltava ilmaisi työntekijöiden välisten tietoturvaosaamisen ja -ymmärryksen erojen sidoksen tietotekniikan osaamiseen. Hän mainitsi, että uhkien muodostumisen ymmärtäminen ja uhkatietojen soveltaminen erilaisiin käytännön tilanteisiin vaatii taustalla olevaa tekniikan ymmärtämistä. Myös muissa vastauksissa tunnistettiin yksilöiden väliset erot, mutta arvioitiin osaamisen olevan kuitenkin muita samalla alalla toimivia yrityksiä korkeammalla. Organisaation työntekijät kompensoivat teknisen osaamisen puuttumista tai ymmärrystä uhkien muodostumisesta yleisellä valveutuneisuudella ja valppaudella: tiedostetaan, että uhkia on olemassa ja tiedetään mikä ei ole järjestelmän tai toisen ihmisen normaalia tieto- ja viestintätekniikkaan liittyvää käytöstä.

"Mut kun nää ihmiset ei oo niinku, niiden osaaminen on jossain muualla. Niille tietoturva on todella sitä, et ei saa käyttää samaa salasanaa eri paikkoihin. Niillä ei oo sitä taustaymmärrystä, niin ne on opetellu sen niinku "hauki on kala", niin ei saa käyttää samaa salasanaa muualla." (TUK 3)

Organisaatio tukee yksittäisiä käyttäjiä ohjeistamalla ja kouluttamalla tietyt perustoiminnot osana perehdyttämistä. Teknisten asetusten ja suojausten osalta on myös olemassa tietyt perustoimintamallit, joita on pakko noudattaa. Tietoturvakäytännöt on mietitty käyttäjän kannalta järkeviksi ja käytettäviksi. Henkilöstölle

on haluttu haastateltavien ilmausten perusteella antaa tietty toiminnanvapaus laitteiden käyttöön, ettei turvallisuus estä työntekoa. Toiminnanvapaudella on haluttu myös estää tilanteet, joissa henkilöstö alkaisi kiertämään liian jäykkiä tai rajoittavia suojauksia. Ylläpito- ja turvallisuushenkilöstö on tiedostanut, että organisaation henkilöstöllä on vaihtelevaa osaamista ja tapoja käyttää tieto- ja viestintätekniikkaa.

"On perusasioita tietoturvassa otettu huomioon. […] Mut kaikkee voi käydä kumminki. Tää on vaan ATK:ta. Ja joku aina keksii jotain. Ja välillä sit taas on se, että ihmiset välillä vähän luovii tai ei ehkä sit ihan ajattele." (TUK 2)

Esimieshierarkian puuttuessa keinot puuttua yksilön toimintaan ovat erilaiset kuin hierarkkisessa organisaatiossa. Yksilöä ei varsinaisesti rajoiteta, vaikka erilaisista ratkaisuista kysellään ja keskustellaan. Tietoturva ja kyberturvallisuus nähdään kuuluvan työntekijän vastuuseen, jota organisaatio tukee mahdollistamalla hyvien ja turvallisten ratkaisujen käytön sekä osaamisen kehittämisen. Tiimin jäsenet ja muut työntekijät auttavat vertaistarkistuksen muodossa, koska yksilön toiminta on osa tiimin toimintaa.

Huolimatta koulutuksesta ja työnantajan välineiden pakollisista teknisistä tai toiminnallisista suojauksista osa haastateltavista ilmaisi, että turvallisuusasioissa yksittäisen työntekijän toimintavapautta tulisi rajoittaa ja vastuun tulisi olla vahvemmin jollain muulla kuin käyttäjällä. Organisaation kulttuuriin kuuluvan vapauden nähtiin olevan selkeä uhka turvallisuudelle. Turvallisuusasioiden ymmärrys ja henkilökohtaisten käytänteet tulisi varmistaa paremmin. Turvallisuutta koskevia käytänteitä nähtiin tarpeen ohjeistaa tarkemmin, koska esille ei tuotu mitään muutakaan tapaa taata riittävän hyvien käytänteiden noudattaminen. Yksittäinen haastateltava ilmaisi, että tietoturvaohjeistukset eivät ole ymmärrettäviä ilman teknistä koulutusta.

"Vois jo unohtaa sen, että kaikki on koodaajia. Meistä tuli koodareita, kun se ei pidä paikkaansa. Mut sen mukaiset ohjeistukset kaipais, mut mä en oo ihan varma onko niillä sellasta tavallisen ihmisen kieltä, taas et osaisko ne kertoa meille näistä, muun muassa turvallisuusasioista ja miten koneita käytetään." (TUK 1)

Kaikki haastateltavat tiesivät kuitenkin keneen tai mihin tahoon ottaa yhteyttä, mikäli heillä on tietoturvaa tai laitteiden toimintaa koskevia kysymyksiä. Useita eri kanavia tuli esille uhkia tai tietoturvapoikkeamia koskevan tiedon saamiseksi. He näkivät organisaationsa työntekijöiden toiminnan aktiiviseksi tietoturvaa koskevissa kysymyksissä.

Haastateltavat näkivät tarvetta kehittää osan henkilöstön mentaliteettia kyberturvallisuutta koskevissa asioissa. Ilmausten perusteella osa henkilöstöstä näkee kyberturvallisuuden heikentävän käytettävyyttä ja monimutkaistavan käytettäviä ratkaisuja. Silti kyberturvallisuus ja tietoturva on otettava vakavasti heti projektien alusta alkaen. Kyberturvallisuuden ja tietoturvan ratkaisuja määrittää tarkoituksenmukaisuus eli ratkaisujen mitoittaminen uhkien mukaan. Turvallisten ratkaisujen ja käytettävyyden yhdistäminen nähtiin kuitenkin mahdolliseksi.

"Aina kun kyberturvallisuutta parantaa, niin aina käytettävyyden taso heikkenee tai haittaa jotain töiden tekemistä. Ja sitten tota meillä on aina ollut paino usein siellä, että tehdään hommat niin että ne toimii. Mut kyl mä uskon, että asioita voi useimmissa tapauksissa yhdistää nää asiat sillei järkevästi." (TUK 2)

Haastateltavien ilmauksissa korostettiin kyberturvallisuuden sisältymistä ammattimaiseen asenteeseen ja toimintaan. Sen vaatimisesta kukaan ammattilainen ei voi loukkaantua vaan ammattilaisen täytyy ymmärtää tarve turvallisuuden ylläpitämiselle ja tietojen jakamisen rajoittamiselle. Tasapaino käytettävyyden ja kyberturvallisuuden välillä nähtiin olevan kohdallaan, vaikka poikkeamia todennäköisesti on kumpaankin suuntaan.

"Tietoturvan kanssa tekemisissä oleva ihminen ei loukkaannu siitä, että tehdään tietoturvaa ja kysytään hänen oikeuttaan olla paikalla." (KON 3)

Organisaatiossa tunnustetaan ihmisten alttius tehdä virheitä myös turvallisuusasioissa, mikä on samalla hyvä ja huono lähtökohta. Silti turvallisuusasioissa virheiden tekeminen ei ole niin hyväksyttävää kuin muissa toiminnoissa, vaikka siitä toivotaan ilmoitettavan ja keskusteltavan yhtä avoimesti kuin muistakin epäkohdista. Virheiden tekemisen syy vaikuttaa myös tapaan suhtautua siihen, koska organisaatio tunnistaa eron inhimillisten ja täydestä huolimattomuudesta johtuvien virheiden välille. Virheiden tunnustaminen mahdollistaa niiden korjaamisen, organisaation toimintamallien tarkastelun ja tarvittaessa muuttamisen.

"Ja tärkeintä on se, et jos sit sattuu mokaan, niin pyritään ylläpitämään sellasta kulttuuria, että sit se moka kerrottais, jolloin siihen voidaan reagoida. Siihen voidaan varautua, se tapa voidaan muuttaa. Olkoon se mikä vaan." (TUK 2)

Haastateltavat tiedostivat, että täydellistä tietoturvaa tai kyberturvallisuutta ei voi saavuttaa, mutta sitä kohti täytyy pyrkiä ja taso on pyrittävä pitämään mahdollisimman korkealla. Mentaliteetti turvallisuusasioita koskevan osaamisen kehittämisessä on vastaava kuin organisaation kaiken toiminnan kehittämisessä: tiimit ja yksilöt huolehtivat toisistaan ja toiselle henkilölle huomauttaminen nähtiin luottamuksenosoituksena.

Tavoitteena on ehkäistä ja ratkaista ongelmatilanteet sisäisesti ennen kuin ne näkyvät ulospäin. Organisaation linja on myöntää selkeät virheet asiakkaalle, vaikka tilanne kyettäisiinkin itse ratkaisemaan mutta asialla on merkittävää vaikutusta asiakkaaseen. Organisaatio nähtiin avoimena myös asiakkaan suuntaan ja haastateltavat esittivät tästä käytännön esimerkkejä.

"Se on helpompi saada ne hommat kiinni ajoissa, kun että jonkun ulkopuolisen, se menee niin pahaks, että joku ulkopuolinen taho tajuaa sen. Se on vaan aikasemmin otettu kiinni ja toimintatavat pysyy mintissä." (KON 1)

Osalla haastateltavista ei ollut vahvaa mielipidettä organisaation kyberturvallisuuden tasosta tai sitä ylläpitävistä käytänteistä. Nämä haastateltavat kokivat pystyvät luottamaan siihen, että tiimin muut jäsenet ottavat enemmän vastuuta asiasta. He kertoivat saavansa tarvittaessa tietoa ja opastusta muilta, asiasta enemmän kiinnostuneilta ja ymmärtäviltä, viimeistään kysymällä. Joka tapauksessa yksittäisen käyttäjän velvollisuutena nähtiin perustoimintojen hallitseminen ja epänormaalien asioiden havainnointi, minkä perusteella käyttäjä voi kysyä muilta tai viedä asioita eteenpäin organisaation turvallisuutta koskevien käytänteiden kehittämiseksi.

"Mä uskon et kysymällä mä saisin sen mitä tarviin. En nää, että mun tarvii olla tässä asiassa aallon harjalla." (KON 4)

Organisaation kasvun ja muutoksen on tunnistettu tuovan uusia uhkia organisaatiota ja sen liiketoimintaa kohtaan sekä vaativan turvallisuusasioiden tarkastelua. Muutostarpeiden tunnistaminen on vaikuttanut jo turvallisuusratkaisujen tarkentamiseen esimerkiksi fyysisen turvallisuuden puolella. Henkilöstömäärän kasvattaminen ja toimintojen lisääntyminen ei enää mahdollista kaikkien työntekijöiden tuntemista. Yksittäinen haastateltava ilmaisi, että organisaatio ei ole vielä riittävällä tasolla sisäistänyt sitä kohtaan kohdistuvia uhkia ja niiden realisoitumista, minkä vuoksi uhkalta suojautumisen toimenpiteet eivät ole vielä olleet riittäviä.

Tietoisuus uhkista ja osaamisen kehittäminen

Kyberturvallisuutta koskevaa koulutusta järjestetään sekä sisäisesti että ulkoisesti. Organisaation sisällä koulutuksia järjestävät asiasta kiinnostuneista yksilöistä koostuva joukko, "community of interest", ja turvallisuudesta vastaavat henkilöt. Edellä mainitut tahot ovat aloitteellisia tunnistaessaan tarpeen koulutuksille. Osa koulutuksista järjestetään ensin tietoturvasta enemmän kiinnostuneille, jonka jälkeen on laajennettu osallistujien määrää ja kirjoa. Sisäisten kulutusten sisältö, toteutustapa ja aihe vaihtelivat tunnistetun tarpeen mukaan.

"Meil oli myös sellainen firman tota tietoturvakoulutus tai varmaan niitä edelleen järjestetään, jossa mä olin niinku muutama vuosi sitten. Siellä ei ollu niinku uhkatyyppien tai sellasten suhteen en muista, että ois hirveesti tullu varsinaisesti uutta asiaa. Mutta se oli sillein tosi hyvä, kun siellä oli sellasii harjotuksii missä piti niinku tota miettiä tavallaan ihan ajatuksen kanssa, ja eri tyyppien kanssa kenen kanssa niinkun tulee päivittäin tehtyä töitä, tietoturvan näkökulmasta asioita." (KON 2)

Sisäiset koulutukset ovat myös sivunneet tietoturvaa, vaikka koulutus ei suoraan ole keskittynyt siihen. Organisaation sisäisesti järjestämien koulutusten lisäksi yksittäinen tiimi voi myös hankkia lisää osaamista tai konsultaatiota organisaation sisältä tai ulkopuolelta tunnistaessaan sille tarpeen. Tietoturvaan liittyvää koulutusta hankittiin myös organisaation ulkopuolelta, mikä nähtiin tarpeelliseksi, jotta toiminta voi kehittyä ja saadaan uutta osaamista.

"Kyl me niinku, me ei voida nostaa omaa tasoo, jos me ei hommata ulkoo." (KON 1)

"Ostetaan palveluita, on ostettu sellasia kursseja mis oon ollu. Tiedän itsekin, oon sellasia käyny. Sisäisiä koulutuksia on kaikennäköisiä niinkun liittyen moneenkin aspektiin. Mietin onks meillä ihan puhdasta tietoturvaa esimerkiksi, jotain tollasta koulutusta, sisäisesti. On niitäkin kyl varmasti ollu. En pysty kyl varmaks sanomaan. On ulkosia, tiedän, oon itekin käyny esimerkiks koulutuksissa. Ostettu ihan selkeesti tietoturvaan, tietosuojaan siihen liittyvää ihan konkreettista taitoo, rakennettu." (KON 3)

Suuri osa haastateltavista kertoi osallistuneensa organisaation sisäisiin koulutuksiin. Kaikki eivät kuitenkaan olleet varmoja kuka oli vastannut koulutuksen järjestämisestä. Osa haastateltavista oli kuullut koulutusten järjestämisestä, mutta ei ollut osallistunut niihin. Useassa ilmauksessa tuli esiin positiivinen suhtautuminen koulutukseen ja sen yhdistyminen tietoturvan tason ylläpitämiseen. Suurin osa ilmaisi halukkuutensa osallistua uusiin kyberturvallisuutta koskevaan koulutuksiin, joka voi koskea niin henkilökohtaisten tietojen suojaamista kuin työssä eteen tulevia tilanteita.

"Mut kyl mä voisin, mä oon aika hyvin perillä, mut mä voisin ottaa kuitenkin jonkun koulutuksen. " (KEH 2)

Itseohjautuvuuteen perustuvaa osaamisen kehittäminen mainittiin keinona organisaation ja yksilöiden tietouden lisäämiseksi. Yksilöt hankkivat tietoa ja jakoivat sen organisaatiossa, mikäli tunnistivat sen hyväksi ja tarpeelliseksi myös muille.

"Osta kirja, se maksaa ehkä kakskymppiä. Jos sait idean, se makso itsensä takaisin. Jaa se idea, se maksoi ittensä takaisin moninkertaisesti." (TUK 2)

Keskustelu turvallisuudesta ja tietoturvapoikkeamien käsittely

Organisaation tapa turvallisuutta koskevassa keskustelemisessa ja epäkohtien ilmoittamisessa noudattaa vastaavaa toimintamallia kuin muistakin asioista keskusteltaessa. Turvallisuuskulttuuri on avoin, vaikka siihen liittyviä ratkaisuja ja järjestelyjä suojataan enemmän kuin muuhun toimintaan liittyvää tietoa. Tiedonjaon rajoittaminen turvallisuusasioista nähtiin ristiriitaisesti: osa henkilöistä ilmaisi ymmärtävänsä tarpeen rajata tiedonjakoa, mutta sen tunnistettiin myös vaikuttavan käytäntöjen kehittämiseen ja työntekijöiden tietoisuuden tasoon.

"Mitä vapaammin niistä pystyy puhumaan, sen paremmin niitä pystyy edistämään." (KEH 3)

Organisaation sisällä jaetaan tietoa havaituista epäkohdista. Havaitut epäkohdat selvitetään, niistä keskustellaan ja tarvittaessa tieto jaetaan eteenpäin. Jokainen

tapaus käsitellään erikseen. Päätökset tehdään vakavuuden sekä laajuuden mukaan.

"Se on pakko reagoida sen mukaan mitä tapahtuu: jos se on phishing-mailia, jos se on niinku palvelu murretaan, jos meidän verkot murretaan. Se riippuu ihan tapauksesta: miten laajasti se vaikuttaa, miten siitä tiedotetaan, kenelle tiedotetaan, minkälaisia raportteja niinku tehdään." (TUK 2)

Vastaavasti avoimesti toimitaan myös ajoissa havaittujen tietoturvapoikkeamien suhteen: analysoidaan mitä tapahtui, mistä se johtui ja mitä olisi voinut tapahtua. Tavoitteena on tiedon jakaminen, jotta vastaava ongelma voidaan välttää tulevaisuudessa ja kehittää rakennettavia ratkaisuja. Tietoa jaetaan myös kollegoiden kesken. Tiedonjako ei vaadi tietoturvapoikkeamaa tai epäkohtaa, vaan sitä vaihdetaan erilaisista ratkaisuista ja niiden toimivuudesta.

"Jos on ollu tälläsiä, et ongelma jossain, [tietoa] välitetään kyllä. On ollut ihan sellasia, et hei täs on ollu tällanen asia, toteutumiskerroin tämä, johtui tästä, korjattiin näin ja nyt tää on kunnossa. Ja nyt tän tyyppisiä on ollut. Mitään ei oo tietääkseni mitään eli kyllä näistä on avoimesti kerrottu. Meillä ei ole salaamisen kulttuuria tämän suhteen." (KON 3)

Haastateltavat näkivät keskeisenä aktiivisuuden tiedonjakamisessa. Vaikka poikkeaman tai epäilyttävän havainnon tehnyt henkilö ei ehtisi, osaisi tai pystyisi tekemään asialle mitään, tiedon jakaminen ja muilta kysyminen on joka tapauksessa tehtävä.

Uhkatietojen ja haavoittuvuuksien jakaminen

Tietoturvauhkat ovat ilmausten perusteella organisaatiossa jatkuvasti esillä oleva aihe. Tietoturvan ja kyberturvallisuuden ylläpito nähtiin monella tavalla kaikkien työntekijöiden tehtäväksi. Käytännössä se tuli esiin esimerkiksi uusia uhkia ja haavoittuvuuksia koskevien tietojen hankkimisena ja jakamisena organisaation muille jäsenille. Vähemmän vakavista uhkista ja erilaisista ilmiöistä keskustellaan keskusteluryhmissä. Osalle henkilöstöstä haavoittuvuus- ja tietoturvatietojen seuraaminen ja jakaminen nähtiin kuuluvaksi työtehtäviin. Osa niiden jakamiseen osallistuvista on kiinnostunut aihealueesta ja seuraa tietoturvaalan kehitystä.

Useampi haastateltava mainitsi vastaanottaneensa haavoittuvuustietoa tai toimintaohjeita sisäisten tiedonvälityskanavien kautta. Juuri tietyllä hetkellä pinnalla olevista asioista tai ilmiöistä, esimerkiksi tietynlaisista kalastelusähköposteista, tiedotetaan suoraan koko organisaatiota. Tarve tiedottaa tarkastellaan kuitenkin aina erikseen ja sen hoitavat lähtökohtaisesti järjestelmien ylläpitoon ja suojaamiseen keskittyvät tiimit.

”Muistaakseni viime viikolla [henkilö] teki tiedotuksen. Hei, tuo palvelu, mitä devaajat käyttää, on murrettu ja sen palvelun salasanat ovat vuotaneet. No [henkilö] oli laittanut siihen ohjeet, että käykää tekemässä näin ja näin ja näin.” (TUK 2)

5 Tutkimustulosten esittely, tarkastelu ja vertailu

Reaktorin kyberturvallisuuskulttuurin muodostumisen tutkimiseksi kerättiin aineistoa tutkimuksen alkuvaiheessa toteutetun teoreettisen tarkastelun, haastatteluiden ja fenomenografisen analyysin avulla. Tässä luvussa esitellään edeltävissä luvuissa esitetyn tutkimusprosessin kautta muodostetut ja tiivistetyt tutkimustulokset. Luvun keskeisenä tavoitteena on vastata tutkimusprosessin alussa asetettuihin ja sen aikana tarkentuneisiin tutkimuskysymyksiin.

5.1 Organisaation kyberturvallisuuskulttuurin muodostumiseen vaikuttavat tekijät

Organisaatiokulttuurin tavoin kyberturvallisuuskulttuuri muotoutuu organisaatioon tietoisen ja tiedostamattoman toiminnan seurauksena riippumatta organisaation aktiivisesta vaikutuksesta sen syntyyn tai luonteeseen. Jos organisaatio tiedostaa kyberturvallisuuskulttuurin muodostumiseen vaikuttavat tekijät, on mahdollista kehittää kyberturvallisuuskulttuuria tietoisesti haluttuun suuntaan. Kyberturvallisuuskulttuurin kehittämisessä organisaation täytyy tunnistaa organisaation itsensä vaikutusmahdollisuudet, sillä esimerkiksi kansallisen tai ammatillisten alakulttuurien tekijät ovat sen välittömien vaikutusmahdollisuuksien ulkopuolella.

Tutkimuksen teoreettisessa osuudessa todettiin, että kansallinen kulttuuri vaikuttaa organisaation ja yksilöiden toimintatapoihin. Kansallinen kulttuuri ja sen sisältämät yleisesti hyväksyttävä käytös ja toimintamallit luovat perustan luontaisille tavoille, joita yksilöt ovat tottuneet toteuttamaan. Organisaation rakenne, organisaatiokulttuuri, prosessit sekä käyttäjien rooli ja tehtävä kyberturvallisuuden ylläpitämisessä vaikuttavat kyberturvallisuuskulttuurin muodostumiseen. Tätä kautta muotoutuvat toimintatavat määrittävät kyberturvallisuutta ylläpitävää käyttäytymistä sekä yksilöiden ja eri organisaation toimijoiden vastuita.

Organisaation osaaminen rakentuu yksilöiden osaamisesta, joten ymmärrys kyberturvallisuuteen liittyvistä uhkista ja niiden realisoitumisesta sekä taidot tieto- ja viestintätekniikan käytössä ovat keskeisiä organisaation kyberturvallisuuteen vaikuttavia tekijöitä. Organisaation toimiala vaikuttaa sen henkilöstön osaamisprofiiliin ja sitä kautta keskimääräisiin tieto- ja viestintätekniikan käytön taitoihin ja ymmärrykseen kyberturvallisuudesta.

Kyberturvallisuuskulttuurin ylläpitäminen ja kehittäminen perustuvat organisaation ja yksilöiden aktiiviselle toiminnalle. Toiminta perustuu niin yksilön kuin organisaationkin asenteesta kyberturvallisuutta kohtaan. Asenteen on tunnistettu liittyvän aikomukseen toimia, mikä usein johtaa myös toimintaan. Yksilöiden tyytyväisyys työhönsä ja positiivinen työilmapiiri tukevat yksilöiden

halua pyrkiä saavuttamaan yhteiset päämäärät myös organisaation tiedon, tietojärjestelmien ja verkkoinfrastruktuurin suojaamisessa.

5.1.1 Kyberturvallisuuskulttuurin muodostumiseen vaikuttavat tekijät suomalaisissa asiantuntijaorganisaatioissa

Monet Suomen kansalliselle kulttuurille ominaiset asiat liittyvät asiantuntijuuteen ja ovat siten hyvä perusta suomalaisten asiantuntijaorganisaatioiden organisaatiokulttuurille. Suomalaisen asiantuntijaorganisaation toiminnan tulisi perustua yksilöllisyydelle ja luottamukselle kansallisen kulttuurin individualismin korkean tason vuoksi. Suomen kansallisen kulttuurin perusteella luottamusta ja yksilöllisyyttä edistetään antamalla yksilöille vapautta toimia ja tehdä päätöksiä heille määritettyjen roolien ja vastuualueiden puitteissa sekä innovoida heidän asiantuntijuutensa hyödyntäen. Suomi matalan kontekstin kulttuurina on suoraviivainen sekä yksilö-, asia- ja toimintakeskeinen. Se näkyy, tai on ainakin aiemmin näkynyt, suomalaisessa kulttuurissa työkeskeisyytenä ja sitoutumisena annettuihin henkilö- tai ryhmäkohtaisiin vastuisiin.

Individualismin lisäksi matala valtaetäisyys vaatii johtamistoiminnassa työntekijöitä käsiteltävän yksilöinä niin että usein johtaminen tapahtuu läheltä, jopa ryhmän sisältä käsin, ja asiantuntijat osallistuvat päätöksentekoon. Yhteisten tavoitteiden asettaminen ja tavoitteleminen sitouttaa henkilöstöä toimimaan yhdessä. Erilaisten asiantuntijuuteen perustuvien projektikohtaisten organisaatioiden luomista käytetään tapauskohtaisten ja muuttuvien tavoitteiden saavuttamiseksi. Matala maskuliinisuuden taso kertoo kulttuurissa arvostettavan joustavuutta, tasa-arvoa, solidaarisuutta ja laatua, joiden saavuttaminen ja ylläpitäminen vaativat organisaation toiminnalta läpinäkyvyyttä, tasavertaisuutta ja faktoihin perustuvaa päätöksentekoa. Palkitsemisen tulee perustua ansioihin. Kulttuurille ominainen epävarmuuden välttäminen näkyy koulutuksen, tiedon ja turvallisuuden arvostamisena. Olosuhteiden muuttuessa ja etenkin teknologia-alojen nopean kehityksen vuoksi epävarmuuden välttäminen ja faktoihin perustuva päätöksenteko vaativat organisaatiolta yksilöiden niin organisaation itsensä kannustamista jatkuvaan kehittymiseen ja kouluttautumiseen. Epävarmuuden välttäminen suomalaiselle kulttuurille ominaisena piirteenä vaatii organisaatiolta enemmän hierarkiaa tai selkeyttä verrattuna esimerkiksi muihin pohjoismaihin.

5.2 Reaktorin kyberturvallisuuskulttuuri käyttäjien kautta kohdistuvan kyberuhkan kannalta

Reaktorin haastatellun henkilöstön käsitykset organisaationsa kyberturvallisuuskulttuurista vaihtelivat riippuen työtehtävästä, ilmiötä koskevan näkymän laajuudesta, osaamisesta, asenteesta sekä tieto- ja viestintäteknisten ratkaisujen ymmärtämisestä. Suurin osa haastateltavista näki organisaationsa

kyberturvallisuuskulttuurin varsin hyvänä, vaikka yksittäisten ilmaisujen perusteella ilmeni epävarmuutta ja tarpeita kehittää sitä. Käyttäjien kautta kohdistuvaan uhkaan vastataan kyberturvallisuuskulttuurilla, jossa käyttäjä on osa ratkaisua, mutta inhimillisten virheiden ja osaamisvaihteluiden olemassaolo tunnustetaan. Reaktorin kyberturvallisuuskulttuurista muodostui haastateltavien ilmausten perusteella hyvin yhtenäinen kuva. Suomen kansallinen kulttuuri tukee Reaktorin matalan hierarkian organisaatiokulttuuria, joka on perusta kyberturvallisuutta koskeville ratkaisuille ja järjestelyille. Organisaatio- ja kyberturvallisuuskulttuurille on ominaista erityisesti yksilön useat erilaiset roolit organisaatiossa, hierarkian vähäisyyden merkitys, tasa-arvoisuus, luottamuksen merkitys, osaamisen arvostaminen sekä hyödyntäminen, joustavuus ja tietoon perustuvassa toiminta.

Kyberturvallisuuden nähtiin kuuluvan kiinteäksi osaksi organisaation turvallisuus- ja liiketoimintaa. Kyberturvallisuus otetaan huomioon ja turvallisuuden ratkaisuja tarkastellaan jatkuvasti, mutta turvallisuusratkaisujen ei anneta estää käytettävyyttä tai toimintamahdollisuuksia. Turvallisuusratkaisut suunnitellaan tapauskohtaisesti, ja vastuu niiden toteuttamisesta on osa tiimien toimintaa. Perehdyttämisen yhteydessä henkilöstölle kerrotaan organisaation tietoturvaratkaisuista. Ylläpitäjät asentavat käyttäjälle luovutettaviin laitteisiin tietyt tietoturvaohjelmistot ja -ratkaisut. Lisäksi kiinnostuksen ja osaamisen perusteella kyberturvallisuuden kehittämiseen sitoutuneet yksilöt osallistuvat organisaation kyberturvallisuuden ja siihen liittyvien toimintatapojen kehittämiseen. Ylläpitohenkilöstö ja turvallisuusvastuulliset seuraa uhkien kehittymistä ja tiedottaa uhkien vaatimista toimenpiteistä.

Henkilökohtaisen ja tiimin osaamisen kehittäminen on jokaiselle kuuluva moraalinen vastuu. Haastateltavat ymmärsivät tieto- ja viestintätekniikan kautta organisaation toimintaan potentiaalisesti ilmenevän uhkan. Yhdelläkään haastateltavalla ei ollut käsitystä täysin turvallisten ratkaisujen olemassaolosta. Toimenpiteitä koskevat riskit pyrittiin tunnistamaan ja laskemaan riskitaso turvallisuusratkaisuilla hyväksyttävälle tasolle.

Yksilöt ja tiimit nähtiin hyvin itseohjautuvina osaamisen ja ymmärryksen lisäämisessä sekä epäkohtien havaitsemisessa ja korjaamisessa. Yksilöiden valppaus ja aktiivisuus mahdollistaa kyberturvallisuuden tason ylläpitämisen ja kehittämisen (HLEG, 2008). Yksilöiden osallistumisen ja vastuun jakamisen kautta tietoturvaratkaisut ovat näkyviä, eikä valheellista turvallisuuden tunnetta pääse helposti syntymään yksilöille (Kearney, 2010; Greene & D'Arcy, 2010; Choi ym., 2013). Organisaation toiminnassa ei tullut esille jäykkiä toimintamalleja tai asenteellisuutta, jolla olisi heikentävä vaikutus yksilön motivaatioon kyberturvallisuutta kohtaan tai toimintamahdollisuuksiin.

Kyberuhkaan vastataan jakamalla vastuu koko organisaatiolle ja henkilöstölle.

Haasteita nähtiin yksilöiden välisessä kyberturvallisuuden osaamisessa ja sitä koskevissa toimintatavoissa, koska yksilöön luotetaan vahvasti ja yksilöillä sekä tiimeillä on runsaasti toiminnanvapautta. Luottamuksen ja toiminnanvapauden vuoksi tiukkoja turvallisuuskontrolleja tai sitovia ohjeita on vähemmän

kuin useissa hierarkkisissa organisaatioissa. Organisaation kasvussa tunnistettiin myös riskejä, kun toiminta hajautuu ja laajenee maantieteellisesti ja kulttuurisesti sekä organisaation jäsenet eivät enää tunne toisiaan. Luottamuksen rakentamisen on havaittu olevan vaikeampaa virtuaalisissa organisaatioissa ja ensivaikutelman merkitys korostuu, koska osaamisen, ja luotettavuuden vahvistaminen etänä on haastavaa (Lewis, 2006).

5.2.1 Reaktorin kyberturvallisuuskulttuurin kannalta keskeiset tekijät

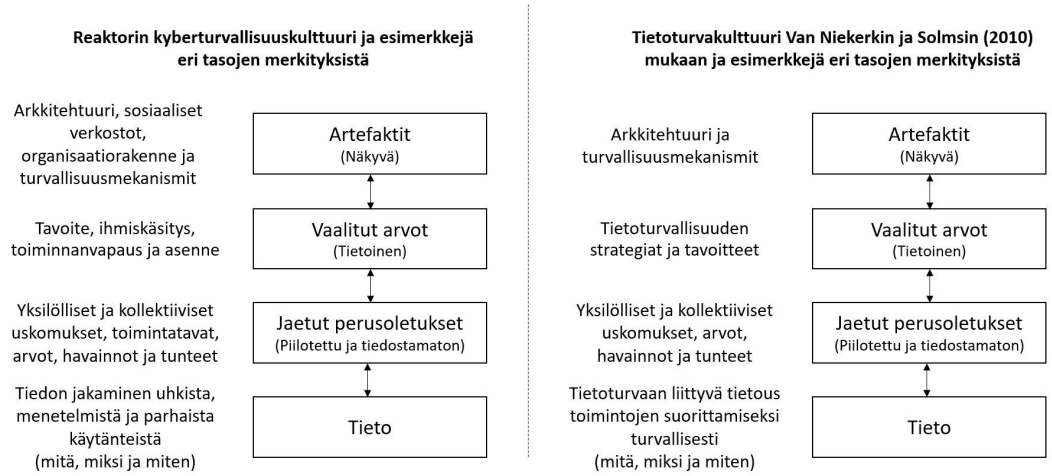
Organisaatiokulttuurin lisäksi yksilöiden asenteella, osaamisella ja henkilökohtaisella kyberturvallisuuskulttuurilla on ehkä ratkaisevin vaikutus organisaation kyberturvallisuuskulttuurin muodostumiseen ja ylläpitämiseen. Kyberuhkien näkökulmasta yksilön toiminta painottuu entisestään, koska se ulottuu myös työn ulkopuoliselle ajalle ja henkilökohtaisiin laitteisiin, keskustelupalstoille- ja ryhmiin sekä sosiaaliseen mediaan. Organisaatioiden sääntely ei ulotu työntekijöiden koko henkilökohtaiseen elämään, vaikka he jakavat siellä tietoa itsestään ja myös edustamastaan organisaatiosta toimiessaan eri toimintaympäristöissä ja rooleissa. Työntekijän organisaatiosta tiedostamatta paljastama informaatio voi olla osa hyökkäystä varten toteutettavaa tiedonkeruuta tai työntekijän henkilökohtaiset laitteet voivat toimia hyökkäysvektorina organisaatiota kohtaan, vaikka ne eivät olisikaan määritetty organisaation erityisesti suojattaviksi kohteiksi (Hutchins, Cloppert & Amin, 2011).

Reaktor on asiantuntijaorganisaatio, jonka toimiala on ohjelmistotuotanto ja konsultointi, minkä vuoksi Reaktorin henkilöstöön kuuluu runsaasti teknisesti taitavia yksilöitä. Organisaation rekrytointiprosessissa selvitetään myös ihmisten kykyä ja halua itsensä kehittämiseen. Nämä ominaisuudet kuvaavat tietoturvatutkimuksissa tärkeäksi havaittua asennetta ja mahdollistavat teknisen osaamisen kompensoinnin ymmärryksellä uhkien luonteesta.

Organisaation aktiiviset yksilöt jakavat tietoa uusista havaituista hyökkäystekniikoista ja uhkista sekä hyvistä käytänteistä. Yksilöiden toiminta perustuu henkilökohtaiseen osaamiseen ja kiinnostukseen, joiden perusteella yksilöille on muodostunut sosiaalinen tai organisaation määrittämä asema. Tietoa jaetaan koulutustilaisuuksien ja sosiaalisten verkostojen kautta. Kriittisistä tai organisaatiota laajasti koskevista tietoturva- tai kyberturvallisuuden uhkista tai havainnoista ohjeistetaan myös suoraan, jotta estetään vastaava poikkeama organisaation muissa osissa. Tietoturva- ja kyberuhkatiedon jakaminen ylläpitää muiden tietoutta ja lisää ymmärrystä niiden vaikutusmahdollisuuksista yksilöön.

Reaktorin kyberturvallisuuskulttuurissa näkyvät ja tietoiset kerrokset, esimerkiksi strategiat ja tavoitteet, eivät korostu ja esiinny perinteisellä, muun muassa Van Niekerkin ja Von Solmsin (2006) tutkimuksessa esitetyllä tavalla (kuva 13). Tavoitteiden asettaminen ei tapahdu yleiseen tapaan organisaation ylätasolla, vaan tiimit, yksilöt ja koko yhteisö asettavat toiminnalleen eritasoisia tavoitteita. Koko organisaatiota ohjaa yhteinen tavoite. Tätä tavoitetta tai sen ilmenemismuotoja ei ole dokumentoitu. Yksilöt omaksuvat tavoitteen perehdyttämisen

sekä mentoroinnin yhteydessä ja oppivat soveltamaan sitä työskentelyn yhteydessä ja organisaation sosiaalisten verkostojen kautta.



Kuva 13. Reaktorin kyberturvallisuuskulttuuri verrattuna Van Niekerkin ja Von Solmsin (2010) tietoturvakulttuurin malliin sekä esimerkkejä eri tasoista

Organisaation turvallisuus on kokonaisuus, jonka keskinäisten vaikutusten vuoksi osia ei tulisi erottaa erillisiksi kokonaisuuksiksi. Kuitenkin tutkimuksen rajaamiseksi haastattelu koski ainoastaan kyberturvallisuuskulttuuria. Kyberturvallisuuskulttuurin onnistunut ylläpitäminen kuitenkin vaatii yksilöiden kyberuhkia koskevan ymmärryksen jatkuvaa lisäämistä sekä henkilöstöltä tieto- ja viestintätekniikan käytön osaamista. Reaktor vastaa turvallisuuden kokonaisuuden ja kyberturvallisuuden tason ylläpitoon organisaatiokulttuurilla, yksilöiden ja tiimien aktiivisuudella sekä kehityshakuisuudella.

5.2.2 Haastateltavien taustat ja henkilökohtainen kyberturvallisuuskulttuuri sekä niiden vaikutus käsityksiin organisaation kyberturvallisuuskulttuurista

Koska teoreettisessa tarkastelussa havaittiin yksilön taustan ja arvomaailman vaikuttavan hänen käsityksiinsä, selvitettiin ja vertailtiin haastateltavien ilmaisuja heidän muihin käsityksiinsä. Haastateltavien kuvailema arvomaailma oli hyvin yhtenevä huolimatta heidän erilaisista taustoistaan, mikä selittyy ainakin osittain rekrytoinnissa kiinnitettävään huomion työntekijän sopeutumiseen organisaation kulttuuriin. Kaikki haastateltavien mainitsemat arvot ja niihin liittyvät yksityiskohdat olivat positiivissävytteisiä, vaikka niihin liittyi myös negatiivisia kokemuksia. Yhteisö, yhteisöt ja yhdessä tekeminen tuli esille usean haastateltavan kuvauksista ja moni esittikin yhteisöllisyyden itselleen tärkeänä arvona. Yhteisöt ilmenivät muun muassa työyhteisönä, kaveriporukkoina sekä harrastus- tai järjestötoimintana. Yhdessä tekeminen ja yhteisten tavoitteiden saavuttaminen koettiin merkitykselliseksi. Haastateltavilla oli vahva halu tehdä ja toimia oikein muita ihmisiä kohtaan. Myös halu kehittää itseään ja halu

ymmärtää erilaisia ilmiöitä yhdisti vastaajia. Toisista huolehtiminen ja ihmisten toimeen tuleminen koettiin tärkeäksi. Vastaavia asioita ja arvoja tuli esille haastateltavien kuvatessa organisaatiokulttuuriaan.

Henkilökohtaisen kyberturvallisuuskulttuurin nähtiin kattavan sekä työn että sen ulkopuolisen elämän, eikä suurin osa haastateltavista ei tehnyt eroa toiminnassaan niiden välillä. Yksittäiset haastateltavat kertoivat suojaavansa työnantajan tietoa ja laitteita tarkemmin kuin henkilökohtaiseen käyttöön tarkoitettuja laitteita ja henkilökohtaisia tietoja. Konkreettiset riskit henkilökohtaisten tietojen väärinkäyttöön ymmärrettiin organisaation tietoja paremmin.

Haastateltavien taustoja ja henkilökohtaista kyberturvallisuuskulttuuria koskevien ilmausten perusteella muodostui karkeasti jaettuna kaksi ryhmää, joihin ryhmiteltyjen ihmisten keskeisinä yhdistävinä tekijöinä olivat koulutus, suuntautuminen ja työtehtävät:

- Ensimmäinen ryhmä muodostettiin teknisesti koulutetuista tai suuntautuneista henkilöistä, jotka olivat suorittaneet diplomi-insinöörin tai maisterin tutkinnon tekniseltä alalta. Vaihtoehtoisesti muodollisen koulutuksen sijaan henkilöt olivat hankkineet teknistä osaamista harrastuneisuuden kautta. Heidän työtehtävänsä lähtökohtaisesti sisälsivät järjestelmien ylläpitämistä, ohjelmointia tai toteutusta asiakkaiden tarpeisiin. Tämän lisäksi he olivat käyttäjinä organisaation järjestelmissä.
- Toinen ryhmä muodostettiin henkilöistä, joilla oli lähtökohtaisesti korkeakoulututkinto joltain muualta kuin tekniseltä alalta. Heidän työtehtävänsä eivät suoraan liittyneet teknisten järjestelmien toteuttamiseen tai heidän roolinsa koskivat muita osa-alueita kuin teknisiä ratkaisuja. Heidän suhteensa teknisiin järjestelmiin oli käyttäjyys tai järjestelmien muiden kuin teknisten ominaisuuksien kanssa työskentely.

Asenne tietoturvaa ja kyberturvallisuutta oli lähes jokaisella haastateltavalla erittäin hyvä. Asenteen on havaittu olevan merkittävä, koska asenne on tietoturva-alan tieteellisissä tutkimuksissa kyetty liittämään aikomukseen, joka puolestaan on toimintaa ennustava tekijä (Mishra & Dhillon, 2006; Rocha Flores ym., 2014; Crossler ym., 2013). Yhteistä kaikkien haastateltavien näkemysten kesken oli kyberturvallisuuden ja -uhkien jatkuva läsnäolo sekä ulottuminen käytännössä kaikille elämän osa-alueille. Haastateltavat tiedostivat tarpeen rajoittaa ja suojata henkilökohtaisia tietojaan. Henkilökohtainen kiinnostus ja asenne kyberturvallisuutta kohtaan vaikuttivat positiivisesti, vaikka henkilöllä ei ollutkaan teknistä taustaa. Kahden ryhmän välillä oli eroja siinä mitä yksityiskohtia tai ilmiöitä he painottivat ja miten he suhtautuivat uhkiin.

Teknisesti suuntautuneet henkilöt hahmottivat kyberturvallisuuden ja -uhkien järjestelmien rakenteen ja teknisen toteutuksen kautta. He näkivät asian pragmaattisena ja jokapäiväisenä huomioon otettavana asiana, joka täytyy ottaa aina huomioon. Kyberturvallisuutta kerrottiin ylläpidettävän sarjoilla tietoisesti toteutetuilla toimenpiteillä. Tavoitteena oli laskea riskit halutulle tasolle, jonka kerrottiin olevan lähtökohtaisesti parempi kuin asiakkaan vaatima taso. Haavoittuvuuksien nähtiin olevan jatkuvasti läsnä, järjestelmien yksittäisten teknisten

ratkaisujen murtaminen mahdollisena riittävillä resursseilla ja inhimillisen virheen mahdollisuus jatkuvana. Kyberturvallisuutta koskeva tieto, taidot ja käytännöt miellettiin tärkeäksi ja osaksi henkilöstön ammattitaitoa. Turvallisuuden ja käytettävyyden suhdetta kerrottiin harkittavan tapauskohtaisesti kuitenkin niin, että turvallisuuden ei tule estää liiketoimintaa. Haastateltavat henkilöt olivat tehneet runsaasti erilaisia ratkaisuja parantaakseen henkilökohtaista kyberturvallisuuttaan.

Muulla tavalla kuin teknisesti suuntautuneet henkilöt olivat tietoisia siitä, että heihin kohdistuu uhkia niin työ- kuin henkilökohtaisessa elämässä. He painottivat enemmän henkilökohtaisten tietojen suojaamista, identiteettivarkauden uhkaa, sosiaalisen median kautta tapahtuvaa tiedonkeruuta ja muita yksityisyyttä koskevia uhkia. Edellä mainittujen ilmausten perusteella tehdyt ratkaisut olivat pääsääntöisesti luonteeltaan enemmän toiminnallisia kuin teknisiä.

Henkilökohtaiset kokemukset kyberuhkista tai tietoturvapoikkeamista vaikuttivat positiivisesti kaikkien haastateltavien käsityksiin uhkien merkityksestä ja asenteisiin kyberturvallisuutta kohtaan. Kokemukset olivat joko henkilökohtaisia tai lähipiirissä tapahtuneita asioita, mutta yhteistä suurimmalle osalle niistä oli ilmausten kautta välittyvä kokemukseen liittynyt tai edelleen liittyvä tunnereaktio. Huolimatta kokemusten negatiivisesta luonteesta, niiden voidaan tulkita lisänneen haastateltavien ja muiden yksilöiden ymmärrystä kyberuhkien ilmenemisestä sekä halusta ja kyvystä selviytyä vastaavista tilanteista.

5.2.3 Reaktorin organisaatiokulttuurin vaikutus yrityksen kyberturvallisuuskulttuuriin

Kyberturvallisuuskulttuuriin kuuluu määritelmällisesti osia organisaatiokulttuurista, koska organisaatiokulttuuri koostuu myös kyberturvallisuutta ylläpitävään toimintaan vaikuttavista rakenteista ja toimintatavoista. Organisaation kyberturvallisuuskulttuuriin vaikuttaa organisaation ulkopuolisia yhteiskunnan ja yksilöiden kyberturvallisuuskulttuureja. (Da Veiga, 2016). Organisaatiokulttuurin vaikutuksen tietoturva- ja kyberturvallisuuskulttuuriin on havaittu aiemmissa tietoturva-alan tutkimuksissa painottuvan enemmän käytäntöihin ja asenteisiin kuin arvoihin (Knapp ym., 2009), mikä kuitenkin voi vaihdella organisaatiomallin, yksilöiden ja organisaation arvojen samankaltaisuuden sekä arvoihin sitoutumisen myötä. Esimerkiksi matalan hierarkian organisaatioissa päätöksentekoa on hajautettu. Yksittäisellä henkilöllä tai tiimillä on hierarkkista organisaatiota enemmän toiminnanvapautta, jolloin organisaation suunnitelmallinen toiminta vaatii vahvaa organisaatiokulttuuria sekä yksilöiden sitoutumista yhteisiin tavoitteisiin ja toimintatapoihin sekä niiden kehittämiseen.

Tutkimuksen kohteena olleen matalan hierarkian organisaation tiimien ja aktiivisten yksilöiden toimintaan perustuvan kulttuurin vaikutus ulottuu myös organisaation kyberturvallisuuskulttuuriin. Keskeisen merkityksensä vuoksi organisaatiokulttuuri on yksilöiden osaamisen, itseohjautuvuuden ja aktiivisuuden ohella yksi Reaktorin kyberturvallisuuskulttuurin kulmakivistä. Toimintatavat, rakenteet ja roolitus kyberturvallisuuden organisoinnissa on samankaltaiset

kuin muussa toiminnassa, mikä luo selkeyttä ja asemoi kyberturvallisuuden kiinteäksi osaksi tiimien ja yksilöiden vastuita sekä toimintaa. Yhteenkuuluvuuden ja yhteishengen kautta yksilöllä on moraalinen vastuu organisaation tavoitteiden, myös kyberturvallisuuden, edistämiseen. Moraalisten vastuiden merkitys yksilöiden tietoisuuden lisäämiseen tähtäävissä koulutuksissa on tunnistettu kyberturvallisuutta parantavaksi (D'Arcy ja Lowry, 2019) ja luovat sisäistä motivaatiota.

Kehityshakuisuus ja eteenpäin pyrkiminen painottuvat Reaktorin kulttuurissa. Organisaatiokulttuuri tukee yksilöiden tai tiimien osaamisen kehittämistä koulutusten kautta sekä kokeilemalla uusia tai vaihtoehtoisia ratkaisumalleja. Hyviä käytänteitä, havaintoja, tietoa ja kokemuksia jaetaan sisäisten koulutusten, yhteistoimintaa tukevien työkalujen ja sosiaalisten verkostojen kautta. Organisaation toimintatapoja, tilaa ja suuntaa tarkastellaan jatkuvasti. Kehittämisessä osallistujina tai keskustelun aloittajina voi olla kuka tahansa organisaation jäsen. Yhteistyö ja vuorovaikutustaidot ovat vaatimus tavoitteiden saavuttamiselle. Annaleena Aira (2012) on tutkinut yhteistyötä ja vuorovaikutussuhteita työelämässä. Hänen mukaansa (Aira, 2012) toimivaa yhteistyötä kuvaavat juuri:

- Vuorovaikutussuhteiden hallinta, joka koostuu luottamuksen rakentamisesta, vuorovaikutussuhteiden ylläpidosta sekä etäisyyden ja läheisyyden välisestä tasapainosta.
- Tiimin prosessien hallinta, jonka osia ovat tiimin muodostuminen, vuorovaikutuskäytänteiden luominen ja aktiivinen johtajuus.
- Verkoston hallinta, joka koostuu keskinäisen kilpailun hallinnasta, erilaisuuden hyödyntämisestä ja suunnitelmien konkretisoinnista toteutukseksi.

Organisaatiossa tapahtuvan yhteistyön tähtäin on tavoitteiden saavuttamisessa. Se voi toteutua läsnäoloa vaatien tai hajautetusti. Yhteistyö on luonteeltaan dynaamista. Yhteistyö on tehokkainta kahden tai kolmen henkilön toteuttamana. (Aira, 2012).

Haastateltavien ilmaukset organisaationsa organisaatiokulttuurista olivat hyvin yhtenevät, mikä kertoo organisaatiokulttuurin vahvuudesta. Organisaation arvot ja työntekijöiden henkilökohtaiset arvot olivat samankaltaisia, mikä vahvistaa työntekijöiden motivaatiota ja sitouttaa organisaation toimintaan sekä toisiaan kohtaan. Reaktorin arvot eivät olleet ristiriidassa organisaation käytäntöjen tai haastateltavien henkilökohtaisten arvojen kanssa, mikä vahvistaa yksilön sitoutumista organisaatioon ja sen toimintatapoihin. Organisaation uudet jäsenet lähtökohtaisesti kykenevät ja haluavat toimia organisaatiokulttuurin mukaisesti, koska yksilön mahdollisuuteen sopeutua organisaation toimintatapoihin kiinnitetään huomiota jo rekrytoinnissa.

Organisaatiokulttuuri perustuu toisten yksilöiden kunnioittamiseen, keskinäiseen luottamukseen ja positiiviseen ihmiskuvaan. Positiivinen työilmapiiri tutkitusti lisää yksilön halua myös noudattaa tietoturvaohjeistuksia (D'Arcy & Lowry, 2019). Reaktorilla oletetaan, että jokaisella on halu ja kyky toimia yhteisten tavoitteiden eteen. Se lisää yksilöiden motivaatiota ja sitoutuneisuutta, kun

organisaatio osoittaa näkevänsä yksilön myös turvallisuutta edistävänä tekijänä, eikä ainoastaan turvallisuusriskinä (Von Solms, 2000). Päätöksenteko yksittäistä toimintoa ja tiimiä koskevista asioista on laskettu asiantuntija- ja tiimitasolle, mikä on samalla organisaation luottamuksenosoitus ja vastuujakoa yksilöitä kohtaan. Päätöksenteko toteutetaan tietoon perustuen, ja siinä arvioidaan tapauskohtaisesti tietoturvaratkaisujenkin tarkoituksenmukaisuutta. Päätöksenteko ei se perustu esimerkiksi operatiivisen toiminnan ulkopuolelta annettuja valmiisiin malleihin tai ohjeisiin. Yksilöiden ja tiimien itseohjautuvuus, aloitteellisuus ja kyky ottaa vastuuta edistää myös kyberturvallisuutta koskevia ratkaisuja. Se myös ohjaa ja vaatii hankkimaan puuttuvaa osaamista tilanteessa, jossa tunnistetaan tarve osaamisen kehittämiselle. Organisaatiokulttuuri vastaa organisaation suojautumiseen kaikilta uhkilta.

Reaktorilla vallitseva luottamus perustuu uskomukseen toisten yksilöiden ja tiimien halusta, kyvystä ja osaamisesta hyödyntää tieto- ja viestintäteknologiaa turvallisella tavalla sekä ottaa järjestelmien suunnittelussa ja käytössä huomioon erilaiset uhkat. Yksilön ja tiimin asenne, ymmärrys ja osaaminen on keskeistä. Uuden projektin alussa muotoutuu paikallinen alakulttuuri, koska osaaminen, työskentelytavat ja kyky hyödyntää organisaation tukea myös kyberturvallisuudessa vaihtelee yksilön ja tilanteen mukaan.

Reaktorin kulttuurissa esiintyy useita myös Geert Hofsteden (1999) tutkimuksessa havaittuja Suomen kansalliselle kulttuurille ominaisia piirteitä. Taulukossa 3 on verrattu Reaktorin henkilöstön tunnistamia piirteitä Hofsteden (1999) tutkimuksen Suomea koskeviin tuloksiin. Yhtenevät piirteet on kuvattu plusmerkillä (+) ja eroavat miinusmerkillä (-).

Suomen kansallisen kulttuurin ulottuvuudet ja käytännön esiintyminen:	**Reaktorille henkilöstön tunnistamat organisaatiolle ominaiset piirteet:**
Korkea individualismin taso 1. Ansioiden merkitys 2. Yksilöiden johtaminen 3. Työsuhteen kaksisuuntainen hyöty 4. Yksilö huolehtiminen itsestään	+ Kokemuksen, ansioiden ja osaamisen merkitys + Johtajuus tiimien sisällä + Yksilön päätösvalta vastuualueellaan ja edistämissään asioissa + Yksilön vastuunottamisen edellyttäminen
Matala valtaetäisyyden taso 1. Hierarkian pieni merkitys 2. Tasa-arvo päätösvallan jakamisessa 3. Valmentava johtajuus 4. Päätösvallan hajautus 5. Suora ja osallistava kommunikointi	+ Organisaation matala hierarkia + Yksilöiden ja tiimien valta tehdä päätöksiä + Johtajuus tiimien tai toimintojen sisällä, ei esimiehiä + Henkilöstön osallistaminen kommunikointiin
Matala maskuliinisuuden taso 1. Toisista välittäminen 2. Elämänlaatu	+ ”Suopeuden periaate” + Laadun ja käytettävyyden arvostaminen

3. Tasa-arvo ja solidaarisuus 4. Joustavuus 5. Konsensukseen pyrkiminen 6. Statusta ei näytetä julkisesti 7. Sukupuoliroolien vähäinen merkitys	+ Huolenpito toisista + Joustavuus + Tasa-arvoisuus +/- Konsensukseen pyritään, mutta yksilö tai tiimi tekee päätöksen vastuullaan olevasta asiasta + Sukupuoliroolien vähäinen merkitys
Korkea epävarmuuden välttämisen taso 1. Tiedon arvostaminen 2. Selkeys 3. Tarve säännöille 4. Täsmällisyys ja tarkkuus 5. Turvallisuus on tärkeä elementti motivaation kannalta	+ Tietoon perustuva toiminta + Tapauskohtaiset ratkaisut + Vastuiden selkeys + Vertaisten tuki ja ohjaaminen + Asiakkaan todellisiin tarpeisiin vastaaminen + Arvojen ja käytännön vastaaminen - Absoluuttisten sääntöjen sijaan yhteinen tapa tehdä asioita - Vaihtelu muodollisissa toimintatavoissa
Matala pitkän aikavälin orientaation taso 1. Absoluuttisten totuuksien arvostaminen 2. Perinteiden arvostaminen 3. Tulosten nopea saavuttaminen	+ Tulosten nopea saavuttaminen ja ketterien menetelmien hyödyntäminen + Pyrkimys säilyttää muutosvaiheessa organisaation alkuperäinen olemus ja henki + Tavoite tuottaa asiakkaalle välitöntä hyötyä - Muuttumattomien totuuksien puute - Toimintatapojen jatkuva kehittäminen ja muuttaminen tarvittaessa
Korkea suopeuden taso 1. Positiivinen asenne 2. Vapaa-ajan arvostaminen 3. Yksilöllinen valinnanvapaus	+ Positiivinen ihmiskuva + ”Suopeuden periaate” + Eteenpäin pyrkiminen, kehityshakuisuus + Yksilön päätöksentekovalta

Taulukko 4. Suomen kansallisen kulttuurille ominaisten piirteiden (Lewis, 2005; Hofstede, 1999) ja Reaktorin asiantuntijoiden käsitysten (haastattelumateriaali) vertailu

Reaktor eroaa absoluuttisten totuuksien ja muodollisten toimintatapojen merkityksen pienemmällä merkityksellä, jos sitä verrataan Geert Hofsteden (1999) ja Richard Lewisin (2005) tutkimusten tuloksiin. Erot mahdollisesti selittyvät Reaktorin luonteella matalan hierarkian organisaationa sekä tutkimuksen painottumisena jatkuvasti muuttuvaan kyberturvallisuuden toimialaan, jossa

toimintamallit muuttuvat ja kehittyvät hyvin nopeasti. Tässä tutkimuksessa ei yritetä analysoida kattavasti organisaatiokulttuuria, koska tutkimuksessa tehtyjen rajausten vuoksi pitkälle vietyjen johtopäätösten tekeminen ei ole tarpeellista.

6 Pohdinta ja yhteenveto tutkimuksen tuloksista

Tässä luvussa arvioidaan tutkimuksen luotettavuutta, tutkimusmenetelmän käyttöä tutkimuksessa ja tulosten hyödynnettävyyttä. Lopuksi esitellään jatkotutkimusaiheita ja yhteenveto tutkimustuloksista.

6.1 Tutkimuksen luotettavuus

Tutkimuksen luotettavuutta arvioidaan yleensä validiteetin, reliabiliteetin ja tutkimustulosten yleistettävyyden näkökulmasta. Näiden käsitteiden arviointi edellyttää sitä lähtökohtaista oletusta, että on olemassa yksi yhteinen todellisuus, jonka yksilöt kokevat samalla tavalla (Lincoln, 1985). Fenomenografisessa tutkimussuuntauksessa olettamus on kuitenkin se, että yksilöt kokevat todellisuuden eri tavoin. Todellisuus on olemassa ihmisille merkitysvälitteisesti, ja se rakentuu merkitystulkinnoista sekä tulkintasäännöistä (Uljens, 1989; Huusko & Paloniemi, 2006). Ei ole perusteltua arvioida tämän tutkimuksen validiteettia ja reliabiliteettia tieteellisessä tutkimuksessa yleisesti käytettyjen mittarien avulla, vaan antaa lukijalle perusteet arvioida tutkimuksen luotettavuutta tutkimusprosessin ja siinä tehtyjen valintojen huolellisella kuvaamisella sekä perustelemisella. Siksi tutkimuksen luotettavuus huomioitiin tutkimusprosessin alusta asti tunnistaen valitun tutkimusmenetelmän tuottamat vaatimukset sen toteutukselle ja dokumentoinnille. Luotettavuutta pyrittiin lisäämään pohtimalla, esittelemällä ja perustelemalla tutkimuksessa tehdyt ratkaisut ja valitut menetelmät sekä tutkimusprosessi ja siihen vaikuttaneet tekijät (Metsämuuronen, 2011).

Vaikka tutkimuksessa ei ollut hypoteesia, tutkijan työelämälähtöiset kokemukset hierarkkisen organisaation kulttuurista, johtamisesta ja kyberturvallisuudesta ohjasivat varmasti tutkijan henkilökohtaisten käsitysten muodostumista ja tulkintoja. Laadullinen tutkimus ei koskaan voi olla täysin vapaata ennakkokäsityksistä, koska tutkijan arvot ja ennakkokäsitykset ohjaavat tulkintoja (Hirsjärvi ym., 2007). Ennakkokäsitykset kuvattiin tutkimuksessa, ja niitä pyrittiin tietoisesti vähentämään ennen haastatteluja. Pelkästään jo tutkijan henkilökohtaisten näkemysten tunnistamisella ja kuvaamisella voidaan vähentää niiden vaikutusta tutkimuksen toteuttamiseen (Ashworth & Lucas, 2000; Uljens, 1992).

Teoreettisen validiteetin takaamiseksi tarkentavat haastattelukysymykset pohjautuivat tutkimuksen ensimmäisessä vaiheessa tuotettuun teoriatietoon (Ahonen, 1994). Tutkimuksessa huomioitiin ja tunnustettiin tutkimusmenetelmästä aiheutuvat rajoitukset sekä valittuihin teorioihin kohdistunut perusteltu kritiikki. Tutkimuksen luotettavuuden lisäämiseksi kiinnitettiin huomiota tutkimuksen toteuttamisen yhteydessä tehtyihin valintoihin ja niiden kuvaamiseen. Tutkimusprosessi ja sen eri vaiheet kuvattiin kattavasti luotettavuuden ja validiteetin arvioimiseksi, vaikka fenomenografinen tutkimus ei olekaan toistettavissa edes samassa tutkimuskontekstissa saman tutkijan toteuttamana johtuen

tutkimustapahtuman ainutlaatuisuudesta. Hirsjärvi & Hurme (2008) ovat todenneet, että laadullisella tutkimuksella ei päästä täydelliseen toistettavuuteen, koska ihminen muuttuu ajan myötä ja eri tutkijat tulkitsevat materiaalia eri tavoin.

Haastattelutapahtuma pyrittiin takaamaan mahdollisimman samanlaiseksi jokaisen haastateltavan osalta, jotta haastattelutapahtuman järjestelyt eivät vaikuttaisi haastateltavan kykyyn tai tapaan pohtia tutkimuksen keskeistä ilmiötä. Teoriapohjan perusteella etukäteen tutkija oli laatinut haastattelujen tukena käytettävän kysymyslistan, jonka avulla taattiin keskeisten teemojen ja niihin liittyvien yksityiskohtien läpikäynti sekä eri näkökulmien huomioiminen. Kysymyslistan avulla pyrittiin myös vähentämään tutkijan asenteiden ja näkemysten vaikutus yksittäiseen haastattelutapahtumaan. Kysymyslistan laatiminen mahdollisti haastattelutapahtumien toteuttamisen mahdollisimman samanlaisena ja auttoi ohjaamaan haastattelutapahtumaa (Boeije, 2010). Kysymykset oli muotoiltu yksinkertaisiksi ja ymmärrettäviksi sekä teoreettisia ilmaisuja tai terminologiaa oli pyritty välttämään väärinymmärryksen välttämiseksi. Fenomenografisen tutkimuksen perusteiden mukaisesti tavoitteena oli luoda avoin ilmapiiri ja antaa haastattelutapahtuman edetä vapaasti. Haastattelut nauhoitettiin, jotta tutkija pystyi keskittymään haastattelutapahtumassa tarkentavien kysymysten esittämiseen ja pyrkimään ymmärtämään ilmaisujen merkityksiä. Nauhoitusten avulla tutkija pystyi jälkikäteen tarkistamaan eri ilmaisujen tarkan muodon ja vertailemaan ilmaisuja.

Tutkimuksen teoriataustan muodostamisessa lähteinä käytettyjen tutkimusten validiteetti ei ole täysin varmistettavissa. Enisa (2018) arvioi erilaisissa tietoturvaa ja kyberturvallisuutta koskevissa tutkimuksissa käytettyjä metodeja. Enisa havaitsi lukuisia ongelmia liittyen muun muassa kerätyn todenmukaisuuteen, eri tieteenaloilta suoraan lainattujen teorioiden käyttöön, uhka- ja rangaistuskeskeisyyden painottamiseen kouluttamisen ja tukemisen sijaan sekä taustatietojen vähäisessä pohtimisessa ja hyödyntämisessä. Useissa tutkimuksissa keskityttiin tutkimaan aihetta kapeasti ja jätettiin huomiotta yksilön käytökseen vaikuttavia tekijöitä, mutta esitettiin silti yleispäteviä johtopäätöksiä. (Enisa, 2018).

Tämän tutkimuksen teoriaosuuden ja tutkimusmenetelmään perehtymisen kautta tunnistettiin myös kontekstin merkitys tutkimusten toteuttamisessa. Moni käsite tai toimintatapa on kulttuurisidonnainen eli muodostuu eri asioiden kontekstin mukaan. Tutkimuksen toteuttamisessa käytetty kieli ja sen ilmaisut vaikuttavat siihen, miten vastaajat ymmärtävät kysymyksenasettelun tai ilmaisevat käsityksensä. Tutkimuksen teoriaosuuden aikana havaittiin, kuinka kieli ja kulttuurikonteksti ovat ratkaisevia ilmaisujen ja käsitteiden ymmärtämisen sekä esittämisen kannalta. Havainto tukee Enisan (2018) löydöstä, että useat tietoturvaalan tutkimukset eivät ole ottaneet riittävästi huomioon vastaajien tai käsittele taustaa ja sen vaikutusta vastauksiin. Myöskään eri käsitteiden mahdollisia merkityseroja tai käyttäytymismallien vaikutusta yksilöiden toimintaan eri kulttuureissa ei käsitellä. Tämä asettaa etenkin käyttäjän asennetta, toimintaa ja aikomuksia tutkineiden tutkimusten tulosten ja johtopäätösten luotettavuuden

kyseenalaiseksi, mikäli edellä mainittuja seikkoja ei ole tutkimuksessa pohdittu tai esitetty kattavasti.

6.2 Tutkimuksessa käytetyt menetelmät

Tutkimuksen pääasialliset metodologiset valinnat olivat laadullinen luonne, fenomenografia tutkimusmenetelmänä ja avoimen teemahaastattelun käyttö aineiston keräämiseen. Valinnat perustuvat tutkimuksen kannalta keskeisten tekijöiden, kulttuurin eri lajien ja kyberturvallisuuden, luonteisiin.

Fenomenografia tutkimusmenetelmänä antaa runsaasti mahdollisuuksia tutkimuksen toteuttamisessa, koska se nojaa enemmänkin periaatteisiin kuin valmiisiin malleihin tutkimuksen käytännön toteuttamisesta. Tämän vuoksi menetelmällisten valintojen vaikutus tutkimukseen täytyy tuntea, jotta osataan arvioida tarve tutkimuksen rajaamiseksi. Tässä tutkimuksessa rajaaminen epäonnistui osittain tutkijan kokemattomuuden vuoksi. Kokonaisuus muodostui liian laajaksi, minkä tuloksena tutkimus jäi paikoin pintapuoliseksi eikä syy-yhteyksien syvällinen arviointi ollut mahdollista.

Haastatteluvaihetta varten valittua menetelmää toteutettiin hyvin vapaasti, koska tavoitteena oli antaa haastateltaville vapaus pohtia käsiteltävää teemaa laajasti eikä rajoittaa ilmaisua koskemaan yksittäistä teemaa kerrallaan. Tämä johtui myös eri teemojen limittymisestä ja kyberturvallisuuden ilmiöiden koskemisesta lähes kaikkia teemoja. Ensimmäiseksi teemaksi valittu haastateltavan kuvaus taustoista ja arvoista toimi erinomaisesti haastateltavien rohkaisemisessa reflektoimaan vapaasti. Tutkijan esittämien tarkentavien kysymysten kautta haastateltavia ohjattiin jatkamaan pohdintaa teemojen tai yksityiskohtien ympäriltä sekä pyrittiin selvittämään ilmausten taustoja ja syitä. Valittu tapa soveltaa tutkimusmenetelmää tuotti runsaasti ja laajasti tietoa sekä teki jokaisesta haastattelutilaisuudesta erilaisen. Se asetti painoarvoa yksilöllisille ilmauksille ja eri tavoille kokea tutkittava ilmiö.

Aineistonkeruutavan valinta tuotti haasteita analyysivaiheessa ja tulosten ryhmittelyssä. Yksittäisessä ilmauksessa saatettiin viitata useaan eri teemaan ja teemat jakoivat keskenään runsaasti asioita, mikä oli odotettavaa teemojen rajapintojen ja tutkittavan ilmiön ominaisuuksien vuoksi. Fenomenografisen analyysin toteuttamiseksi oli kuitenkin tarve käsitellä asiakokonaisuudet teemoittain, joten yksittäisten ilmaisujen yhdistäminen oikeaan teemaan ja toiston välttäminen osoittautuivat haasteelliseksi. Tutkimusprosessissa tuli useasti esiin fenomenografisen tutkimusmenetelmän käyttöön sisältyvä olettamus tutkimustilanteen ainutlaatuisuudesta ja lukuisten yksittäisten valintojen vaikuttamisesta tutkimuksen toteuttamiseen.

Fenomenografiaa on kritisoitu tutkimusmenetelmänä, koska se on hyvin empiirinen ja kuvaa vain otosta yksittäisellä hetkellä. Kritiikki koskee etenkin Ference Martonin ajatusta ”puhtaasta fenomenografiasta”. Haastateltavat ilmaisevat ymmärryksensä ilmiöstä tietyllä ajanhetkellä. Fenomenografiaa on kritisoitu myös näiden yksittäisten ilmausten sovittamisesta tutkimuksessa luotaviin

kategorioihin. Kuvauskategorioita voi olla olemassa vain rajallinen määrä, joka riippuu tutkijasta. Muissa laadullisten tutkimuksen menetelmissä kuin fenomenografiassa käytettävä instrumentti täytyy aina vahvistaa tai osoittaa teoreettinen saturaatio. Tutkijan käsitykset myös muuttuvat tiedonkeruun ja analyysin edetessä, mikä vaikuttaa hänen tulkintaansa. (Alsop, G. & Tompsett, C., 2006; Entwistle, 1997).

Moni fenomenografian kritisoitu piirre voidaan kuitenkin nähdä enemmän varottavana tekijänä tai uhkana kuin esteenä menetelmän hyödyntämiselle. Kysymysten asettelu haastattelutilanteessa täytyy toteuttaa niin, ettei haastattelija ohjaa haastateltavan kuvausta vaan hän voi toteuttaa sen omista lähtökohdistaan. Ilmauksista muodostuneiden kategorioiden välillä tulee olla selkeitä, kuvattavissa olevia eroja. Tutkijan tulkinta voi vaikuttaa ilmausten sijoittamiseen kategorioihin, joten kategorioiden tulee mahdollisimman pitkälle edustaa ilmauksia. Vertailtaessa kategorioiden välisiä suhteita tulee hyödyntää aiempien tutkimusten tuottamaa tietoa. (Entwistle, 1997).

6.3 Tutkimustulosten hyödynnettävyys

Tutkimuksen tulokset ovat hyödynnettävissä kyberturvallisuuden ja tietoturvan tutkimuksessa, kyberturvallisuuskulttuurin, matalan hierarkian organisaatiota tai sen organisaatiokulttuuria sekä tutkittaessa kansallisen kulttuurin vaikutusta organisaatiokulttuuriin suomalaisessa kontekstissa. Tutkimus antaa perusteet tarkastella organisaation kyberturvallisuuskulttuuriin vaikuttavia tekijöitä ja hyödyntää tutkimuksessa esille nostettuja kyberturvallisuuden sekä organisaatiokulttuurin parhaita käytänteitä. Tutkimustuloksia tarkastellessa täytyy ottaa huomioon, että fenomenografisella tutkimusmenetelmällä saadut tulokset ovat hyvin kontekstisidonnaisia eikä tarkoitus ole tuottaa täysin yleistettäviä tuloksia ilman viittausta tutkimuskontekstiin (Marton & Booth, 1997).

Tutkimustuloksia hyödynnettäessä täytyy huomioida tutkimuksen konteksti (Alasuutari, 2011). Haastateltavien näkemyksiin ja organisaatiokulttuuriin vaikuttaa suomalainen kansallinen kulttuuri. Reaktor on luonteeltaan matalan hierarkian asiantuntijaorganisaatio ja ohjelmistoyritys, joten tutkimustulosten hyödynnettävyyttä täytyy tarkastella kriittisesti tutkittaessa hierarkkisempaa, jollain muulla toimialalla toimivaa tai henkilöstön tietoturva- ja kyberturvallisuuden osaamiseltaan poikkeavaa organisaatiota.

Tutkimustulosten hyödynnettävyyttä voi parantaa jatkotutkimuksella. Tässä tutkimuksessa haastateltavien määrä (n = 10) oli rajallinen, eikä välttämättä edustanut organisaation kaikkia osia. Yksittäisen henkilön toimintaympäristön arviointi ei ollut tutkimuksen rajoitusten vuoksi mahdollista, vaikka se vaikuttaa hänen näkemyksiinsä. Jatkotutkimus parantaisi tämän tutkimuksen tulosten luotettavuutta ja hyödynnettävyyttä sekä yleistettävyyttä.

6.4 Jatkotutkimusaiheet

Tämä tutkimus toteutettuna pro gradu -opinnäytetyönä oli ainoastaan pintaraapaisu tutkimuksen kohteena olleesta ilmiöstä ja tutkimuksessa käsitellyistä aiheista. Useita tutkimuksessa käsiteltyjä ilmiöitä tai aiheita olisi tarpeellista syventää tai varmistaa jatkotutkimuksella. Kyberturvallisuus ja kyberturvallisuuskulttuuri ovat tuoreita ilmiöitä, joiden ilmeneminen yhteiskunnissa, organisaatioissa ja yksilöiden elämissä muuttuvat teknologian kehittyessä ja ymmärryksen lisääntyessä.

Tässä tutkimuksessa keskeisenä tutkimuskohteena olivat yksilöiden käsitykset organisaationsa kyberturvallisuuskulttuurista. Tutkija ei tietoisesti subjektiivisuuden välttämisen, tutkimuksen julkisen luonteen tai kyberturvallisuuden järjestelyjen herkkyyksien vuoksi selvittänyt tai esittänyt kattavasti itse ilmiötä koskevia yksityiskohtaisia tietoja. Reaktorin rakenteiden sekä tietoturvan ja kyberturvallisuuden ohjeistusten vertaaminen asiantuntijoiden käsityksiin antaisi mahdollisuuden verrata organisaatioiden ja yksilöiden käsitysten yhteneväisyyttä sekä eri mekanismien toimivuutta ja näkyvyyttä. Ilmiö myös esiintyy ihmisille eri tavalla toimintaympäristöstä riippuen. Mikäli ilmiötä Reaktorilla halutaan tarkemmin ymmärtää, on kyberturvallisuuskulttuurin erojen tutkiminen Reaktorin tiimien ja toimintojen välillä tarpeellista.

Julkisen sektorin organisaatioita sitovat useat eri tiedonkäsittelyä, arkistointia ja julkisuutta koskevat lait ja asetukset. Edellä mainituilla tekijöillä on vaikutusta myös kyberturvallisuuskulttuuriin, joten yksityisen ja julkisen sektorin yritysten tutkiminen esimerkiksi tapaustutkimuksin tai vertailu mahdollistaisi lakien ja asetusten vaikutusten arvioinnin. Julkisen sektorin organisaatiot ovat lähtökohtaisesti hierarkkisia, joten tutkimuskohteena voisi olla myös organisaatiokulttuurin vaikutus kyberturvallisuuskulttuuriin sekä eri organisaatioissa havaitut erot ja yhteneväisyydet.

Kyberturvallisuuskulttuuri voi ilmetä eri tavalla matalan hierarkian asiantuntijaorganisaatioissa eri kulttuurikonteksteissa. Organisaatiokulttuurin ja kansallisen kulttuurin vaikutusta kyberturvallisuuskulttuuriin tulisi tutkia organisaatiorakenteeltaan ja -kulttuuriltaan samankaltaisissa organisaatioissa eri kulttuureissa tai monikansallisen yrityksen eri maissa sijaitsevissa toimipisteissä.

Tässä tutkimuksessa haastateltavien otos oli melko pieni, jolloin yksittäisten haastateltavien näkemykset korostuvat. Organisaation kaikki osat eivät myöskään olleet edustettuina, koska kulttuuri ilmenee eri tavoin organisaation eri osissa. Organisaation kyberturvallisuuskulttuurista olisi mahdollista saada tarkempi käsitys tutkimalla organisaation kyberturvallisuuskulttuuria useassa vaiheessa yhdistämällä laadullista ja määrällistä tutkimusta. Tämä mahdollistaisi laajemman tiedonkeruun.

Yksilön henkilökohtaisen kyberturvallisuuskulttuurin muodostuminen ja perusteet sen muodostumiselle sekä yksilön tietoturvaa koskeva käytös ja päätöksenteko erilaisissa tilanteissa ovat olennainen tutkimuksen kohde ennustettaessa yksilön käyttäytymistä ja tunnistettaessa siihen sisältyviä riskejä. Yksilön

toiminta on kuitenkin organisaation kannalta keskeisin tekijä, koska tietoturva ja kyberturvallisuus on pohjimmiltaan sarja yksilöiden valintoja ja tekoja.

6.5 Yhteenveto tutkimuksen tuloksista

Käyttäjien kautta organisaation kyberturvallisuutta vastaan suuntautuvia hyökkäyksiä kyetään estämään tehokkaasti, jos koko organisaatio osallistuu kyberturvallisuuden ylläpitämiseen määritettyjen vastuiden ja roolien mukaisesti. Kyberturvallisuuskulttuuri rakentuu yksilöiden toiminnasta, jossa keskeistä on heidän asenteensa ja ymmärryksensä kyberturvallisuudesta. Kyberturvallisuuskulttuuria tarkasteltaessa täytyy huomioida erot siinä, että osaamisen ja ymmärryksen ohella yksilöt eroavat siinä mitä he omaksuvat ympäröivistä kulttuureista ja minkä verran he ymmärtävät kulttuurin muodostumisesta. Tämä vaikuttaa heidän kykyynsä tehdä itsenäisiä ratkaisuja sekä kehittää ja ylläpitää kulttuuria yksilötasolla.

Käyttäjiä ja inhimillisiä virheitä koskevan haasteen ratkaisemiseksi ei ole olemassa vain yhtä oikeanlaista kyberturvallisuuskulttuuria. Ymmärtääkseen kyberturvallisuuskulttuurin muodostuminen organisaatiossa on tärkeää tunnistaa organisaation toimintaympäristö sekä organisaatiossa vallitseva kulttuuri ja siihen vaikuttavat tekijät. Organisaatio koostuu yksilöistä, joilla voi olla kasvatuksen, koulutuksen tai sosiaalisten ympäristöjen kautta omaksuttuja arvoja, toimintamalleja tai tiedostamattomia peruskäsityksiä. Arvioimalla edellä mainituista tekijöistä muodostuvaa kokonaisuutta voidaan päästä sille yleistämisen tasolle, joka mahdollistaa organisaatiolle sen kyberturvallisuuskulttuurinsa tietoisen ohjaamisen. Erittelemällä organisaation kyberturvallisuuden tavoitteet, mahdollisuudet ja rajoitukset voidaan räätälöidä organisaation kontekstiin parhaiten soveltuvat ratkaisut.

Tutkimuksessa haastatellun yrityksen, Reaktorin, henkilöstön käsitysten perusteella organisaatiossa ylläpidetään tietoisesti vahvaa kyberturvallisuuskulttuuria. Reaktorin organisaatio- ja kyberturvallisuuskulttuurit perustuvat myös suomalaiselle kansalliselle kulttuurille ja asiantuntijuudelle ominaisille piirteille. Reaktorin toimintaan ja kyberturvallisuuskulttuuriin vaikuttaa organisaation painotus tietotekniselle alalle, mikä näkyy henkilöstön keskimääräistä korkeammassa teknisessä osaamisessa ja sitä kautta myös kyberturvallisuuden sekä -uhkien ymmärtämisessä. Kyberturvallisuutta ylläpidetään tietoisesti osana henkilöstön ratkaisuja ja organisaation liiketoimintaa. Yrityksen kyberturvallisuuskulttuurin ominaispiirteet ja ratkaisut ovat myös laajalti yhteneviä lukuisten tietoturvaa sekä turvallisuus- ja tietoturvakulttuuria koskevien tieteellisten ja toiminnallisten tutkimusten löydösten ja hyvien käytänteiden kanssa.

Reaktorin kyberturvallisuuskulttuurin muodostumiseen vaikuttaviksi keskeisiksi tekijöiksi haastatteluaineiston perusteella nousivat yksilöiden tieto, osaaminen ja ymmärrys, organisaatiokulttuuri, tiimit ja organisaation rakenteet. Reaktorilla kyberturvallisuus on organisaation työntekijöiden jaettu vastuu. Tiimit jakavat vastuun myös kyberturvallisuuden huomioimisesta projekteissa yhtenä

toiminnan osa-alueena, jossa ratkaisut valitaan tietoisesti projektin vaatimusten ja käytettävyyden perusteella. Yksilöiden sosiaaliset verkostot toimivat kyberturvallisuutta uhkaavan tiedon ja käytänteiden jakamisessa sekä tiedottamisessa.

Kun keskeisin toimija on ihminen, niin inhimillisten virheiden olemassaolo ja mahdollisuus tunnustetaan realiteetiksi. Yksilöllä on moraalinen vastuu yhteisöä kohtaan, mikä yhdessä Reaktorin positiivisen ilmapiirin kanssa lisää halua toimia kyberturvallisuutta ylläpitävällä tavalla. Havaitut virheet ja epäonnistumiset käsitellään, jolloin toiminnan ja seurausten suhde hahmottuu sekä kyberturvallisuuteen liittyvä käyttäytyminen voi muuttua. Poikkeamista tai havainnoista tiedotetaan henkilöstöä, jotta koko organisaatio voi oppia ja muistutetaan erilaisten uhkien olemassaolosta. Henkilöstö tietää roolinsa kyberturvallisuuden ylläpitämisessä ja kehittää osaamistaan. Organisaatio puuttuu aktiivisesti kyberturvallisuutta koskevaan toimintaan ja toimintatapoihin. Osaamisen ja toiminnan jatkuva kehittäminen tunnistetaan organisaation toimintaedellytysten ja kyberturvallisuuden ylläpitämisen edellytykseksi.

Reaktorin kaltaisessa luottamukseen sekä yksilön ja tiimin toiminnanvapauteen perustuvassa organisaatiossa yksittäisen henkilön välinpitämättömyys, osaamattomuus tai ymmärtämättömyys voi muodostaa riskin organisaation kyberturvallisuudelle. Reaktorilla käynnissä oleva organisaation kasvu voi myös haastaa osan nykyisistä toimintamalleista ja lisääntynyt julkisuus voi kasvattaa yritykseen kohdistuvien uhkien määrää. Yrityksen laajeneminen muiden kansallisten kulttuurien vaikutuspiiriin voi luoda haasteita organisaation eri osien yhteistoiminnalle ja ainakin Suomen toimipisteessä käytössä olevan organisaatiomallin soveltuvuudelle muihin toimipisteisiin, koska kulttuureille ominaisissa toimintatavoissa on eroavaisuuksia.

Reaktorin ratkaisu ylläpitää yksilöiden aktiivisuuteen ja luottamukseen perustuvaa organisaatiokulttuuria vastaa alkuperäisen tutkimusongelman, käyttäjien kautta toteutettujen hyökkäysten vähentämisen, lisäksi inhimillisten virheiden vähentämiseen myös yrityksen toiminnan muilla osa-alueilla. Organisaatiokulttuurin keskiössä ovat tietoisten ratkaisujen toteuttaminen, organisaation jatkuva oppiminen, tiedon jakaminen ja inhimillisten virheiden välttäminen, joilla ylläpidetään korkeaa tasoa esimerkiksi järjestelmien toimivuudessa ja tietosuojan huomioimisessa.

LÄHTEET

Aira, A. (2012). Toimiva yhteistyö: Työelämän vuorovaikutussuhteet, tiimit ja verkostot. Jyväskylä: University of Jyväskylä.

Ahonen, S. (1994). Fenomenografinen tutkimus. Teoksessa Syrjälä, L., Ahonen, S., Syrjäläinen, E., & Saari, S. (toim.) Laadullisen tutkimuksen työtapoja. Helsinki: Kirjayhtymä.

Alasuutari, P. (2011). Laadullinen tutkimus 2.0. 4. uudistettu painos. Tampere: Vastapaino, 2011.

Alsop, G. & Tompsett, C. (2006). Making sense of 'pure' phenomenography in information and communication technology in education. Research in Learning Technology Vol. 14, No. 3, September 2006, pp. 241–259.

Ashworth, P. & Lucas, U. (2000). Achieving empathy and engagement: a practical approach to the design, conduct and reporting of phenomenographic research. Studies of Higher Education 25 (3), 295-309.

Bandura, A. (1982). Self-efficacy mechanism in human agency. American Psychologist, 37(2), 122–147.

Bandura, A. (1986). Social Foundations of Thought and Action: A Social Cognitive View. Academy of Management Review, 12(1), 169– 171.

Bandura, A. (1997). Self-efficacy: The exercise of control. New York, NY: Freeman.

Barry, H., Child, I., & Bacon, M. (1959). Relation of child training to subsistence economy. American Anthropologist, 61, 51-63.

Bartels, R. (1967). A Model for Ethics in Marketing. Journal of Marketing. New York Vol. 31, 20.

Berry, J. W. (2008). Globalization and acculturation. International Journal Intercultural Relations, 32 (4) (2008), pp. 328-336.

Boeije, H. (2010). Analysis in qualitative research. Thousand Oaks: Sage publications, 2010.

Chen, Y. & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors: polycontextual contrasts between the United States and China. MIS Quar-terly Vol. 40, No. 1, pp. 205-222.

Choi, M. S., Levy, Y. & Hovav, A. (2013). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse.

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

Costa, P. T., & MacCrae, R. R. (1992). Revised NEO personality inventory (NEO PI-R) and NEO five-factor inventory (NEO-FFI): Professional manual. Psychological Assessment Resources, Incorporated.

Cronan, T. P., Foltz, C. B. & Jones T. W. (2006). Piracy, computer crime and IS misuse at the University. Communications of the ACM. Volume 49, No. 6.

Cross, S. E. and Madson, L. (1997). Models of the Self: Self-Construals and Gender. Psychological Bulletin. Issue: Volume 122(1), Pages 5–37.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32 (1) (2013), pp. 90-101.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.

D'Arcy, J. & Lowry, P. B. (2019). Cognitive affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal. 2019; 29: 43–69.

Da Veiga, A. & Eloff, J. H. P. (2010). A framework and assessment instrument for Information Security Culture. Computer Security, vol. 2010, no. 29, pp. 196-207.

Da Veiga, A. & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security. 49.

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.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I. and Colautti, C. (2006). Privacy calculus model in e-commerce – a study of Italy and the United States, European Journal of Information Systems, 15:4, 389-402.

Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009). User behaviour towards protective in-formation technologies: the role of national cultural differences. Info Systems Jour-nal, Volume 19, Pages 391–412.

Echt, K. V., Morrell, R. W., & Park, D. C. (1998). Effects of age and training formats on basic computer skill acquisition in older adults. Educational Gerontology, 24(1), 3–25.

Entwhistle, N. (1997). Phenomenography in higher education. In Higher Education Research and Development, 16, 127-134. Centre for Research on Learning and Instruction. University of Edinburgh.

Eskola, J. & Suoranta, J. (1998). Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

European Union Agency for Cybersecurity (Enisa). (2016). Definition of Cybersecurity - Gaps and overlaps in standardisation. Haettu 24.11.2018 osoitteesta: https://www.enisa.europa.eu/publications/definition-of-cybersecurity

European Union Agency for Cybersecurity (Enisa). (2017). Cyber Security Culture in organisations. Haettu 24.11.2018 osoitteesta: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

European Union Agency for Cybersecurity (Enisa). (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. Haettu 21.4.2019 osoitteesta: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

Galvez, S. M. (2015). Identifying factors that influence individual information security practices at work. Faculty of Business Administration. Trident University International. Cypress, California.

Gonzalez, J. & Sawicka, A. (2002). "A framework for human factors in information security": WSEAS International Conference on Information Security, Rio de Janeiro.

Greene, G. & D'Arcy J. (2010). Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance. 5th Annual Sympo-sium on Information Assurance (ASIA-2010).

Guzman, I. R., Stam, K. R. & Stanton, J. M. (2008). The Occupational Culture of IS/IT Personnel within Organizations. The DATA BASE for Advances in Information Systems, Volume 39, Number 1.

Halevi, T., Memon, N., Lewis, J. & Kumaguru, P., Arora, S., Dagar, N., Aloul, F. & Chen, J. (2016). Cultural and Psychological Factors in Cybersecurity. 18th ACM International Conference of Information Integration and Web-based Applications & Servics (IIWAS), Singapore.

Hall, E. T. (1976). Beyond culture. Anchor Press/Doubleday, New York.

Hall E. T. (1981).The Silent Language. Anchor Books/Random House Inc., New York.

Hall, E. T. (2000). Context and meaning. In L. A. Samovar & R. E. Porter (Eds.), Intercultural Communication: A Reader, 9th ed., pp. 34-43, Belmont, CA: Wadsworth Publishing Co.

Hall, E., & Hall, M. (1990). Understanding cultural differences: Germans, French and Americans. Yarmouth: Intercultural Press.

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. P. (2011). Value conflicts for information security management. Journal of Strategic Information Systems. 20, Pages 373-384.

High-Level Experts Group (HLEG). (2008). ITU Global Cybersecurity Agenda High-Level Experts Group (HLEG) Global Strategic Report, Geneva, haettu 25.4.2019 osoitteesta: www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2007). Tutki ja kirjoita. (13. uud. painos). Helsinki: Tammi.

Hirsjärvi, S. & Hurme, H. (2008). Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus Helsinki University Press.

Hofstede, G. (1980). Culture's Consequences: International differences in work related values. Beverly Hill, CA, Sage.

Hofstede, G., Neuijen, B., Ohayv, D. D., & Sanders, G. (1990). Measuring Organizational Cultures: A Qualitative and Quantitative Study across Twenty Cases. Administrative Science Quarterly, 35(2), 286–316. Hofstede, G. (1993). Cultural constraints in management theories. The Academy of Management Executive, 7(1), 81-94.

Hofstede, G. (1991). Cultures and organizations: software of the mind. London: McGraw-Hill.

Hofstede, G., Hofstede, G. J., & Minkov, M. (2010). Cultures and organisations-software of the mind: intercultural cooperation and its importance for survival (3rd ed.): McGraw-Hill. New York, NY.

Hovav, A. & D'Arcy, J. (2012) Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the U.S. and South Korea. Information and Management, Volume 49, Pages 99–110.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. European Journal of Infor-mation Systems, 18, 140-150.

Huusko, M., & Paloniemi, S. (2006). Fenomenografia laadullisena tutkimussuuntauksena kasvatustieteissä. Kasvatus, 37(2), 162–173.

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In J. Ryan (Ed.), Leading Issues in Information Warfare & Security Research (pp. 80-106). Reading, UK: Academic Publishing International Limited.

Häkkinen, K. (1996). Fenomenografisen tutkimuksen juuria etsimässä. Teoreettinen katsaus fenomenografisen tutkimuksen lähtökohtiin. Jyväskylän yliopisto. Opettajankoulutuslaitos. Opetuksen perusteita ja käytänteitä 21.

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC). (2012). International Standard ISO/IEC 27032: Information Technology – Security Techniques – Guidelines for Cybersecurity, vol. 2012.

Johnson, J. & Rowlands, T. (2012). The interpersonal dynamics of in-depth interviewing. In Gubrium, J. F., Holstein, J. A., Marvasti, A. B., & McKinney, K. D. The SAGE handbook of interview research: The complexity of the craft (pp. 99-114). Thousand Oaks, CA: SAGE Publications, Inc.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. MIS Quarterly, 39(1), 113–134.

Jones, M. (2007). Hofstede - Culturally questionable?. Faculty of Commerce - Papers. University of Wollongong, Australia.

Karahanna, E., Evaristo, R. & Srite, M. (2005). Levels of Culture and Individual Behavior: An Integrative Perspective. Journal of Global Information Management (13:2), pp. 1-19.

Kearney, P. (2010). Security: The Human Factor. Cambridgeshire: IT Governance Pub-lishing.

Kluckhohn, C. (1951). Values and value-orientations in the theory of action: an exploration in definition and classification. Harper & Row, New York.

Knapp, K., Morris, R. E., Marshall, T. & Byrd, T. (2009). Information security policy: An organizational-level process model. Computers & Security. 28. 493-508. 10.1016/j.cose.2009.07.001.

Kolkowska, E. (2011). Security subcultures in an organization – exploring value conflicts. ECIS 2011 Proceedings. 237.

Krombholz, K., Hobel, H., Huber, M. & Weippl, E. (2014). Advanced Social Engineering Attacks. SBA Research, Vienna.

Krumov, K., & Larsen, K. S. (2013). Cross-cultural Psychology : Why Culture Matters. Charlotte, NC: Information Age Publishing.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, 37(12), 1049–1092.

Lewis, R. D. (2005). Finland, cultural lone wolf. Yarmouth, ME: Intercultural Press.

Lewis, R. D. (2006). When cultures collide. Boston: Nicholas Brealey.

Lincoln, Y. S. (1985). Naturalistic inquiry. SAGE.

Markus, H. & Kitayama, S. (1991). Culture and the Self: Implications for Cognition, Emotion, and Motivation. Psychological Review 1991, Vol. 98, No. 2, 224-253.

Marton, F. (1981). Phenomenography: Describing Conceptions of the World around Us. Instructional Science, 10, 177–200.

Marton, F. (1986). Phenomenography- A research approach to investigating different understandings of reality. Journal of Thought, 21(3), 28-49. Re-printed 1988 in R. R. Sherman & W, B. Webb (Eds.), Qualitative research in education: Focus and methods (pp. 141-161). London: Falmer Press.

Marton, F. & Booth, S. (1997). Learning and awareness. Mahwah, NJ: Lawrence Erlbaum Associates.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. & Pattinson, M. (2017). Individual differences and Information Security Awareness, Computers in Human Behavior, Volume 69, 2017, Pages 151-156.

McSweeney, B. (2000). The Fallacy of National Culture Identification. 6th Interdisciplinary Perspectives on Accounting Conference, Manchester, UK.

Metalidou, E., Marinagic, C., Trivellasc, P., Eberhagen, N., Skourlasd, C. & Gianna-kopoulosa, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, Volume 147, Pages 424 – 428.

Metsämuuronen, J. (2011). Tutkimuksen tekemisen perusteet ihmistieteissä: E-kirja opiskelijalaitos. Helsinki: International Methelp, Booky.fi.

Minkov, M. (2011). Cultural Differencies in a Globalizing World. Great Britain: Emerald Group Publishing Limited.

Mishra, S. & Dhillon, G. (2006). Developing Theoretical Base for Studying Governance: The Case of Information Security. Paper presented at the Web 2006 - International Conference on Information System.

Nelson, R. E., & Gopalan, S. (2003). Do Organizational Cultures Replicate National Cultures? Isomorphism, Rejection and Reciprocal Opposition in the Corporate Values of Three Countries. Organization Studies, 24(7), 1115–1151.

Niikko, A. (2003). Fenomenografia kasvatustieteellisessä tutkimuksessa. [Joensuu]: Joensuun yliopisto.

Nisbett, R. & Masuda, T. (2003). Culture and point of view. Proceedings of the National Academy of Sciences.

Nishimura, S., Nevgi, A. & Tella, S. (2008). Communication Style and Cultural Features in High/Low Context Communication Cultures: A Case Study of Finland, Japan and India. Teoksessa A. Kallioniemi (toim.), Uudistuva ja kehittyvä ainedidaktiikka. Ainedidaktinen symposiumi 8.2.2008 Helsingissä. Osa 2 (ss. 783–796). Helsingin yliopisto.

Parker, M. (2000). Organizational culture and identity: Unity and division at work. London: SAGE.

Paternoster, R., Bachman, R., Bushway, S., Kerrison, E., & O'Connell, D. (2015). Human agency and explanations of criminal desistance: Arguments for a rational choice theory. Journal of Developmental and Life-Course Criminology, 209–235.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31, 597-611.

Potter, J. & Hepburn, A. (2012). Eight challenges for interview researchers. In Gubrium, J. F., Holstein, J. A., Marvasti, A. B., & McKinney, K. D. The SAGE handbook of interview research: The complexity of the craft (pp. 555-570). Thousand Oaks, CA: SAGE Publications, Inc.

Rauscher, K. F. & Yashenko, V. (Eds.), Critical Terminology Foundations, EastWest Institute: London, 2011.

Reid, R. & van Niekerk, J. (2014). From Information Security to Cyber Security Cultures Organizations to Societies. Conference: Information Security South Africa (ISSA). Johannesburg, South Africa.

Rocha Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, Volume 43, June 2014, Pages 90-110.

Rokeach, M. (1973). The nature of human values. New York: Free Press.

Ross, L., Nisbett, R., & Gladwell, M. (2011). The Person and the Situation: Perspectives of Social Psychology. Pinter & Martin, London.

Ruusuvuori, J. & Tiittula, L. (2005). Haastatelu – Tutkimus, tilanteet ja vuorovaikutus. Vastapaino. Tampere.

Saarinen, M. (2018). Social network fragmentation in a team based organisation. Diplomityö, Aalto yliopisto.

Safa N. S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, Volume 56, pp. 70-82.

Schein, E. H. (1985). Organizational Culture and Leadership. San Francisco: Jossey-Bass.

Schein, E. H. & Schneier, P. (2017). Organizational Culture and Leadership. 5th edition. The Jossey-Bass Business and Management Series. John Wiley & Sons, Incorporated.

Schein, E. (1999). The corporate culture survival guide. Jossey-Bass Publishers, San Francisco.

Schlienger, T. & Teufel, S. (2002). Information Security Culture - The SocioCultural Dimension in Information Security Management. Security in the information society: visions and perspectives. IFIP TC11 International Conference on Information Security (Sec 2002), pp. 191–201.

Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & Security, Volume 21, Issue 6, 2002, Pages 526-531, ISSN 0167-4048.

Selmer, J., & De Leon, C. (1996). Parent Cultural Control Through Organizational Acculturation: HCN Employees Learning New Work Values in Foreign Business Subsidiaries. Journal of Organizational Behavior, 17, 557-572.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information and Management, 51(2), 217–224.

Smircich, L. (1983). Concepts of culture and organizational analysis. Administrative Science Quarterly, 28(3), 339–358.

Sommestadt, T., Hallberg, J., Lundholm, K. & Bengtsson, J. (2012). Variables influencing information security policy compliance A systematic review of quantita-tive studies. Swedish Defence Research Agency (FOI), Linkoping, Sweden.

Sowell, T. (2007). A Conflict of Visions: Ideological Origins of Political Struggles. Basic Books. New York.

Corbin, J. M. & Strauss, A. L. (2008). Basics of qualitative research: Techniques and procedures for developing grounded theory (3e [ed.].). Los Angeles, [Calif.] ; London: SAGE.

Torkzadeh, G., & Lee, J. (2003). Measures of perceived end-user computing skills. Information & Management, 40 (7), 607-615.

Trice, H. & Beyer, J. M. (1993). The Culture of Work Organizations. New York, Englewood Cliffs, NJ: Prentice-Hall.

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Turvallisuuskomitea. (2013). Suomen kyberturvallisuustrategia. Haettu 24.11.2018 osoitteesta: http://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/

Uljens, M. (1989). Fenomenografi – forskning om uppfattningar. Lund: Studentlitteratur.

Uljens, M. (1992). Phenomenological features of phenomenography (Report no 1992:03). Göteborg: University of Göteborg, Department of Education and Educational Research. 160 p.

Van Niekerk, J. & Von Solms, R. (2010). Information security culture: A management perspective. Computer Security, vol. 29, no. 4, pp. 476–486, June.

Van Niekerk, J. & Von Solms, R. (2006). Understanding Information Security Culture: A Conceptual Framework. Conference: Proceedings of the ISSA 2006 from Insight to Foresight Conference. Sandton, South Africa.

Verizon. (2018). Data Breach Investigations Report. Haettu 19.11.2018 osoitteesta: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Von Solms, R. (2000). Information security - the third wave? Computers & Security, 19(7), 615–620.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

Walsham, G. (2002). Cross-cultural software production and use: A structurational analysis. MIS Quarterly, 26(4), 359-380.

Wang, J. & Yan, Y. (2012). The interview question. In Gubrium, J. F., Holstein, J. A., Marvasti, A. B., & McKinney, K. D. The SAGE handbook of interview research: The complexity of the craft (pp. 231-242). Thousand Oaks, CA: SAGE Publications, Inc.

Wash, R., Rader, E. & Fennell, C. (2017). Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures**.** CHI 2017. Denver, CO.

Wenestam, C-G. (1984). Hur vi skapar mening I det vi erfar – en introduktion. Teoksessa Marton, F. & Wenestam, G-C. (toim.) Att uppfatta sin omvärld. Varför vi förstår verkligheten på olika sätt. Kristianstaf: AWE: Gebers, 17-51.

Wilson, M. & Hash, J. (2003). Computer Security: Building an Information Technology Security Awareness and Training Program. Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8933.

LIITE 1 HAASTATTELULOMAKE

Janne Kastepohjan pro gradun empiirisen vaiheen, teemahaastattelujen, toteutus

Haastattelun toteutus

1. Kysyn perustiedot vasta haastattelun lopussa, ettei vaikuta haastateltavien ajatuksiin
    a. Ikä, tehtävä, koulutus ja kauanko on ollut töissä yrityksessä
2. Motivointi ja tarkoitus, tietojen käsittely, tietosuoja ja anonymiteetti
    a. Kyberturvallisuuteen liittyen tekisi itsekin välillä mieli kaunistella asioita, koska aina ei tule toimittua oikein kiireen, raskaiden toimintatapojen tai väsymyksen vuoksi. Haastattelussa tärkeintä on kuitenkin olla rehellinen niin hyvässä kuin pahassa, koska
        i. yritys saa tietoa työntekijöiden käsityksistä ja voi hyödyntää havaintoja turvallisuuteen liittyvien toimintatapojen muuttamiseen.
        ii. Tutkimuksen käyttöarvo ja luotettavuus
    b. Vastaamisessa ei tule pyrkiä miellyttämään tutkijaa tai vastaamaan niin kuin tietää olevan ”oikein” tai oikea toimintatapa, vaan kertoa mahdollisimman totuudenmukaisesti mielipiteensä tai käsityksensä.
    c. Ei ole oikeita tai vääriä vastauksia, vaan näkemyksiä ja kokemuksia.
    d. Vastaajien vastauksia ei erotella tutkimuksessa niin että niiden perusteella pystyy yhdistämään vastauksia yksittäiseen henkilöön vaan kaikki pseudonymisoidaan.
    e. Tiedot tulevat vain tutkimuskäyttöön ja säilytetään huolellisesti salatulla muistitikulla
3. Haastattelun toteutus ja kulku
    a. Haastateltava pohtii ja tutkija kysyy tarvittaessa tarkentavia kysymyksiä.
    b. Tutkimusmenetelmässä tärkeintä on pohdinta, vuorovaikutus ja dialogi sekä haastateltavan käsitykset ja mihin ne perustuvat.
    c. Haastattelu toteutetaan teemoittain
        i. Haastateltavan tausta sekä häneen vaikuttaneet kulttuurit ja tekijät
        ii. Henkilökohtainen kyberturvallisuuskulttuuri
        iii. Organisaatiokulttuuri
        iv. Organisaation kyberturvallisuuskulttuuri
    d. Teemat ovat haastateltavien nähtävillä koko ajan pohdinnan helpottamiseksi
4. Kannustus vapaaseen puheeseen ja pohdintaan.
    a. Luodaan rento ilmapiiri pyrkimällä saamaan aikaan luottamussuhde haastateltavaan.
    b. Tutkija pitää huolta, että kaikki asiat tulee käsiteltyä, jolloin haastateltava voi keskittyä pohtimiseen.
    c. Pyritään välttämään teoreettisten tai vaikeiden termien käyttämistä vaan operationalisoidaan termit eli kysytään yksinkertaisia kysymyksiä ja saadaan haastateltavat pohtimaan käsityksiään.
5. Onko kysymyksiä ennen haastattelun aloittamista?
6. Voin haastattelun lopussa kertoa tutkimuksesta ja teoriasta enemmän, koska en halua sen vaikuttavan pohdintaan tai antavan alitajuista kuvaa siitä millaiset vastaukset ovat toivottuja.

Haastattelun teemat

1. Haastateltavan tausta sekä häneen vaikuttaneet kulttuurit ja tekijät
2. Henkilökohtainen kyberturvallisuuskulttuuri
3. Organisaatiokulttuuri
4. Organisaation kyberturvallisuuskulttuuri

Haastattelukysymykset

1) Haastateltavan käsitysten tausta sekä häneen vaikuttaneet kulttuurit ja tekijät
    a. Millainen on henkilökohtainen arvomaailmasi? Millaisia arvoja sinulla on?
    b. Millaisessa kulttuuritaustassa olet kasvanut?
    c. Vaikuttaako tai onko joku vahva uskonnollinen, etninen tai paikallinen kulttuuri vaikuttanut sinuun?
    d. Miten arvot vaikuttavat toimintaasi?
2) Henkilökohtainen kyberturvallisuuskulttuuri
    a. Mitä on kyberturvallisuus ja mitä siihen kuuluu henkilökohtaisella tasolla?
        i. Minkälaisia uhkia sinuun kohdistuu?
        ii. Mitä toimenpiteitä olet tehnyt niiltä suojautumiseksi?
    b. Millainen on henkilökohtainen asenteesi koskien kyberturvallisuutta?
    c. Mitkä asiat asenteeseesi vaikuttavat?
        i. Esimerkiksi tekninen osaaminen, koulutus, opiskelu, uutiset, organisaation tuki, henkilökohtaiset tai lähipiirin kokemukset?
    d. Koetko itsesi varmaksi tieto- ja viestintätekniikan käytössä?
    e. Minkä verran kiinnität huomiota henkilökohtaisessa elämässäsi tietoturvaan ja -suojaan?
        i. Miten se ilmenee käytännössä?

3) Kohdeyrityksen organisaatiokulttuuri
    a. Oletko lähtökohtaisesti tyytyväinen työpaikkaasi ja työtehtävääsi?
    b. Koetko yleensä, että sinua arvostetaan ja sinuun luotetaan?
    c. Millainen organisaatiokulttuuri työpaikallasi on eli ”miten asiat tehdään”? Esimerkiksi tietyt toimintatavat tai arvot?
        i. Hierarkkisuus, aloitteellisuus, luottamus, päätöksenteko, johtajan rooli yms.
    d. Miten organisaatiokulttuuri näkyy työpaikallasi?
    e. Mitä näkymättömiä rakenteita on?
    f. Miten organisaatiokulttuuri vaikuttaa sinuun?
    g. Miten uusi työntekijä oppii organisaationne kulttuurin?
        i. Ohjeistukset, säännöt, strategiat, mallin ottaminen, prosessit?
    h. Toimitko eri tavalla töissä kuin vapaa-ajalla?
        i. Onko yrityksen organisaatiokulttuuri muuttanut sinua ihmisenä?
        ii. Onko työpaikan organisaatiokulttuuri vaikuttanut henkilökohtaisen elämäsi arvoihin tai toimintatapoihin?
    i. Mistä tiedät, miten sinun kuuluu toimia eri tilanteissa?
    j. Millaisia yleisesti turvallisuutta ja kyberturvallisuutta koskevia arvoja on ja miten ne ilmenevät?

        i. Esim. luottamus, selkeys, ihminen on turvallisuutta edistävä tekijä eikä riski
    k. Onko organisaatiosi kulttuuri yhtenäinen vai onko siinä erilaisia paikallisia kulttuureja ja ryhmiä, joilla on oma kulttuurinsa?

4) Yrityksen kyberturvallisuuskulttuuri
    a. Miten organisaatiosi kyberturvallisuus on organisoitu?
        i. Kuka siitä vastaa ja ketkä kaikki siihen osallistuvat?
        ii. Onko se selkeästi roolitettu ja toimiiko se?
        iii. Mikä on sinun roolisi ja tehtäväsi organisaation turvallisuusasioissa?
        iv. Miten turvallisuutta johdetaan?
    b. Tukevatko työvälineet, ohjelmistot ja toimintatavat turvallisia toimintatapoja?
    c. Miten organisaatiossa puututaan turvallisuuteen liittyviin ongelmiin?
    d. Saatko riittävästi tietoa uusista organisaatioon kohdistuvista turvallisuusriskeistä?
    e. Osaatko toimia havaitessasi tietoturvapoikkeaman?
        i. Ovatko ohjeet riittävän selkeät ja kattavat? Ovatko ne saatavilla?
        ii. Oletko saanut riittävästi koulutusta?
        iii. Tiedätkö mistä saat tukea?
    f. Mikä on organisaatiosi suhtautuminen turvallisuus-/tietoturvapoikkeamiin?
    g. Miltä sinusta tuntuu ajatus tietoturvapoikkeamasta ilmoittamisesta?
    h. Vaihteleeko mielestäsi ihmisten suhtautuminen ja toiminta suhteessa kyberturvallisuuteen?
        i. Jos, niin arvelet sen johtuvan?
    i. Mitkä asiat mielestäsi heikentävät kyberturvallisuutta organisaatiossasi?
    j. Miten mielestäni organisaatiosi kyberturvallisuutta tai kyberturvallisuuskulttuuria voitaisiin kehittää?