Krista Karusalmi

KYBERTURVALLISUUSKULTTUURI AMMATTILIITOISSA JA SEN VAIKUTUKSET ARKALUONTEISEN TIEDON SUOJAAMISEEN

Opinnäytetyö

Tekniikan ylempi ammattikorkeakoulututkinto

Kyberturvallisuuden koulutus

2025

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (ylempi AMK)
Tekijä	Krista Karusalmi
Työn nimi	Kyberturvallisuuskulttuuri ammattiliitoissa ja sen vaikutukset arkaluonteisen tiedon suojaamiseen
Toimeksiantaja	Suomen Ekonomit
Vuosi	2025
Sivut	107 sivua, liitteitä 10 sivua
Työn ohjaaja	Jarkko Hänninen

TIIVISTELMÄ

Tämä opinnäytetyö tarkastelee ammattiliittojen kyberturvallisuuskäytäntöjä, niiden kehitykseen vaikuttavia tekijöitä sekä haasteita, jotka voivat estää turvallisuuskulttuurin vahvistumista. Tavoitteena oli laatia käytännönläheinen opas, jonka avulla kyberturvallisuuskulttuuria voi kehittää. Ammattiliitot käsittelevät arkaluonteisia jäsentietoja, mikä korostaa kyberturvallisuuskulttuurin merkitystä.

Tutkimus toteutettiin kehittämistutkimuksena, jossa analysoitiin kyselyaineistoa Akavalaisten liittojen tietosuojaverkostosta sekä aiempaa tutkimusta kyberturvallisuudesta ja organisaatiokulttuurista.

Tulosten mukaan kyberturvallisuus ymmärretään tärkeäksi ja johto on pääosin sitoutunut sen edistämiseen. Haasteet liittyvät käytännön toteutukseen: osaamisen, resurssien ja koulutuksen puute sekä epäselvät vastuut ovat merkittävimpiä esteitä kyberturvallisuuskulttuurin vahvistamisessa. Monissa liitoissa vastuut ovat hajanaisia, mikä vaikeuttaa toiminnan kehittämistä, kyberturvallisuuskulttuurin juurtumista ja mm. poikkeamien havaitsemista ja hallintaa.

Tutkimus vahvistaa aiempien tutkimusten havaintoja siitä, että kyberturvallisuuskulttuuri kehittyy johdon tuella, jatkuvalla koulutuksella ja selkeillä toimintaperiaatteilla. Kyberturvallisuuskulttuuri koostuu näkyvistä käytännöistä, jaetuista arvoista ja syvälle juurtuneista uskomuksista, jotka ohjaavat organisaation toimintaa kyberuhkien torjumisessa. Kyberturvallisuuskulttuuri ei ole staattinen tila, vaan se vaatii jatkuvaa kehittämistä vastaamaan muuttuvia uhkia.

Johtopäätöksenä voidaan todeta, että ammattiliitoilla on merkittävä mahdollisuus vahvistaa kyberturvallisuuskulttuuriaan. Se kuitenkin edellyttää selkeää strategiaa, riittäviä resursseja ja säännöllistä koulutusta. Kyberturvallisuuden vahvistaminen ei voi jäädä yksittäisten asiantuntijoiden vastuulle vaan sen tulee olla osa koko organisaation toimintaa ja kulttuuria. Kun henkilöstö saa riittävät työkalut ja koulutuksen, ihmisestä voi tulla organisaation vahvin lenkki kyberuhkien torjunnassa.

Opinnäytetyössä laadittu koulutuspaketti tarjoaa yhden konkreettisen työkalun kyberturvallisuuskulttuurin vahvistamiseen. Sen avulla organisaatiot voivat selkeyttää vastuita, kasvattaa osaamista ja rakentaa johdonmukaista strategiaa kyberturvallisuuden kehittämiseksi.

Asiasanat: ammattiliitot, järjestöt, kyberturvallisuus, organisaatiokulttuuri, tietosuoja, tietoturva

Kaakkois-Suomen ammattikorkeakoulu

Degree title	Master of Engineering
Author	Krista Karusalmi
Thesis title	Cybersecurity culture in labor unions and its impact on the protection of sensitive data
Commissioned by	The Business School Graduates in Finland
Time	2025
Pages	107 pages, 10 pages of appendices
Supervisor	Jarkko Hänninen

ABSTRACT

This thesis examined cybersecurity-related practices within labor unions, the key factors that influenced their development, and the challenges that may hinder the strengthening of the cybersecurity culture. The study aimed to produce a practical guide to support its development. Labor unions process sensitive member data, which highlights the importance of a strong cybersecurity culture.

The thesis was conducted as a constructive, design-based study, in which data were analyzed from a survey carried out within the data protection network of Akava-affiliated unions, alongside previous research on cybersecurity and organizational culture.

The findings indicate that cybersecurity is recognized as important, and that leadership is largely committed to its advancement. The main challenges lie in practical implementation: lack of expertise, resources, and training, as well as unclear responsibilities, are the most significant barriers to strengthening the cybersecurity culture. In many unions, responsibilities are fragmented, which complicates the development of practices, embedding cybersecurity culture, and the detection and management of security incidents.

The study confirms previous findings that cybersecurity culture develops through leadership support, continuous training, and clear operational principles. Cybersecurity culture consists of visible practices, shared values, and deeply rooted beliefs that guide an organization’s actions in preventing cyber threats. It is not a static state; it requires ongoing development and adaptation to address evolving threats.

In conclusion, labor unions have significant potential to strengthen their cybersecurity culture, but this requires a clear strategy, sufficient resources and regular training. Strengthening cybersecurity cannot be left solely to individual experts; it must be integrated into the organization’s overall operations and culture. When employees are provided with adequate tools and training, they can become the organization's strongest link in cybersecurity.

As part of this thesis, a practical training package was developed to help organizations strengthen their cybersecurity culture by clarifying responsibilities, enhancing employee skills, and supporting a consistent development strategy.

Keywords: associations, cyber security, data protection, data security, labor unions, organizational culture

SISÄLLYS

1 JOHDANTO

Organisaation työntekijä on tietoturvan heikoin lenkki. Ainakin, jos on uskominen tietoturvayhtiö Verizonen (2024, 8) ”2024 Data Breach Investigations Report” -julkaisua. Siinä todetaan, että ihminen on osallisena 68 %:ssa tietovuodoista, oli kyse sitten varastetuista käyttäjätunnuksista, tietojenkalastelusta, väärinkäytöksestä tai inhimillisestä virheestä. Trendi on onneksi laskeva, koska vastaava luku vuoden 2023 raportissa oli 74 % (Verizone 2023, 8) ja vuoden 2022 raportissa 82 % (Verizone 2022, 8).

Kyberturvallisuuskeskuksen (2024b, 30) ”Tietoturvan vuosi 2023” -raportin mukaan tietoturvapoikkeamien lukumäärä Suomessa vuonna 2022 oli noin 13 000 kpl. Vuonna 2023 poikkeamia ilmoitettiin lähes 19 000 kpl. Kasvua oli vuodessa yli 40 %, joka koostui huijausten, tietomurtoyritysten ja huijausviestien lisääntymisestä. Vuonna 2024 ilmoitukset pysyivät suurin piirtein samalla tasolla, poikkeamia raportoitin reilut 18 000 kpl (Kyberturvallisuuskeskus 2025). ”Kyberturvallisuuden vuosi 2024” -raportti (Kyberturvallisuuskeskus 2025) kertoo, että huomattavan suuri osa vuoden 2024 ilmoitetuista poikkeamista koskee huijauksia ja kalasteluyrityksiä. Edelleen raportin mukaan tietojenkalastelulla kaapatut kirjautumistunnukset ovat yksi rikollisten yleisimmistä keinoista tunkeutua organisaatioiden tietojärjestelmiin.

Kyberhyökkäykset lisääntyvät ja kehittyvät yhä nopeammiksi ja monimutkaisemmiksi. Kun organisaatiot vahvistavat tietoturvaansa, hyökkääjät hyödyntävät niiden heikkouksia. Erityisesti työntekijöiden alttiutta sosiaaliselle manipuloinnille ja järjestelmien puutteellisia turvamekanismeja hyödynnetään. Vuonna 2024 ääntä hyödyntävät kalastelukampanjat yleistyivät vuoden aikana 442 %. (CrowdStrike 2025, 9.)

Hyökkäykset ovat aiempaa kohdennetumpia ja räätälöidympiä. Erilaisten kyberuhkatoimijoiden kyvykkyydet ovat kehittyneet mm. helposti saatavilla olevien palveluiden ja automatisoinnin myötä. Eri tavoin motivoituneet uhkatoimijat hyödyntävät samoja haittaohjelmia ja kriittisiä haavoittuvuuksia. (Kyberturvallisuuskeskus 2024b, 8.) Generatiivinen tekoäly (GenAI) on yhä houkuttele-

vampi työkalu kyberrikollisille, sillä sen käyttö on helppoa ja se on laajasti saatavilla. Vuoden 2024 aikana hyökkääjät alkoivat hyödyntää GenAI:ta yhä enemmän, etenkin sosiaalisen manipuloinnin ja nopeiden informaatiovaikuttamiskampanjoiden tukena. (CrowdStrike 2025, 19.)

Kyberrikollisten tarkoituksena on päästä yrityksen järjestelmiin työntekijältä saadulla tiedolla. Kyberturvallisuuskeskuksen (2024b, 11) mukaan tietojenkalastelun yleisin toteutustapa on pankkitunnusten kalastelu. Toiseksi yleisin muoto on Microsoft M365 -tunnusten kalastelu. Työntekijän toiminta on siis yrityksen kannalta oleellista. Se, miten työntekijä kalasteluun reagoi, riippuu niin työntekijän valppaudesta kuin yrityksen käytännöistä, prosesseista ja koulutuksesta suhteessa kyberturvallisuuteen.

Se, että ihminen on heikoin lenkki, voidaan kääntää myös vahvuudeksi. Jos kyberturvallisuus nostetaan yrityksessä tärkeäksi asiaksi ja puhutaan sekä koulutetaan henkilökuntaa säännöllisesti, voidaan luoda ja kehittää kyberturvallisuuskulttuuri, joka on yrityksen vahvuus.

Kyberturvallisuuskulttuuri yrityksissä rakennetaan yhdessä. Verkko-operaattori DNA:n syksyllä 2024 julkaistussa ”Tietoturvatutkimus 2024” DNA:n yritysliiketoiminnan johtaja toteaa tulevaisuudesta osuvasti: ”Tekoälyn merkitys kasvaa, mutta avainasemassa tietoturvan toteutumisessa ovat ihmiset – ja näin tulee olemaan vielä pitkään. Vastuu on tälläkin alueella organisaatioiden johdolla: meidän tehtävämme on huolehtia siitä, että teknisen tietoturvan ohella myös osaaminen ja ymmärrys on kunnossa. Tietoturvakulttuuri luodaan yhdessä, ja se on meidän kaikkien tehtävä.” (DNA 2024, 3.)

Osaajapula on yrityksille valtava haaste: 67 % edellä mainitun tietoturvatutkimuksen vastaajista nimeää osaajapulan haasteeksi hyvän kyberturvan saavuttamisessa. Saman haasteen kanssa kamppailevat yritykset koosta riippumatta. Kukaan ei pärjää yksin, sillä jopa 89 % vastaajista ilmoittaa hyödyntävänsä kumppaneita tietoturvan ja kyberturvallisuuden saralla. Mitä pienempi yritys on, sitä enemmän palveluita ostetaan kumppaneilta. (DNA 2024, 5.)

Ammattiliiton tärkein suojattava omaisuus on liiton jäsenten jäsentiedot, joiden käsittelyyn jäsen on antanut suostumuksensa liittyessään jäseneksi. Jäsenrekisteriä suojataan teknisin ja hallinnollisin toimenpitein, joihin vaatimukset tulevat tietosuoja-asetuksesta. Jäsenrekisteriä käsittelevät kuitenkin ihmiset. Uhkana on mm. inhimilliseen erehdykseen pohjautuva vahinko, jonka vuoksi jäsentiedot saattavat vaarantua. Vahinko voi uhata jäsenrekisteriä välillisesti esimerkiksi tietojenkalastelun kautta. Kohteena oleva erityinen henkilötieto tekee vahingosta tietosuojalain näkökulmasta vakavamman. Kyberturvallisuuskulttuurin luominen ammattiliittoon ja peruskyberhygieniaosaamisen jalkauttaminen luonnolliseksi osaksi jokaisen työntekijän arkea on ensiarvoisen tärkeää. Vahva kulttuuri voi vähentää inhimillisten virheiden riskiä ja tehdä kyberturvallisuudesta organisaation yhteisen vahvuuden.

Tässä tutkimuksessa on tarkoitus kyselyllä selvittää, minkälainen kyberturvallisuuskulttuuri ammattiliitoilla on, mitkä ovat suurimmat haasteet tai esteet kyberturvallisuuskulttuurin kehittämiselle sekä luoda kyberturvallisuuskulttuurin koulutuspaketti ammattiliitoille.

Opinnäytetyön tilaajana on Suomen Ekonomit. Se on kauppatieteellisen yliopistotutkinnon suorittaneiden tai sitä opiskelevien ammattiliitto. Henkilöjäseniä on lähes 60 000. Tutkimus tehdään tilaajaorganisaatiolle, jossa työn tekijä toimii tietohallintopäällikkönä ja tietoturvavastaavana. Tutkimus on tarkoitus laatia niin, että sen tulokset ovat hyödynnettävissä muissakin ammattiliitoissa.

2 AIKAISEMMAT TUTKIMUKSET JA KIRJALLISUUSKATSAUS

Miten inhimillinen riski jäsentietojen menettämisen ympärillä voidaan kääntää uhkan sijasta vahvuudeksi, on tämän tutkimuksen liikkeelle sysäämä kysymys. Ongelman selvittämiseksi on perehdyttävä ensinnäkin organisaatiokulttuuriin, josta on kirjoitettu paljon teoksia. Muun muassa Panu Luukka on kirjoittanut vuonna 2019 laajan teoksen: ”Yrityskulttuuri on kuningas – Mikä, miksi ja miten?”. Siinä hahmotetaan, mikä yrityskulttuuri on, miten se muotoutuu ja miksi siihen kiinnittäminen on oleellisen tärkeää.

Toinen oleellinen viitekehykseen liittyvä aihealue on kyberturvallisuus. Kyberturvallisuuden tilasta tehdään vuosittain paljon tutkimuksia. Esimerkiksi

verkko-operaattori DNA julkaisi syksyllä tutkimuksen nimeltä ”Tietoturvatutkimus 2024 - Miltä kyberturvallisuuden kenttä näyttää suomalaisyritysten silmin?”. Tutkimukseen vastanneiden yritysten ICT-päättäjistä jopa 73 % ilmaisee huolensa Suomessa toimivien yritysten kyberturvallisuudesta. Huolenaiheita ovat muun muassa tietojen kalastelu, tietomurrot ja palvelunestohyökkäykset. (DNA 2024, 5.) Kansainvälisiä tutkimuksia kyberturvallisuuden tilasta vuosittain tekevät mm. tietoturvayhtiöt, kuten Verizone ja CrowdStrike. Verizonen ”2024 Data Breach Investigaton Report” (2024, 7) osoittaa, että haavoittuvuuksiin pohjautuvien hyökkäysten määrä lähes kolminkertaistui (180 %) vuodessa. CrowdStriken (2024, 2) vastaava raportti ”2024 Global Threat report” toteaa, että "riittävän hyvä" lähestymistapa kyberturvallisuuteen ei enää riitä vastaamaan nykypäivän uhkiin. Kun organisaatiot siirtävät liiketoimintaansa yhä enemmän pilveen, vastustajat kehittävät kykyjään hyödyntää tätä ja käyttää pilven erityispiirteitä hyväkseen. Raportin havaintojen mukaan identiteettiin perustuvat hyökkäykset ovat yhä keskeisemmässä roolissa. Näissä hyökkääjät keskittyvät sosiaalisen manipuloinnin hyökkäyksiin, jotta pääsevät kiertämään monivaiheisen tunnistautumisen.

Kyberturvallisuudesta käsitteenä on hyvin saatavilla teoksia eikä kansallinen aineisto häpeä kansainväliselle aineistolle. Vuonna 2014 Limnéll, Majewski ja Salminen kirjoittivat ”Kyberturvallisuus”-kirjan, joka onnistuneesti piirtää kuvaa digitaalisesta toimintaympäristöstämme haasteineen keskittyen kyberturvallisuustietoisuuden ja kokonaisturvallisuuden kasvattamiseen. Teos on säilyttänyt arvonsa tähän päivään asti. Pitkän linjan tietotekniikkakirjailija Petteri Järvinen on kirjoittanut mm. vuonna 2022 ”Yrityksen tietoturvaopas” -kirjan, joka toimii hyvänä perusteoksena niin pienelle organisaatiolle, kuin jokaiselle kansalaisellekin. Vuonna 2018 Järvinen kirjoitti ”Kyberuhkia ja somesotaa” -kirjan, joka nimensä mukaisesti keskittyy kyberajan sodankäynnin uhkiin. Kimmo Rouskun (2014) ”Kyberturvaopas – Tietoturvaa kotona ja työpaikoilla” käsittelee käytännönläheisesti tietoturvan ja kyberturvan vinkkejä henkilötasolla. ”Suomen kyberturvallisuusstrategia 2024–2025” (Paananen ym. 2024) on erinomainen lähde perehdyttäessä kansallisen kyberturvallisuuden kehittämiseen.

Kansallisesta kirjallisuudesta ei löydy lainkaan suoria tutkimuksia ammattiliittojen kyberturvallisuuden tilasta tai sen haasteista tai erityispiirteistä, jotka erityisten henkilötietoryhmien tietojen käsittely aiheuttaa. Finnan (Finna.fi) tutkimuskannasta haettuna sanalla ”kyberturvallisuus” löytyy tutkimuksia, jotka keskittyvät tietyn alan kyberturvallisuuteen tai niiden uhkiin tai kansallisen kyberturvallisuuden tilaan. Kyberturvallisuuden merkityksestä ammattiliitoille (hakusana: cyber security culture in labor unions) löytyy turkkilainen tutkimus vuodelta 2021 (Sevgi 2021), jossa pääpaino on ammattiliittojen kyberturvallisuusuhkien kasvussa, mikä johtuu sosiaalisen median ja internetin käytön yleistymisestä niiden toiminnassa.

Kolmas ja tärkein osa-alue on kyberturvallisuuskulttuuri. Kyberturvallisuuskulttuurin tutkimus pohjautuu tietoturvakulttuurin tutkimuksiin ja toisaalta organisaatiokulttuurin malleihin, joita on tutkittu kyberturvallisuuskulttuuria enemmän. Kansallisesti tutkimus pohjautuu pitkälti yksittäisen yrityksen kyberturvallisuuskulttuurin selvityksiin. Kansainvälisesti kyberturvallisuuskulttuuria (cyber security culture) on tutkinut mm. Ejigu ym. (2021), Bada ym. (2021), Da Veiga (2023, 2019) ja Tolah ym. (2021). Da Veiga (2023) on mm. nostanut luovuuden ja innovoinnin kyberturvallisuuskulttuurin rakentamisen keskiöön. Ejigun ym. (2021) “Investigating the Impact of Organizational Culture on Information Security Policy Compliance: The Case of Ethiopia” käsittelee sitä, miten kulttuurilliset tekijät vaikuttavat työntekijöiden halukkuuteen noudattaa tietoturvaohjeita. Bada ym. (2021) korostavat, että kyberturvallisuuskulttuurin ylläpito vaatii jatkuvaa kehittämistä eikä se ole staattinen tila. Huomionarvoista on, että pääosa kansainvälisestä kyberturvallisuuskulttuurin tutkimuksesta on tehty Etelä-Afrikan kontekstissa, jossa aktiivisena tutkijana on ollut tässäkin tutkimuksessa paljon viitattu Da Veiga. Yllättävän vähän on tutkimuksia koskien esimerkiksi Eurooppaa tai Pohjois-Amerikkaa.

Kyberturvallisuuskulttuurista on Suomessa viime vuosina tehty muutama pro gradu -työ liittyen joko yksittäisen yrityksen tai toimialan kyberturvallisuuskulttuuriin. Esimerkkinä Markus Savolaisen ”Kaikki tietää, että se on semmoinen villi länsi tuo netti vielä - Narratiivinen tutkimus kyberturvallisuuskulttuurista kaupungin hallinto-organisaatiossa” (2022). Lähinnä tämän tutkimuksen ai-

hetta on Janne Kastepohjan pro gradu -työ vuodelta 2020 aiheella ”Kyberturvallisuuskulttuuri – ohjelmistoyritys reaktorin ratkaisuja henkilöstön kautta kohdistuvien kyberuhkien vähentämiseksi”.

Yleinen kyberturvallisuuskulttuurin tutkimus on käyttökelpoinen niin ammattiliitoille kuin mille tahansa toimialalle. Joka tapauksessa on selvää, että kyberturvallisuuden alalla kansallisia tutkimuksia ihmisen käyttäytymisestä ja sen vaikutuksesta organisaation kyberturvallisuuteen on vain vähän ja niitä tarvitaan lisää. Myös kansainvälistä kyberturvallisuuskulttuurin tutkimusta mm. Euroopassa tarvitaan.

3 TUTKIMUSASETELMA

Tässä työssä tavoitteena on selvittää, minkälainen kyberturvallisuuskulttuuri ammattiliitoissa vallitsee, miten se vaikuttaa arkaluonteisen tiedon suojaamiseen ja miten kyberturvallisuuskulttuuria voisi kehittää. Tutkimusongelmana voidaan pitää sitä, että ammattiliittojen käytössä ei ole kyberturvallisuuskulttuurin yhtenäisiä käytäntöjä eikä koulutusta ja tämä vaikuttaa arkaluonteisen tiedon suojaamiseen.

3.1 Tutkimuskysymykset

Edellä mainitusta tutkimusongelmasta on johdettu seuraavat tutkimuskysymykset:

1. Mitä on kyberturvallisuuskulttuuri ja miten sitä kehitetään?
2. Minkälainen kyberturvallisuuskulttuuri ammattiliitoissa on?
3. Mitkä ovat suurimmat esteet ja haasteet kyberturvallisuuskulttuurin kehittämiselle ammattiliitoissa?

3.2 Tutkimusote

Tutkimuksen taustalla on ongelma, että ammattiliitoilla ei ole yhteneväisiä käytäntöjä liittyen kyberturvallisuuteen. Tutkimuksen tavoitteena on selvittää kyselyllä, minkälainen kyberturvallisuuskulttuuri ammattiliitoissa vallitsee ja tuottaa sen ja teorian pohjalta laajemmin hyödynnettävissä oleva ohjeistus kyberturvallisuuden vahvistamiseen.

Tutkimusote on näin ollen laadullisen ja määrällisen tutkimuksen väliin sijoittuva muutokseen pyrkivä (interventio) kehittämistutkimus. Kehittämistutkimuksen avulla luodaan ohjeistus/opas, jota testataan tilaajaorganisaatiossa, mutta samalla sen sovellettavuutta ja hyödyllisyyttä tarkastellaan muiden ammattiliittojen näkökulmasta. Tämä varmistaa, että opas on laajasti käyttökelpoinen useammille organisaatioille.

Kehittämistutkimuksessa on taustalla ilmiö, prosessi tai asiantila, jonka halutaan olevan kehittämisen tai muutoksen jälkeen paremmin (Kananen 2012, 13). Ongelman poistaminen edellyttää ongelman syiden löytämistä ja keinojen valintaa, jolla todettu ongelma poistetaan. Tässä piilee kehittämistutkimuksen ja perinteisen tutkimuksen (laadullinen ja määrällinen) välinen ero. Kehittämistutkimuksessa toteaminen ei riitä, sillä poistaminen vaatii myös toimintaa, joka johtaa toivottuun muutokseen. (Kananen 2012, 16.)

Tämän tutkimuksen tutkimusote on lähellä toimintatutkimusta. Toimintatutkimus on tapa tehdä tutkimusta siten, että siitä on käytännön hyötyä. Sen avulla pyritään aktiivisesti muuttamaan toiminnan tapoja eli sosiaalisia käytäntöjä parempaan suuntaan. (Heikkinen & Kaukko 2023.) Toimintatutkimuksen tavoitteena on, kuten konstruktiivisessa tutkimuksessakin, muutos, mutta muutoksen kohteena on usein ihmisten toiminta. Tutkija on itse mukana toiminnassa toteuttaakseen muutosprosessia. Ero on siis lähinnä siinä, onko tutkija itse mukana muutosprosessin toteuttamisessa vai ei. (Kananen 2017, 17.)

Rajanveto näiden välillä on hiuksenhieno ja tutkimuksessa on piirteitä molemmista. Kehittämistutkimus tutkimusotteena on perustellumpi tässä työssä siitä syystä, että lopputuloksena syntyisi käytännönläheinen ratkaisu, koulutuspaketti ammattiliitoille. Tässä työssä tutkija ei ole muutosprosessissa aktiivinen toimija vaan ulkopuolinen osallistuja toteuttaessaan ongelmaan ratkaisun, jonka ammattiliitot voivat ottaa käyttöönsä.

3.3 Rajaukset

Kulttuurin jalkauttaminen on hidasta. Näin ollen työssä ei ole tarkoitus validoida, paraneeko ammattiliittojen kyberturvallisuuskulttuuri tämän tutkimuksen

myötä. Tässä tutkimuksessa ei myöskään ole tarkoitus selvittää yksittäisen ammattiliiton kyberturvallisuuden tasoa.

3.4 Aineiston kerääminen ja tulosten analyysi

Kehittämistutkimus alkaa aina ongelma-analyysillä, jossa tavoitteena on analysoida kehittämisen tarpeet, mahdollisuudet ja haasteet (Pernaa 2013, 8). Todellisen ongelman löytäminen ja rajaaminen on ongelman ratkaisun kannalta erittäin tärkeää (Kananen 2017, 57).

Tutkimuksen empiirinen primääriaineisto kerättiin kyselylomakkeella, joka lähetettiin Akavalaisten liittojen yhteiselle tietosuojaverkostolle. Verkostoon kuuluu tietosuojavastaavia sekä tietoturvavastaavia tai niiden tehtävien kanssa jollain tavalla työtä tekeviä. Kyselyssä käytettiin teemoitettuja avoimia kysymyksiä, valmiiksi annettuja vastauksia, asteikkoja sekä monivalintakysymyksiä. Kysely toteutettiin Microsoft Forms -sovelluksella.

Tulokset analysoitiin MS Formsin sisältämillä analysointiominaisuuksilla. Analysoinnissa yhdistettiin kvalitatiivisia (avoimet vastaukset) ja kvantitatiivisia (valmiit vastaukset, asteikot) menetelmiä. Kyselytutkimuksen tulosten analysoinnissa käytettiin lisäksi apuna tekoälyä. Tekoälyä hyödynnettiin eri kysymysten ristiin analysoinnissa. Tekoälytyökaluna toimi ChatGPT (OpenAI, versio 4) -tekoälyohjelma. Analysointia tehtiin myös asettamalla vastaukset miellekarttaan. Miellekartta on paljon käytetty ongelmien visualisointitapa. Menetelmässä ongelma sijoitetaan kaavion keskelle ja ongelmaan vaikuttavat tekijät kytketään peräkkäisiksi sarjoiksi. (Kananen 2017, 59.) Saatujen vastausten avulla hahmotettiin kyberturvallisuuskulttuurin olemassaoloa ja siihen vaikuttavia asioita. Miellekartan avulla pyrittiin hahmottamaan ongelmat, jotka ilmenevät kyberturvallisuuskulttuurin jalkauttamisessa ja kehittämisessä.

Tulokset analysoitiin niin, että niistä voitiin johtaa teemojen pohjalta oppaan sisältö. Työtä iteroitiin sykleissä, jotta saatua analyysitietoa ja teoriaa aiheesta voitiin yhdistää ja työstää oppaaksi ammattiliitoille laajemman materiaalin ja tiedon lisääntymisen pohjalta.

3.5 Tavoite

Tutkimuksen tavoitteena oli toteuttaa opas tai koulutuspaketti ammattiliitoille, mitä kyberturvallisuus ja kyberturvallisuuskulttuuri ovat, miten jokaisen päivittäinen toiminta vaikuttaa ammattiliiton arkaluonteisen tiedon suojaamiseen ja miten kyberturvallisuuskulttuuri nostetaan osaksi yrityskulttuuria. Oppaan avulla oli tarkoitus saada kaikille ammattiliitoille yhtenevä ohjeistus, jolla nostetaan kyberturvallisuuden tietoisuutta ja -kulttuuria niin, että jäsenten arkaluonteinen tieto on yhtenevästi turvattu.

Oppaan ei ole tarkoitus olla yksi esitys, jonka avulla ammattiliitto voisi uskotella itselle, että nyt kyberturvallisuuskulttuuri on jalkautettu. Opas pyrkii ennemminkin luomaan pohjan ymmärryksestä, kuinka kulttuurin jalkauttaminen on pitkä polku ymmärryksen luomisesta ja tietoisuuden kasvattamisesta pitkäjänteisesti. Oppaalla tai koulutuspaketilla tässä työssä tarkoitetaan PowerPoint-esitystä, joka on laajennettavissa tilanteen ja tarpeen mukaan haluttuun suuntaan perustuen tämän opinnäytetyön sisältöön.

4 TEOREETTINEN VIITEKEHYS

Tutkimuksen teoreettisena viitekehyksenä toimii organisaatiokulttuuri ja se, miten turvallisuuskulttuuri on osa organisaation kulttuuria. Kyberturvallisuuskulttuurin sulauttaminen osaksi organisaatiokulttuuria on yksi tutkimuksen tärkeimmistä teemoista ja viitekehyksistä. Viitekehykseen kuuluu kyberuhat ja niiden vaikutus ammattiliittojen toimintaan. Ammattiliittokontekstissa tietojen suojaus ja erityisesti arkaluonteisen tiedon suojaus on tärkeä osuus. Lopuksi paneudutaan lakeihin ja asetuksiin, jotka edellä mainitussa viitekehyksessä on otettava huomioon.

4.1 Organisaatiokulttuuri

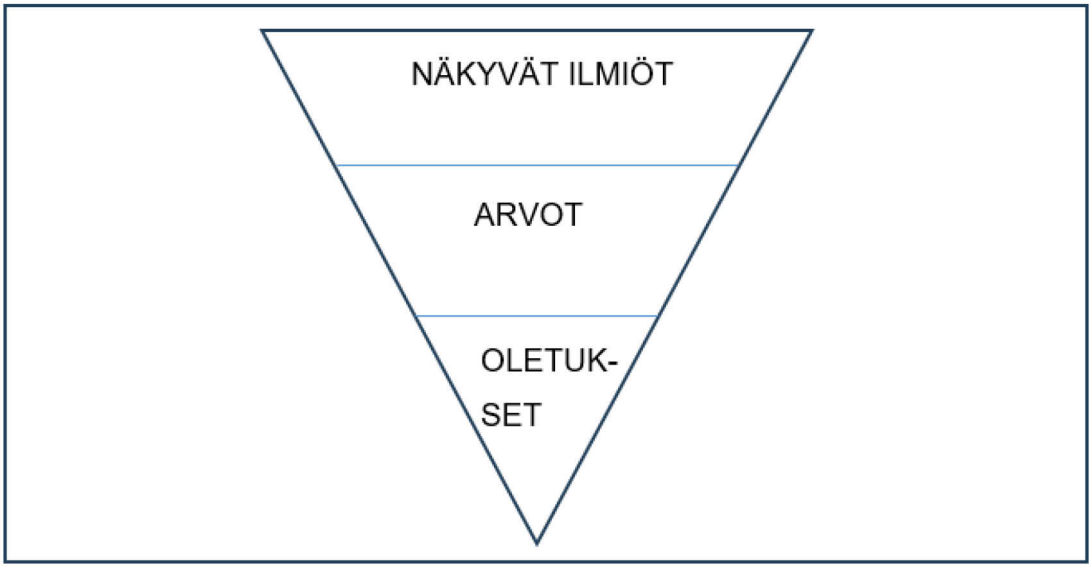
Työntekijöiden tapaan toimia ja suhtautua asioihin vaikuttaa organisaation kulttuuri. Organisaatiokulttuurin voi lyhyesti tiivistää määritelmään ”miten asiat organisaatiossa tehdään” (Kastepohja 2020, 33).

”Yrityskulttuuri on yrityksen kaikki”. Näin Panu Luukka (2019, 25) määrittelee organisaatiokulttuurin lyhimmillään teoksessaan ”Yrityskulttuuri on kuningas”

ja omin sanoin röyhkeimmillään. Organisaatiokulttuurista voidaan käyttää myös termiä yrityskulttuuri. Hieman pidempi Luukan (2019, 25) määritelmä on:

> ”*Yrityskulttuurilla tarkoitetaan yrityksen tiedostettuja ja tiedostamattomia arvoja, rakenteita ja toimintatapoja, jotka ohjaavat sen työntekijöiden ajattelua ja käyttäytymistä sekä yhdistävät heitä ja erottavat organisaation muista organisaatioista*”.

Anna-Maria Teperin (2023, 208) ”Ihminen turvallisuuden tekijänä” -teoksen mukaan organisaatiokulttuuri muodostuu yksilöiden ja ryhmien ajattelusta, kokemuksista ja käyttäytymisestä. Ne vaikuttavat koko ajan toiminnan taustalla ja ohjaavat sitä. Juutilainen kuvaa teoksessaan (2022, 26) organisaatiokulttuurin Scheinin kolmen tason kautta (kuva 1). Siinä päällimmäisenä ovat näkyvät ilmiöt, keskellä yrityksen arvot ja pohjimmaisena oletukset ja uskomukset. Vain osa näistä on havaittavissa, loput ovat pinnan alla piilossa vaikuttaen silti voimakkaasti ihmisten toimintaan.



Kuva 1. Organisaatiokulttuurin tasot Scheinin mukaan (Juutilainen 2022, 26)

Luukan (2019, 25) mukaan ymmärtääksemme yrityskulttuuria, tulee ymmärtää sen seuraavat keskeiset ominaisuudet:

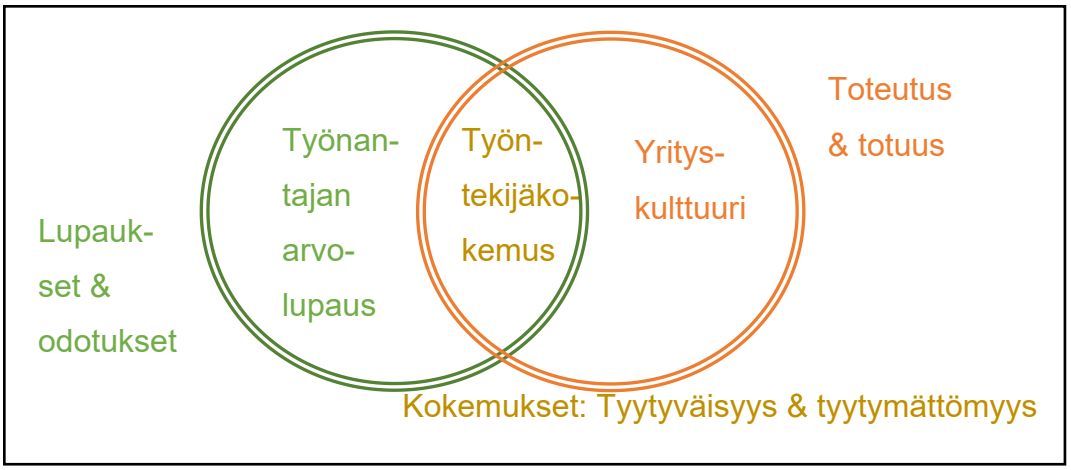
- *kulttuuri on aina ryhmään liittyvä ominaisuus*
- *kulttuuri luodaan yhdessä, ryhmän sisällä*
- *kulttuuri opitaan ja se on opetettavissa*

- *kulttuuri on jaettu: se yhdistää ryhmän jäseniä ja erottaa heidät muista ryhmistä*
- *kulttuuri vaikuttaa ja yhdistää ryhmään oletusten, arvojen ja käyttäytymisen tasolla ja*
- *kulttuuri on aina yksilöä vahvempi.*

Luukka jatkaa (2019, 55), että se, miten johtajat toimivat, mistä ja miten puhuvat ja kenelle puhuvat, on keskeinen yrityskulttuuria määrittävä tekijä. Kulttuuri on siis aina enemmän tai vähemmän johtajansa varjo, niin hyvässä kuin pahassa. Yrityskulttuuriin pitää erikseen tiedostaen keskittyä, niin johtajan kuin johtoryhmän. Se, millainen kulttuuri kulloisellakin johtajalla on, riippuu hänestä itsestä. Toisaalta Luukka toteaa (2019, 56), että paljon riippuu myös vallitsevasta kulttuurista, sillä vahva kulttuuri pureksii ja sylkee pois siihen sopimattoman johtajan.

Yrityskulttuurilla ei ole itseisarvoa. Yrityskulttuuri tulee nähdä työkaluna, jolla tavoitellaan toivottuja päämääriä ja tavoitteita, väittää Luukka (2019, 116). Luukka perustelee väitteensä sille, että yrityskulttuuri on keskeinen työkalu yrityksen menestykseen. Luukka laajentaa perusteluaan siten, että yrityskulttuuri on menestysketjun yksi osatekijä. Muut osatekijät ovat työntekijäymmärrys, työntekijäkokemus ja asiakaskokemus. En käsittele tässä tutkimuksessa enempää näitä osatekijöitä, mutta avaan kuitenkin työntekijäkokemusta ja sen liittymistä yrityskulttuuriin, koska se pohjaa työntekijän halukkuutta tietoturvaohjeiden noudattamisessa.

Luukka kirjoittaa (2019, 128), että työntekijäkokemus kuvaa työntekijän kokemusta työpaikasta. Se ei ole yrityskohtainen. Työntekijäkokemus on henkilökohtainen kokemus, jossa yksittäisen työntekijän odotukset ja hänelle annetut lupaukset törmäävät työnteon arjen ja yrityksen kulttuurin kanssa yhteen luoden tyytyväisyyttä tai tyytymättömyyttä ja sitoutumista tai sitoutumattomuutta. Lupauksien ja odotuksien väistämätöntä törmäystä arjen ja kulttuurin kanssa ei voi välttää ja väliin jää työntekijän henkilökohtainen kokemus (kuva 2). Luukka toteaa (2019, 128) vielä, että hyvä ja toivotunlainen työntekijäkokemus ei tapahdu, vaan se johdetaan. Aivan kuten kulttuurin kanssa, huono ja ei-toivottu työntekijäkokemus tapahtuu johtamattakin ja usein juuri niin.



Kuva 2. Työntekijäkokemus ja yrityskulttuuri (Luukka 2019, 128)

Luukka kertoo teoksessaan (2019, 421) Great Place to Work Instituten perustajan Robert Leveringin kertoneen, että parhaan kuvan yrityksen kulttuurista saa istumalla yrityksen ruokalassa. Se, miten ihmiset työpaikkaruokalassa vuorovaikuttavat ja käyttäytyvät, kertoo kulttuurista usein enemmän kuin yritykselle tehty kysely.

4.2 Turvallisuuskulttuuri

Turvallisuuskulttuuri-termin lähtökohdat ovat 1980-luvulla sattuneessa ydinvoimalaonnettomuudessa silloisessa Neuvostoliitossa. Turvallisuuskulttuuri-käsitteen alla on tarkasteltu organisaation kykyä tunnistaa, nostaa esille ja käsitellä toiminnan poikkeamia, kykyä puuttua vääränlaiseen toimintaan läpinäkyvillä ja selkeästi esille tuoduilla tavoilla sekä taitoa oppia tapahtuneista. (Teperi 2023, 210.)

Turvallisuuskulttuuri-termin keskeisenä tavoitteena on ollut korostaa turvallisuuden ensisijaisuutta toiminnassa. Termillä on kuvattu niitä ihmisen toiminnassa ilmeneviä uskomuksia, normeja, asenteita, rooleja sekä käytäntöjä, joilla organisaatio pyrkii vähentämään yksilöiden altistumista turvallisuutta uhkaaville tekijöille. Hyvällä turvallisuuskulttuurilla on tunnistettu olevan turvallisuutta parantava vaikutus turvallisuuden hallinnan, turvallisuuskäytäntöjen ja työntekijöiden turvallisuuskäyttäytymisen kautta. (Teperi 2023, 210.)

Teperi toteaa (2023, 225), että turvallisuuden kannalta on keskeistä, otetaanko päätöksissä huomioon hankinnan turvallisuusvaikutuksia vai tehdäänkö päätöksiä esimerkiksi pelkästään liiketoimintaperustein. Teperi (2023, 225) mainitsee yhdysvaltalaisen tutkijan Charle Perrow'n nostaneen esille, että organisaation ylin johto voi tehdä jopa harkittuja, organisaatiota ja sen ympäristöä vahingoittavia valintoja, koska heillä on mielessään muita etuja, joita "liian tehokas" turvallisuuskulttuuri uhkaisi.

Juutilainen (2022, 26) kuvasi edellä organisaatiokulttuurin Scheinin kolmen tason kautta (kuva 1). Niiden tasojen avulla Juutilainen (2022, 27) myös kuvaa turvallisuuskulttuurin ilmenemisen organisaatiossa. Näkyvä ylin taso ilmentää turvallisuuskulttuurissa esimerkiksi työsuojeluorganisaation rakennetta, turvallisuuden johtamisjärjestelmän dokumentaatiota, työturvallisuusohjeita, infotauluja, tiedotteita ja kuvattuja riskianalyyseja.

Toisella tasolla on organisaation arvot ja normit, jotka vaikuttavat ihmisten päätöksiin, valintoihin ja käyttäytymiseen. Osa arvoista on näkyviä ja osa on tiedostamattomia. Juutilainen (2022, 27) kuvaa, että olemassa olevia arvoja voidaan tunnistaa esimerkiksi pohtimalla, millaista toimintaa ja käyttäytymistä pidetään turvallisuuden kannalta hyväksyttävänä, tärkeänä ja arvostettavana, millaista taas ei-toivottuna tai mistä voi seurata sanktioita. Olemassa olevien arvojen tunnistamisen ohella organisaatioissa on tapana määritellä tavoitearvoja eli miten ihmisten toivotaan toimivan. Monessa organisaatiossa esimerkiksi toivotaan ihmisten puuttuvan turvallisuutta vaarantavan toimintaan asemasta ja roolista riippumatta.

Tässä kohtaa Juutilainen (2022, 28) herättää mielenkiintoisella ja varmasti monessa organisaatiossa relevantilla todellisuudella: johtajat korostavat, että turvallisuus on ykkösasia, mutta lähiesihenkilöiden ja henkilöstön kokemusten mukaan kiire saada tavara tai palvelu valmiiksi menee kuitenkin lopulta turvallisuuden edelle. Jos johtajat katsovat, että he voivat poiketa yhteisistä turvallisuussäännöistä, menee puheilta pohja.

Toinen esimerkki ristiriidasta on puhutun ja todellisen arvon väliltä se, miten organisaatiossa suhtaudutaan virheisiin ja poikkeamiin. Puheissa saatetaan

korostaa, että meillä saa tehdä virheitä ja niistä opitaan. Mutta uskaltaako jokainen varmasti tuoda oman mokansa esiin – ja jos uskaltaa, miten siihen lopulta suhtaudutaan? Uskaltaako jokainen puuttua kenen tahansa muun henkilön toimintaan, kun havaitsee tämän toimivan turvallisuutta vaarantavasti? (Juutilainen 2022, 28.)

Kolmannella, syvimmällä, Juutilaisen (2022, 28) esittämällä tasolla on organisaatiossa pohjimmaiset perusoletukset, uskomukset, käsitykset ja ajattelutottumukset, niin sanotut talon tavat. Nämä perusoletukset ovat syntyneet vuosien kuluessa organisaatiossa työskennelleiden ihmisten vaikutuksesta ja oppimisen tuloksena. Nämä vaikuttavat vahvasti ihmisten toimintaan ja käyttäytymiseen, mutta niiden tiedostaminen ja tunnistaminen on vaikeaa. Kulttuurin sanotaan olevan seinissä. Vahvat kulttuurin piirteet voivat säilyä, vaikka ihmiset vaihtuvat.

Jälleen Juutilainen herättää vahvalla esimerkillä: Kokenut asentaja ottaa uuden työntekijän mukaansa ja opastaa tätä tekemään jonkin yksittäisen tehtävän ohjeista poiketen tai ohjeita oikaisten kommentoimalla: ”Virallisestihan tämä pitäisi tehdä vähän toisin, mutta tämä hoituu nopeammin, kun teet sen tällä tavalla”. Tämä antaa uudelle työntekijälle selkeän viestin, että työpaikallamme on asioita, joissa noudatetaan turvallisuusohjeita ja asioita, joissa ohjeita ei pidetä niin tärkeänä. (Juutilainen 2022, 29.)

4.3 Kyberturvallisuuskulttuuri

Kyberturvallisuuskulttuuri yrityksessä on tavoitetila, jossa kyberturvallisuuden toteutumiseen voidaan luottaa ja jossa sen toiminta turvataan. Samalla tavalla kuin organisaation yleinen kulttuuri, myös kyberturvallisuuskulttuuri toimii. Niin teknisin keinoin kuin ihmisresurssein ja ihmisen toiminnalla. Kyberturvallisuuskulttuuri tulisi nähdä osana organisaatiokulttuuria.

Psykologi Ricardo Lugo (2023, 1) korostaa, että ihmistekijän merkitystä kyberturvallisuudessa ei voi liioitella, sillä se ulottuu paljon pelkkää teknistä osaamista laajemmalle. Ihmisten käyttäytymisen ymmärtäminen ja vuorovaikutus erilaisten menetelmien, kuten mallintamisen, pelillistämisen ja neuroergonomian, kautta on välttämätöntä kestävän kyberturvallisuusinfrastruktuurin

rakentamiseksi. Lugo (2023) jatkaa, että kyberturvallisuuden tarkastelussa on otettava huomioon paitsi teknologia, myös ihmiset ja näiden välillä tapahtuva vuorovaikutus. Tämä edellyttää monitieteistä lähestymistapaa, jossa huomioidaan muun muassa maantiede, politiikka ja aikatekijät. Näiden tekijöiden kautta voidaan paremmin ymmärtää niin kybertoimintaympäristön piirteitä kuin myös hyökkääjien motiiveja ja käyttäytymistä.

Kyberturvakulttuuri kuvaa sitä, miten käyttäjät toimivat suojatakseen tietoa kyberympäristössä, kuten internetissä tai muissa digitaalisissa verkoissa. Se keskittyy digitaalisen tiedon suojaamiseen verkkouhkia vastaan. Tietoturvakulttuuri, puolestaan kattaa sen, miten käyttäjät toimivat suojatakseen organisaation tietoa sen koko elinkaaren ajan ja kaikissa mahdollisissa muodoissa digitaalisena (esim. tiedostot ja sähköpostit), fyysisenä (esim. paperidokumentit) ja suullisesti tai visuaalisesti (esim. keskustelut tai näytöillä näkyvä tieto). (Da Veiga 2019.)

Jos yrityksen kulttuurissa nähdään turvallisuusasiat tärkeinä, on osoitettu resurssi tämän kehittämiseen ja tiedetään, miksi se on tärkeää sekä ymmärretään yksilön vaikutus siihen, ollaan jo hyvässä vauhdissa kyberturvakulttuurin luomisessa. Kun yksittäinen työntekijä ymmärtää isossa kuvassa miksi kyberturvallisuus on tärkeää ja miten hän voi itse siihen vaikuttaa, ja häntä rohkaistaan tuomaan epäkohtia esiin, työntekijä todennäköisimmin myös noudattaa saamiaan ohjeita. Da Veiga (2019) kiteyttää tietoturvakulttuurin edellä mainitun mukaisesti näin:

> *“A security culture can be seen as the unconscious manner in which things are done in an organization to secure information.”.*

Organisaation arvot, toiminnan perusoletukset ja tuntemukset vaikuttavat organisaation eri kulttuureihin kuten kyberturvallisuuskulttuuriin. Luodakseen turvallisuutta tukevan organisaatiokulttuurin tulisi organisaation tunnistaa millaisia arvoja se näkyvästi ja näkymättömästi ylläpitää sekä räätälöidä ohjeet, toimintamallit ja koulutukset vastaamaan niitä. (Kastepohja 2020, 36.) Da Veiga (2023, 283) korostaa, että se miten asiat organisaatiossa tehdään, tulee olla linjassa tietoturvapolitiikkojen kanssa ja että työntekijät jakavat samat arvot ja

keinot turvata tietoa. Toisin sanoen, vain vahva kyberturvallisuuskulttuuri takaa, että ihmiset toimivat kuten ohjeissa sanotaan.

Kyberturvallisuuskulttuurin käsitteessä korostuu ajatus siitä, että organisaatioiden tulisi huomioida työntekijöidensä tietoturvaan liittyvät arvot, asenteet, käyttäytyminen, merkitykset, uskomukset tiedot ja taidot organisaation tietovarantoja suojellessaan. Kyberturvallisuuskulttuuri pohjautuu ajatukseen organisaatiokulttuurista ja tietoturvakulttuurista, painottaen tietoturvakulttuurin tiedonhallintaan liittyvän näkökulman sijaan kokonaisvaltaista näkemystä ihmisen käyttäytymisestä tietotekniikan kontekstissa. (Da Veiga 2016, Savolaisen 2022, 7 mukaan.)

Uschendu ym. (2021, 9) tutkivat vuoteen 2020 mennessä julkaistut tieteelliset artikkelit ja tutkimukset kyberturvallisuuskulttuuriin liittyen. Tutkimuksesta ilmeni tekijät, jotka siihen mennessä julkaistujen artikkelien mukaan ovat tärkeimmät kyberturvallisuuskulttuurin vaikuttavista elementeistä. Tärkein vaikuttava tekijä on johtaminen ja johdon sitoutuminen, seuraavaksi tärkein tietoturvaohjeet/käytännöt ja kolmantena tietoturvatietoisuus (kuva 3). Myös Juutilainen (2022, 57) totesi organisaation johtajien roolin olevan kulttuurin johtamisessa ratkaisevia. Johto asettaa suunnan ja tavoitteet, joihin henkilöstö pystyy sitoutumaan. Johto määrittää talon tavat, periaatteet ja pelisäännöt, jotka viestitään niin, että jokainen ymmärtää ne.

Factors	Total
Top management support, leadership or involvement	34
Security policy	27
Security awareness	24
Security training	21
Change management	12
Compliance	12
Knowledge	11
Accountability and responsibility	9
Security risk	8
Commitment	8
Communication	8
User management	7
Motivation	7
Trust	6
National culture	5
Ethical conduct	4
Regulations	4
Establishing a network of champions	1
Rewards and sanctions	1

Kuva 3. Keskeiset tekijät kyberturvallisuuskulttuurin luomisessa ja ylläpitämisessä (Uchendu ym. 2021, 9)

Vahva tietoturvakulttuuri edistää myönteistä työntekijöiden käyttäytymistä, mikä vähentää käyttäjien virheistä tai huolimattomuudesta johtuvia tietoturvapoikkeamia ja tietomurtoja (Da Veiga 2019). Tietoturvan tulisi olla osa organisaation strategiaa ja visiota, ja sitä tulisi pitää strategisena etuna eikä hidasteena. Organisaatiokulttuurissa, jossa tietoturvaa arvostetaan, nähdään sääntöjen mukaista käyttäytymistä, jota vahvistetaan positiivisella kannustamisella ja ennakoivilla toimenpiteillä, kuten työntekijöiden tietoisuuden lisäämisellä, koulutuksella ja valmennuksella. (Da Veiga 2023, 283.)

ENISAn (2017, 37) raportissa todetaan, että ihmiset ovat sosiaalisia olentoja, joiden käytökseen vaikuttaa ryhmän käytös ja ryhmän paine. Koska ihmiset haluavat kuulua joukkoon ja hakevat muiden hyväksyntää, heidän käytökseensä voi vaikuttaa vahvastikin niin muiden työntekijöiden, kuin esihenkilöiden odotukset. Jos työntekijät uskovat muidenkin noudattavan ohjeita, he te-

kevät sen myös itse. Lisäksi, jos työntekijät uskovat, että yksittäisen työntekijän toimilla on vaikutusta yrityksen kokonaisturvallisuuteen, he työskentelevät sitä kohti.

Näitä kaikkia edellä mainittuja tekijöitä voidaan kuvata sisäisiksi tietoturvakulttuuriin vaikuttaviksi tekijöiksi. Ihmisten toimintaan yrityksessä vaikuttaa organisaatiokulttuurin lisäksi myös kansallinen lainsäädäntö ja kansallinen kulttuuri (ENISA 2017, 38; Hofstede ym. 2010, Da Veigan 2019 mukaan). Nämä ovat erilaisia eri maissa ja maanosissa ja voivat vaikuttaa ihmisten suhtautumisessa tietoturvaan. Näitä kutsutaan ulkoisiksi tekijöiksi.

Ejigu ym. (2021, 4) esittävät hypoteesin, että sanktiot ja häpeä lisäisivät tietoturvaohjeiden (ISP) noudattamista. Samat tutkijat esittävät myös hypoteesit moraalisesta käsityksestä ja henkilökohtaisesta hyödystä tehostaa ISP noudattamista. Ejigun ym. (2021) tutkimus on case-tutkimus ja tehty Afrikan kontekstiin. Maantieteellinen ja kansallinen ero lienee huomattava vaikutin tässä eikä ole tutkittu tai osoitettu vastaavia hypoteeseja ja niiden ilmenemistä pohjoismaisessa kontekstissa.

4.3.1 Vallitsevan turvallisuuskulttuurin takana piilee alakulttuureita

Ymmärrys organisaation kulttuurista ja sen eri ammattiryhmien edustamista alakulttuureista on olennaista, kun halutaan kehittää turvallisuutta. Kulttuuria ei voi muuttaa tai uudistaa, ellei ensin tunnista nykyistä toimintakulttuuria ja sen taustalla olevia perusolettamuksia ja arvoja. Kulttuurin muutos on hidasta, kuten edellä jo todettu, mutta usein se on välttämätöntä, jos toimintaa halutaan uudistaa tai muuttaa. (Teperi 2023, 200.)

Da Veiga (2019) toteaa samoin, että organisaation tietoturvakulttuuri ei ole yksinkertainen ja yhtenäinen kokonaisuus, vaan se koostuu:

1. pääasiallisesta (dominoivasta) tietoturvakulttuurista ja
2. siihen liittyvistä alakulttuureista.

Näiden kulttuurien erilaisuus ja vuorovaikutus vaikuttavat siihen, miten tietoturvaan suhtaudutaan ja miten tietoturvakäyttäytymistä voidaan kehittää organisaation eri osissa. Da Veiga (2019) avaa dominoivaa tietoturvakulttuuria niin, että se edustaa enemmistön yhteistä näkemystä siitä, miten tietoa tulisi suojata organisaation perusvaatimusten mukaisesti. Se toimii ikään kuin organisaation "yleisenä kulttuurina" tietoturva-asioissa. Alakulttuurit puolestaan muodostuvat työntekijäryhmissä, joilla on yhteisiä piirteitä, kuten:

- maantieteellinen sijainti (esim. eri toimistot eri alueilla)
- osastot tai työtehtävät (esim. IT-osasto vs. myyntiosasto) tai
- demografiset tekijät (ikä, sukupuoli, koulutustausta).

Kaikkiin ryhmiin muodostuu erilaisia rooleja, joko virallisesti määriteltyjä tai epävirallisesti saatuja tai itse otettuja. Ryhmiin syntyy lisäksi epävirallisia auktoriteetteja, jotka voivat olla vahvempia kuin virallisten roolien kautta tulevat vaikutukset. Näitä henkilöitä ryhmässä todellisuudessa kuunnellaan. Jos haluamme muokata tai kehittää organisaation kulttuuria, on tärkeää tunnistaa epäviralliset roolit. (Juutilainen 2022, 121.)

Alakulttuureilla voi olla omia näkemyksiään tietoturvan tärkeydestä, kuten esimerkiksi osastossa, jossa tiedon jakaminen ja nopeus asetetaan etusijalle tietosuojan kustannuksella. Jos näin on, ei voida puhua vahvasta tai positiivisesta tietoturvakulttuurista vaan riskit mm. tiedon menettämiselle alkavat kohota. Tätä voidaan kehittää Da Veigan (2019) mukaan niin, että hyödynnetään dominoivaa tietoturvakulttuuria vaikuttamaan alakulttuurien asenteisiin ja käyttäytymiseen ja saadaan ne siten linjattua yhteneviksi organisaation yleisiin tietoturvatavoitteisiin. Samaa lähestymistapaa ei voida kuitenkaan käyttää kaikille ryhmille, koska alakulttuurien näkemykset ja noudattamatta jättämisen syyt voivat vaihdella ja organisaation tulee soveltaa räätälöityjä ja kohdennettuja toimenpiteitä dominoivan kulttuurin ja alakulttuurien kehittämiseen. Juutilainen (2022, 121) toteaa, että osallistavilla muutoksen käsittelymalleilla voidaan tehdä näkyväksi ihmisten suhtautumiset ja näin organisaatio pystyy paremmin suunnittelemaan johtamisen käytännön toimia.

Yksi Juutilaisen (2022, 158) esittämä osallistava asioiden käsittelymalli on viisivaiheinen OPERA (kuva 4). Se on hänen mukaansa monimuotoinen työkalu,

jolla saadaan koko ryhmän kyvykkyys käyttöön ja jota voidaan hyödyntää lähestulkoon kaikenkokoisissa ryhmissä.

O	**Omat näkemykset** • saadaan kaikki mukaan ajattelutyöhön miettimään käsiteltävää asiaa • saadaan kaikki yksilöinä tehokkaasti tuottamaan ajatuksia ja ehdotuksia • saadaan jokaisen kokemus ja asiantuntemus käyttöön • saadaan erilaisia näkökulmia asiaan
p	**Pari- tai pienryhmäkeskustelut** • saadaan aikaan tehokas vuorovaikutus, kaikki tulevat kuulluksi • saadaan hiljaisemmat mukaan osallistumaan • saadaan laajennettua omia näkökulmia, kun kuulee parin tai pienryhmän muiden jäsenten ajatuksia • syntyy uusia ideoita ja ehdotuksia • saadaan koottua yksittäisten ihmisten ajatuksista parin tai pienryhmän mielestä tärkeimmät
E	**Esittely ja kaikki asiat näkyville** • saadaan asiaan liittyvät näkemykset ja ajatukset esille • saadaan erilaiset näkemykset esille yhtä aikaa, niin että niitä voidaan arvioida • niin yksiköille kuin ryhmällekin syntyy parempi kokonaisymmärrys ja kuva käsiteltävästä asiasta
R	**Ristiin arviointi ja tärkeimpien valinta** • saadaan kyseisen asian kannalta tärkeimmät asiat poimittua jatkokehittämistä varten positiivisen valinnan avulla • saadaan aikaan parempi yhteinen ymmärrys ja sitoutuminen käyntiin • syntyy porukan kannalta mielekkäitä aiheita jatkotyöstöön
A	**Asiakokonaisuuksien ryhmittely** • saadaan jatkototeuttamisen kannalta järkeviä ja jäsentyneitä kokonaisuuksia • ryhmän yhteinen näkemys jäsentyy • sitoutuminen yhteiseen asiaan vahvistuu

Kuva 4. Tietoturvaohjeet pureskeltuna top 5 -muotoon (Juutilainen 2022, 160)

Juutilainen (2022, 165) huomauttaa vielä, että OPERA on kätevä toteuttaa nykypäivän hybridityössä myös virtuaalisesti esimerkiksi Teams-sovelluksessa.

4.3.2 Kyberturvallisuuskulttuurin nykytilan arviointi

Ennen kehittämistoimia on syytä tehdä nykytilan arviointi, joka auttaa ymmärtämään eri ryhmien sisällä vallitsevia asenteita ja niiden mahdollisia poikkeamia yleiseen kyberturvakulttuuriin. Arviointi tarjoaa dataa, joka auttaa organisaatiota ymmärtämään kulttuurin nykytilaa, suunnittelemaan tehokkaita toimenpiteitä ja seuraamaan edistymistä pitkällä aikavälillä. Tämä tekee tietoturvakulttuurin kehittämisestä kohdennettua ja tuloksellista.

Tietoturvakulttuurin arviointi on keskeinen työkalu, jonka avulla organisaatiot voivat:

1. **Tunnistaa poikkeamia:** Selvittää, ovatko tietyn osaston tai ryhmän työntekijöiden käyttäytyminen ja asenteet linjassa odotetun tietoturvakulttuurin kanssa.
2. **Priorisoida riskejä:** Löytää tietoturvakulttuurin riskitekijät ja räätälöidä interventiot niiden mukaisesti.
3. **Arvioida muutosten vaikutuksia:** Seurata ja mitata tietoturvakulttuurin muutosten onnistumista interventioiden jälkeen.
4. **Kohdentaa koulutusta:** Käyttää arvioinnin tuottamaa dataa tietoisuuden, koulutuksen ja opetuksen ohjelmien sisällön ja kohderyhmien määrittämiseen.

(Da Veiga 2019.)

Nykytilan arviointiin kyselytutkimus (kvantitatiivinen lähestymistapa) on tehokas keino kartoittaa työntekijöiden asenteita ja mielipiteitä organisaation käytännöistä tieto- ja kyberturvakulttuurista (Saunders 2009, Da Veiga 2019 mukaan). Lisäksi voidaan käyttää monimenetelmäistä lähestymistapaa, jossa dokumenttien, kuten tietoturvapolitiikoiden, ohjeiden ja auditointiraporttien analyysi tukee kyselydataa. Haastattelut tai ryhmäkeskustelut voivat antaa syvällisempiä näkemyksiä kyselytulosten taustalla olevista syistä. Tutkimus on suunniteltava huolellisesti, varmistuttava tietosuojan toteutumisesta, riittävästä otannasta, etu- ja jälkikäteisviestinnästä ja mm. harkittava palkitsemista. Tulokset on syytä jakaa niin johdolle kuin työntekijöille läpinäkyvyyden varmistamiseksi. (Da Veiga 2019.)

Mittaamiseen on perinteisesti käytetty kyselyitä tai kyselylomakkeita. Da Veiga & Martins (2017, 80) huomauttaa kuitenkin, että kysely kertoo vain tietoisuudesta, ei käyttäytymisestä. Se miten henkilökunta todellisuudessa eri tilanteissa toimii, ei välttämättä selviä kyselylomakkeella vaan sen selvittämiseen on parempi suorittaa käyttäytymistestejä. Kyberturvallisuuden mittaamiseksi olisikin tehtävä sekä kyselyitä että käyttäytymistä mittaavia testejä. Uchendu ym. (2021, 80) huomauttavat myös, että kysely kertoo vain sen hetkisen tilanteen. Jotta saataisi kattavampaa kuvaa, tulisi sama kysely suorittaa säännöllisin väliajoin.

4.4 Kyberturvallisuuskulttuurin kehittäminen

Vahva tietoturvakulttuuri johtaa myönteiseen käyttäytymiseen, mikä vähentää tietoturvapoikkeamia ja inhimillisistä virheistä aiheutuvia uhkia (ENISA 2017, 29. Kyberturvallisuuskulttuuri, samoin kuin yrityskulttuuri, on luonteeltaan sellainen, että sitä täytyy kehittää ja vaalia jatkuvasti sen sijaan, että se suunniteltaisiin jäykästi. Tämä käy ilmi Badan ym. (2021) tutkimuksestakin.

Huolimatta laajasta teorioiden ja lähestymistapojen kirjosta, samankaltaiset kulttuurin jatkuvaan kehittämiseen liittyvät näkökohdat ja ominaisuudet toistuvat kirjallisuudessa. Jotta kyberturvallisuuskulttuuria voi kehittää, on ensin a) tunnistettava minkälainen organisaation nykyinen vallitseva kyberturvallisuuskulttuuri, b) minkälaisia kyberturvallisuuden alakulttuureita on ja c) minkälaisia toimenpiteitä tulisi tehdä, jotta kyberturvallisuuskulttuuri paranisi.

Kulttuuri ei synny hetkessä. Se ei ole yksi koulutus henkilökunnalle tai opas, jonka voi lukea. Kuten olemme havainneet, kulttuuri syntyy ymmärryksestä, ihmisistä, tavoista ja työn laadusta pitkällä aikajänteellä. Tämän päivän digitalisoituneessa yhteiskunnassa kyberturvallisuus ja turvallisuusasiat tulee ottaa huomioon organisaatiokulttuurin osana. Kulttuurin muuttaminen on hidasta eikä kukaan voi tehdä sitä yksin, edes johtaja. Vanhasta on ensin opittava pois ennen kuin uusi voi tarttua ihmisiin. (Luukka 2019, 56.)

Ihmisen toiminnan ymmärtäminen on keskeistä kulttuurin kehittämisessä ja hallinnassa, varsinkin nykyaikaisissa työympäristöissä, jotka ovat yhä moni-

mutkaisempia ja hajautuneempia. Ihmisen toiminta useimmiten luo turvallisuutta, mutta haastavissa olosuhteissa ihminen omalta osaltaan vaikuttaa turvallisuuden horjumiseen. Ihmisen toimintaan on kiinnitetty huomiota erityisesti onnettomuuksien yhteydessä ja silloinkin ihmisen tekemien virheiden kautta. Ihmistä on pidetty heikkona lenkkinä. (Teperi 2023, 21.) Teperi (2023, 21) jatkaa, että se, miten ihminen kuitenkin kytkeytyy turvallisuuteen, on paljon monitahoisempi kuin inhimilliset virheet. Aivan samoin kuin turvallisuuden kehittäminen on paljon muutakin kuin tekniset laitteet, ohjeet tai suojaukset. Huomio pitäisi Teperin (2023, 22) mukaan suunnata siihen, miten ihmisille voidaan luoda edellytykset toiminnassa onnistumiseksi ja turvallisuuden toteutumiseksi.

Sääntöihin ja ohjeisiin perustuva kyberturvallisuuskulttuurin kehitysmalli ei ole nykypäivää. Tämä käy ilmi tohtori Alshaikhin (2020, 1) tutkimuksesta, jossa tutkittiin kolmen australialaisen finanssialalla toimivan yrityksen kyberturvallisuuskulttuurin kehitystoimia. Tutkimus herättää ajattelemaan kyberturvallisuuskulttuurin saavuttamista konkreettisilla uusilla toimilla perinteisten sääntöihin ja ohjeisiin perustuvien koulutusten sijaan.

> *Esimerkiksi, jos yrityksessä on 300 sivua tietoturvallisuusmateriaalia, miten voimme olettaa, että työntekijät arjessa sen muistaisivat?*

Kulttuurin muodostumisen sijaan muodostuu ahdistus ohjeista. Kyberturvallisuustiimien tulisikin purkaa ohjeet helposti omaksuttaviksi iskulauseiksi (kuva 5).

Kuva 5. Tietoturvaohjeet pureskeltuna top 5 -muotoon (Alshaikh 2020, 4)

Alshaikhin (2020, 7) tutkimuksesta löytyy viisi konkreettista kokonaisuutta, joiden avulla yritykset saavuttavat aidon kyberturvallisuuskulttuurin aikaisemman vaatimuksiin ja ohjeisiin perustuvien koulutuksien sijaan. Teemat ovat seuraavat (kuva 6):

- **Keskeisten kyberturvallisuusohjeiden tunnistaminen**
    - Tunnista tärkeimmät ohjeet, joita työntekijöiden tulisi noudattaa, kuten "ajattele ennen kuin klikkaat" ja "ilmoita epäilyttävistä tapahtumista" (kuva 5).
- **Kyberturvallisuuslähettiläsverkoston luominen**
    - Perusta kyberturvallisuuslähettiläiden verkosto (cybersecurity champions), jotka toimivat linkkinä tietoturvatiimin ja työntekijöiden välillä.
    - Lähettiläät auttavat levittämään tietoisuutta ja tukemaan kollegoitaan kyberturvallisuusasioissa.
- **Kyberturvallisuushubin rakentaminen**
    - Perusta sisäinen verkkosivusto, jossa on kaikki turvallisuuteen liittyvät resurssit, ohjeet ja ilmoitukset yhdessä paikassa. Paikka, jossa voi keskustella ja kysyä ja jonne voi poikkeuksista raportoida. Teams-tiimi toimisi tähän myös hyvin.
- **Kyberturvallisuustiimin brändääminen**
    - Luo visuaalinen identiteetti (logo, brändi tms.) kyberturvallisuustiimille, jotta se olisi helpommin tunnistettavissa. Tämä voi lisätä tietoisuutta ja helpottaa viestien perille menoa.
- **Turvallisuustietoisuuden yhdistäminen muuhun viestintään**
    - Kyberturvallisuuskampanjat kannattaa ajoittaa organisaation muiden koulutusten ja valistuskampanjoiden kanssa (esim. tietosuojaviikko, verkkoturvallisuuspäivä). Tämä voi vähentää työntekijöiden koulutuskuormaa.

Kuva 6. Viisi keskeistä tekijää perinteisen tietoturvaohjelman muuttamiseksi vaatimustenmukaisuudesta kulttuuriksi (Alshaikh 2020, 8)

Da Veiga (2023) tutki luovuuden ja innovoinnin käyttöä tietoturvakulttuurin kehittämisessä. Tutkimuksessa selvitettiin, millainen tietoturvakulttuurimalli muodostuu, kun luovuus ja innovointi toimivat sen mahdollistajina. Tämän pohjalta tutkija esitti konseptuaalisen mallin, jossa tietoturvakulttuuria vahvistetaan luovuuden ja innovoinnin avulla. Tutkimuksessa tunnistettiin keskeisiä piirteitä, jotka stimuloivat luovuutta ja innovointia organisaatiossa. Näitä ovat muun muassa muutosmyönteisyys, monimuotoisuus, autonomia, tiimityöskentely ja luottamus. Luovuuden ja innovoinnin toteuttaminen tietoturvakontekstissa tulee tehdä ottaen huomioon organisaation riskiprofiili ja riskinsietokyky. Tämä edellyttää huolellista hallintaa strategian ja politiikkojen kautta, jotka määrittelevät luovuuden ja innovoinnin rajat. Luovuus ja innovointi ei voi siis ohittaa annettua politiikkoja ja ohjeita vaan innovointi tapahtuu niiden rajoissa. Arvoa voidaan lisätä sisällyttämällä luovuus ja innovointi tietoturvakoulutukseen, tietoisuuden lisäämiseen ja viestintään. Tämä edistää tiedon jakamista ja vahvistaa työntekijöiden tietoturvaosaamista. Da Veiga (2023, 299) kuitenkin huomauttaa, että mallia ei ole validoitu tilastollisesti.

Lugo (2023, 1) kiinnittäisi huomiota pehmeiden taitojen (viestintä, yhteistyö, tilannetietoisuus) kehittämiseen kyberturvallisuuden tehostamiseksi. Kyberturvallisuusharjoitusten suunnittelussa voidaan hänen mukaansa hyödyntää useita eri menetelmiä oppimisen tehostamiseksi. Mm. pelillistäminen on nousemassa tärkeäksi työkaluksi sekä sitoutumisen että oppimisen kannalta. Pe-

lillistämisen avulla voidaan parantaa myös tilannetietoisuutta ja tehdä oppimisesta interaktiivisempaa ja helpommin omaksuttavaa. Erityisesti monimutkaisten kyberturvallisuuskäsitteiden opettamisessa tämä voi olla hyödyllistä, sillä se tekee oppimisesta helpommin lähestyttävää.

4.4.1 Kyberturvallisuuskulttuurin kehittämisen haasteet

Suurimpia haasteita kyberturvallisuuskulttuurin kehittämisessä yleisesti on Da Veigan ym. (2020) tutkimuksen mukaan koulutuksen ja tietoisuuden puute, johtamisen puute, riskien/uhkien/poikkeaminen ymmärryksen puute, tietoturvakulttuurissa luottamuksen puute, tekniset puutteet ja resurssien (raha, tekijät) puute (kuva 7).

Kuva 7. Suurimmat haasteet tietoturvakulttuurin kehittämiselle (Da Veiga ym. 2020, 17)

Markus Savolaisen (2022, 101) tutkimus päätyi puolestaan siihen, että suurin haaste kyberturvallisuuden kulttuurin kehittämiselle työntekijöiden näkökulmasta on organisaation halun tai välineiden puute, tai molemmat. Lisäksi tietoturvaa koordinoivan tahon johto-oikeuden puute koetaan haasteeksi ja tietoturvakoulutuksen taso heikoksi. Tämä voidaan yleistää ylipäätään myös resurssien puutteeksi, kuten Da Veiga listasi.

Suurimman haasteen eli tietoisuuden kasvattamiseksi organisaatioilla on käytössä monia eri keinoja kahdenkeskisestä palaverista verkkokoulutuksiin ja hybriditoteutuksiin. Keinoja tulee käyttää monipuolisesti käyttäen hyväksi esimerkiksi seuraavia:

- keskusteluja
- testejä
- koulutuksia
- webinaareja
- asiantuntijaluentoja
- pelejä
- lavastettuja kalastelukampanjoita
- videoita
- tositarinoiden kuvauksia
- flyereita
- workshoppeja
- tietoiskuja
- FAQ-vinkkejä
- uutiskirjeitä.

(ENISA 2017, 18.)

Organisaation tulee valita tietoisuuden kasvattamiseen sellaiset keinot, jotka sopivat omaan organisaatiokulttuuriin ja viestintätapaan sekä puhuttelee erilaisia käyttäjäryhmiä. Valittujen toimenpiteiden tulee olla jatkuvia, säännöllisiä ja toisiaan tukevia.

Lugo (2023, 2) korostaa myös kyberturvallisuuskoulutuksen suunnittelussa kokonaisuutta, joka on monimuotoinen ja saavutettava eri käyttäjäryhmille. Hänen mukaansa kyberturvallisuuskoulutuksessa on tärkeää kehittää hyvin suunniteltuja koulutusmalleja ja malleissa voidaan ottaa esimerkkiä muilta aloilta, vaikkapa terveydenhuollosta. Kyberturvallisuusharjoitusten arvioinnissa tulee kiinnittää huomiota tasapuolisuuteen ja selkeyteen. Avoimuus ja läpinäkyvyys ovat keskeisiä tekijöitä, jotta osallistujat voivat todella hyötyä harjoituksista ja kehittyä kyberturvallisuusosaajina.

On syytä huomata, että koulutukset yksinään eivät johda hyvään lopputulokseen. Uchendu ym. (2021) toteavat, että 50 % koulutuksen informaatiosta on unohdettu tunnissa, 70 % vuorokaudessa ja 90 % viikossa (Ghafir ym. 2018, 16).

4.4.2 Kyberturvallisuuskulttuurin kehittämisen mallit

Useimmat tutkimukset esittävät uusia viitekehyksiä tai korostavat tietoturvakulttuuriin vaikuttavien tekijöiden ymmärtämisen tärkeyttä. Kuitenkaan ei ole yhteistä näkemystä siitä, mitä konkreettisia keinoja tulisi käyttää kyberturvallisuuskulttuurin kehittämiseksi. Näihin malleihin tutustuminen auttaa kuitenkin osoittamaan kyberturvallisuuteen vaikuttavia tekijöitä, jäsentämään kehitystyötä, kartoittamaan nykytilaa ja ohjaamaan toimenpiteitä organisaation tarpeiden mukaisesti.

Ammattiliittojen toimintaympäristössä, jossa suojellaan erityisen arkaluonteista jäsentietoa ja, joissa resursseja on usein rajallisesti, on kyberturvallisuuskulttuurin vahvistaminen elintärkeää. Tämä vaatii systemaattisia keinoja kulttuurin arvioimiseksi ja kehittämiseksi, mihin mallit tarjoavat varteenotettavia työkaluja. Tässä opinnäytetyössä esitellään neljä kyberturvallisuuskulttuurin kehittämisen mallia ja arvioidaan lopuksi niiden soveltuvuutta ammattiliittojen tarpeisiin. Mallit ovat seuraavat:

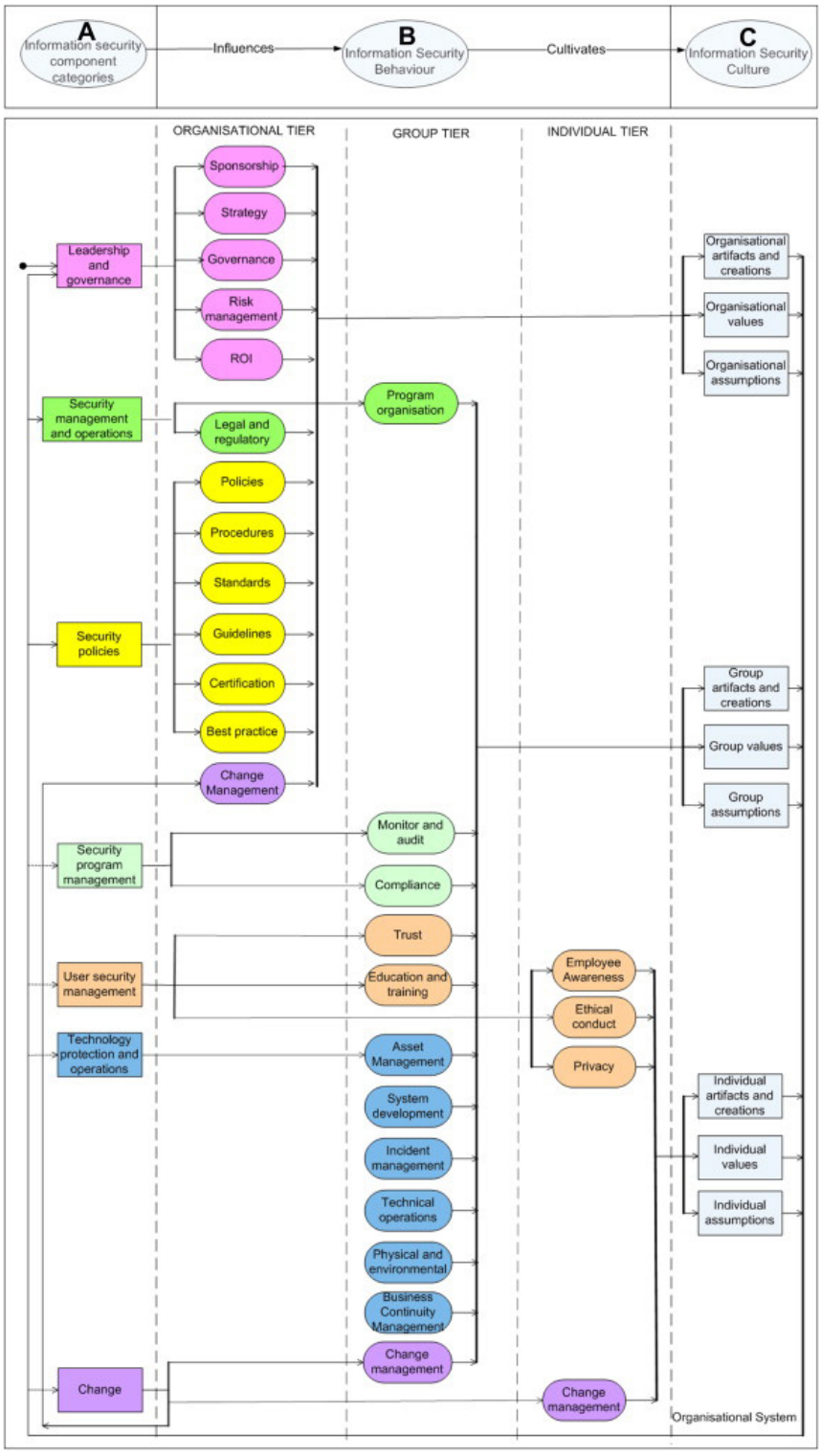
- ISCF (Information Security Culture Framework)
- ISCCM (Information Security Culture Change Management)
- ENISAn malli
- ISCFF (Information Security Culture and Key Factors Framework).

On tärkeää ymmärtää, että kaikki tutkitut mallit ovat yleistyksiä, niitä ei välttämättä ole testattu tutkijoiden toimestakaan käytännössä, ne ovat usein isojen organisaatioiden kontekstiin tehtyjä ja suoraan yksikään niistä ei ole tarkoitettu varsinaisesti ammattiliitoille. Tämän työn tarkoitus on validoida malleista tutkimuksen tekijän suositus ammattiliittojen käyttöön. Jokainen organisaatio kuitenkin valitsee elementit omaan organisaation sopivaksi.

ISCF (Information Security Culture Framework)

ISCF on Da Veigan ja Eloff:n (2010, 197) kehittämä malli organisaation tietoturvakulttuurin arviointiin. ISCF-malli perustuu seitsemään tietoturvan osa-alueeseen, jotka on esitetty erillisessä kuvassa sen vasemmassa reunassa sarakkeessa A (kuva 8). Osa-alueet ovat johtaminen, turvallisuuden hallintatoi-

minnot, turvallisuuskäytännöt, turvallisuusohjelman hallinta, käyttäjäturvallisuuden hallinta, tekniset suojaukset ja muutos. Tietoturvan osa-alue luokitellaan organisaation, ryhmän tai yksilön tasolle sen perusteella, miten se vaikuttaa tietoturvakäyttäytymiseen (sarake B). Tietoturvakulttuuri rakentuu jokaisella tietoturvakäyttäytymisen kolmella tasolla ja lopulta ilmenee ulospäin näkyvänä tietoturvakulttuurina (sarake C).



Kuva 8. ISCF malli (Da Veiga & Eloff 2010, 200)

ISCF-mallia voidaan käyttää mittaamaan organisaation kyberturvallisuuskulttuurin nykytilaa, tällöin mallista käytetään erikseen tehtyä arviointimallia ISCA (Information Security Culture Assesment) (Da Veiga & Eloff 2010, 203). Arviointimalli koostuu 85 väittämästä, kuten ”Ymmärrän miten tietoturvaa hallitaan yrityksessä tietojen suojaamiseksi” ja ”Yritys on sitoutunut tietoturvaan suojellakseen tietoja”. Nämä kaikki väittämät arvioidaan 5-asteisella Likert-asteikolla. (Uchendu ym. 2021, 11.) ISCA-malli voi auttaa määrittämään, parantaako tietoturvakulttuurin taso organisaation tieto-omaisuuden turvallisuutta. Johdetut mittarit tarjoavat tiekartan, jonka avulla voidaan myönteisesti vaikuttaa työntekijöiden käyttäytymiseen ja asenteisiin liittyviin kehitysalueisiin. (Da Veiga & Eloff 2010, 203.)

ISCCM (Information Security Culture Change Management)

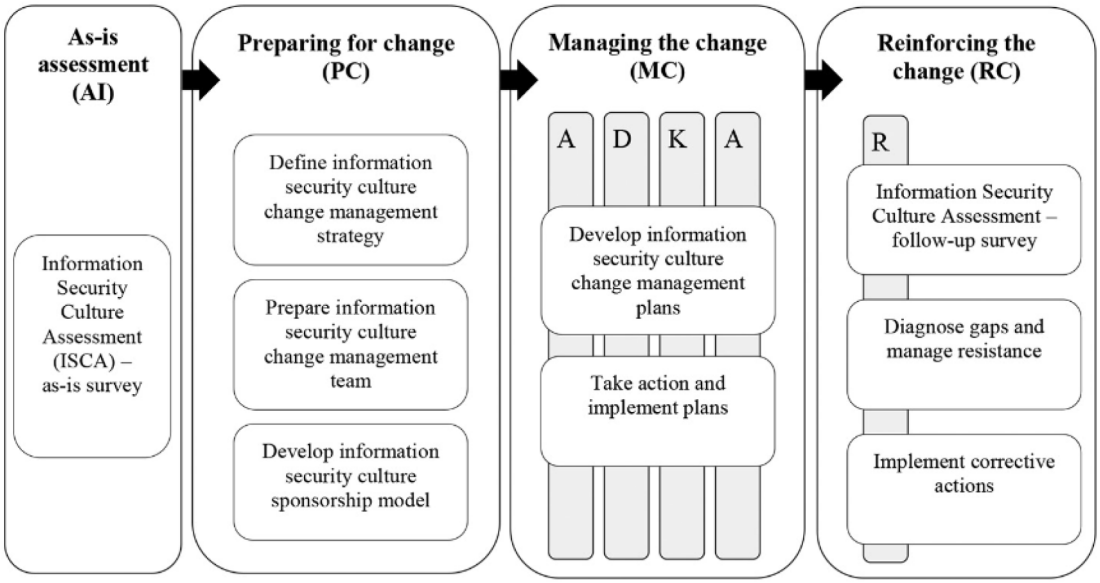
Da Veiga (2018, 585) hahmotteli tietoturvakulttuurin muutosprosessin viitekehyksen, ISCCM-mallin, koska työntekijöiden käyttäytyminen on hänen mukaansa jatkuva huolenaihe ja merkittävä osa tietoturvapoikkeamista johtuu heidän toiminnastaan. Tämä lähestymistapa yhdistää olemassa olevia muutosjohtamisen malleja, kuten Prosci ADKAR-mallin, sekä tietoturvakulttuurin arviointiin tarkoitetun aikaisemmin mainitun ISCA-arviointimallin. Mallin avulla voidaan paremmin hallita työntekijöiden käyttäytymiseen liittyviä riskejä, jotka saattavat vaarantaa tietoturvan.

> ”Prosci ADKAR-malli on tavoitteellinen ja ihmislähtöinen muutosjohtamisen malli, joka ohjaa muutosta sekä yksilö- että organisaatiotasolla. Proscin perustajan Jeff Hiattin luoma ADKAR on lyhenne, joka edustaa viittä konkreettista elementtiä, jotka yksilön tulee saavuttaa pysyvää muutosta varten: tietoisuus (Awareness), halu (Desire), tieto (Knowledge), taidot (Ability) ja vahvistaminen (Reinforcement).” (Change Partners Finland Oy s.a.)

ISCCM-lähestymistapa ja ISCA-arviointi tarjoavat organisaatioille keinoja tietoturvakulttuurin muutoksen hallintaan, täydentäen perinteisiä tietoturvakehyksiä, kuten COBIT ja ISO/IEC 27002. Ne auttavat johtoa ymmärtämään organisaation nykyistä tietoturvakulttuuria, kehittämään ajankohtaisia koulutus- ja tietoisuusohjelmia sekä priorisoimaan riskialttiita alueita. ISCCM tukee myös muutoksen seurattavuutta ja jatkuvaa parantamista, mahdollistaen resurssien

tehokkaan kohdentamisen. Akateemisesti ISCCM toimii viitekehyksenä tietoturvakulttuurin tutkimukselle ja sovellettavaksi eri toimialoille ja maihin. (Da Veiga 2018, 585.)

ISCCM on kokonaisvaltainen, nelivaiheinen malli, joka tukee tietoturvakulttuurin kehittämistä. Sen tavoitteena on vähentää inhimillisiin tekijöihin liittyviä riskejä tietoturvan suojelussa. Malli toteutetaan syklisesti ja sisältää keskeisiä toimenpiteitä tietoturvan parantamiseksi (kuva 9). (Da Veiga 2018, 591.)



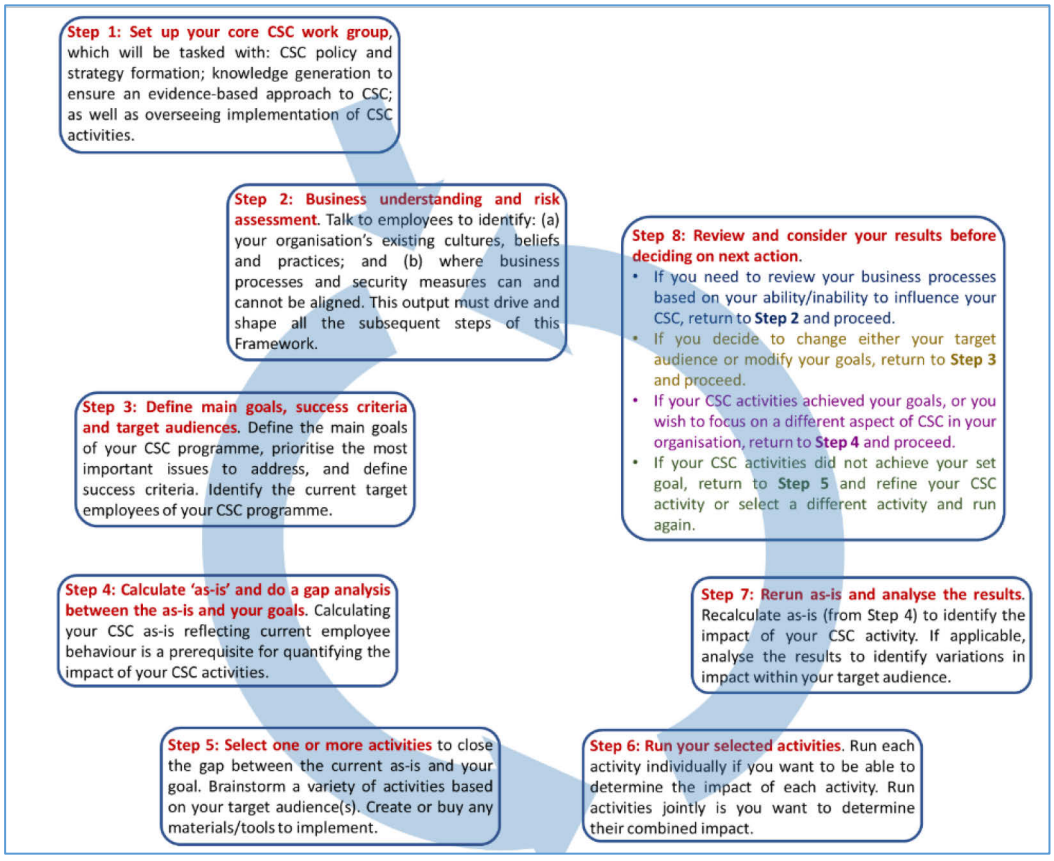
Kuva 9. ISCCM (Da Veiga 2018, 591 2010, 200)

ISCCM:n ensimmäisessä vaiheessa arvioidaan organisaation tietoturvakulttuurin nykytila ISCA-diagnostiikkavälineen avulla, jolloin tunnistetaan vahvuudet ja kehityskohteet. Toisessa vaiheessa valmistellaan muutosta määrittelemällä strategia, joka voi vaihdella pienistä toimenpiteistä laajoihin interventioihin tietoturvakulttuurin ja vaatimustenmukaisuuden parantamiseksi. Kolmannessa vaiheessa hallitaan muutosta kehittämällä ja toteuttamalla toimenpidesuunnitelmia ADKAR-mallin (Awareness, Desire, Knowledge, Ability, Reinforcement) mukaisesti, jolloin vastuualueet ja aikataulut määritellään selkeästi. Viimeisessä vaiheessa vahvistetaan muutosta seuraamalla työntekijöiden käyttäytymisen kehittymistä ISCA-seurantamittauksilla, auditeilla ja jatkuvalla viestinnällä, jotta tietoturvakulttuurin muutos vakiinnutetaan pysyväksi osaksi organisaatiota. (Da Veiga 2018, 592.)

ENISAn askelmalli

ENISAn (Euroopan unionin kyberturvallisuusvirasto ENISA) malli tarjoaa konkreettisen askelmallin kyberturvallisuuskulttuurin kehittämiseen organisaatioissa. Se painottaa erityisesti johdon sitoutumista, koulutusta ja viestinnän merkitystä.

ENISAn (2017, 40) mallissa (kuva 10), edetään vaiheittain eteenpäin ja tähdätään kyberturvallisuuskulttuurin (Cyber Security Culture, CSC) parantamisen.



Kuva 10. Kyberturvakulttuurin rakentamisen ja kehittämisen askelmalli (ENISA 2017, 10)

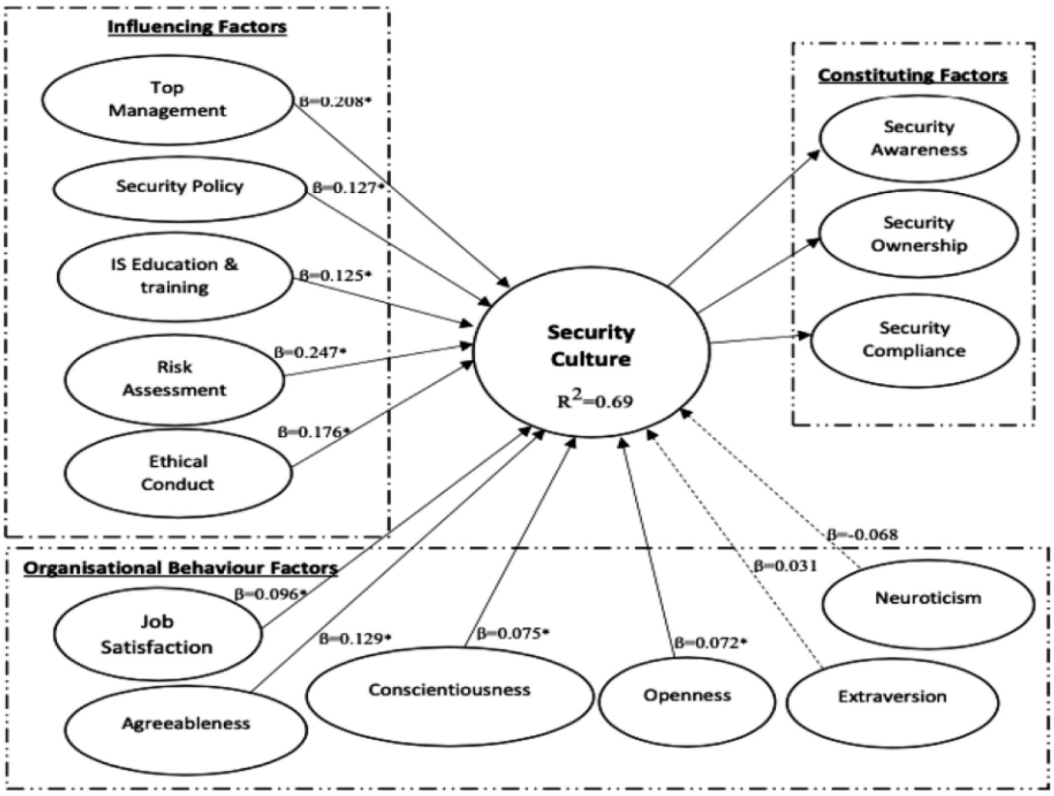
Ensimmäinen askel on kyberturvallisuustyöryhmän perustaminen, seuraavaksi on tehtävä nykytila-analyysi, jotta ymmärretään vallitsevaa kulttuuria ja liiketoiminnan riskejä. Kolmannessa askeleessa määritellään kyberturvallisuusprojektin päätavoitteet, mittarit ja kohderyhmät. Neljännessä vaiheessa tulee tehdä nykytilan ja tavoitetilan välinen arviointi. Viidennessä vaiheessa valitaan toimenpiteet, jotka tehdään (yksi tai useampia). Kuudennessa askeleessa suoritetaan valitut toimenpiteet. Seitsemännessä vaiheessa uusitaan neljännen vaiheen nykytilan ja tavoitetilan välinen analyysi, jotta selvitetään tehtyjen

toimenpiteiden vaikutus. Viimeinen eli kahdeksas vaihe palauttaa analysoimaan ja arvioimaan liiketoimintaa, riskejä ja kulttuuria sekä haluttuja kehitystoimia eli askeleita kaksi, kolme, neljä ja viisi ja näiden perusteella uusimaan polkumallin.

ISCFF (Information Security Culture and Key Factors Framework)

Tolah ym. (2017) esittelivät viitekehyksen, joka auttaa organisaatioita ymmärtämään, kehittämään ja arvioimaan tietoturvakulttuuriaan huomioimalla inhimilliset tekijät. Viitekehys perustuu Alnatheerin vuonna 2012 tieteellisesti validoituun malliin sekä laajaan kirjallisuuskatsaukseen ja sisältää kahdeksan keskeistä tekijää, jotka vaikuttavat tietoturvakulttuuriin. Näistä viisi – ylin johto, tietoturvapolitiikka, koulutus ja harjoittelu, tietoturvatietoisuus sekä tietoturvan omistajuus – on jo aiemmin todettu myönteisesti vaikuttaviksi, kun taas riskinarviointi ja eettinen toiminta ovat tärkeitä huomioitavia, vaikka niiden suoraa vaikutusta ei ole täysin todistettu. Tämä viitekehys tukee organisaatioita tehokkaan tietoturvahallinnan suunnittelussa ja toteutuksessa. (Tolah ym. 2017, 57.)

Tolah ym. (2021) suorittivat myöhemmin tutkimuksen, jonka tavoitteena oli kehittää ja validoida tekemänsä tietoturvakulttuurin viitekehys (ISCFF). Tutkimuksessa keskityttiin erityisesti siihen, mitkä tekijät vaikuttavat työntekijöiden käyttäytymiseen ja asenteisiin tietoturvakulttuurin suhteen. Tutkimuksen data kerättiin 266 työntekijältä eri maista ja organisaatioista. Otos sisälsi eri aloja, organisaatiotyyppejä ja hierarkiatason työntekijöitä. Tutkimus osoitti, että eri viitekehyksen tekijät vaikuttavat positiivisesti tietoturvakulttuuriin ja erityisesti turvallisuustietoisuuteen, omistajuuteen ja ohjeiden noudattamiseen (kuva 11). Tutkimuksen keskeiset havainnot tukevat aikaisempia tutkimuksia aiheesta.



Kuva 11. Information Security Culture and Key Factors Framework, ISCFF-rakennemalli tietoturvakulttuuriin vaikuttavista tekijöistä (Tolah 2021, 11)

Keskeiset tietoturvakulttuuriin vaikuttavat tekijät ja havainnot Tolahin ym. (2021) mukaan ovat seuraavat:

- Johtajuus ja turvallisuuspolitiikat – Ylin johto ja selkeät turvallisuuspolitiikat parantavat tietoturvakulttuuria.
- Koulutus ja tietoisuus – Turvallisuuskoulutuksen puute liittyy alhaisempaan tietoturvatietoisuuteen ja heikompaan ohjeiden noudattamiseen.
- Eettinen toiminta ja työtyytyväisyys - Eettiset toimintatavat ja korkea työtyytyväisyys edistävät positiivista tietoturvakulttuuria.
- Persoonallisuuspiirteet - Persoonallisuuden piirteet, kuten tunnollisuus ja sovinnollisuus, vaikuttavat positiivisesti tietoturvakäyttäytymiseen.
- Demograafisten tekijöiden vaikutus:
    - Organisaation tyyppi, sukupuoli ja maa vaikuttavat tietoturvakulttuurin kehittymiseen. Esimerkiksi julkisissa organisaatioissa työtyytyväisyydellä oli suurempi merkitys tietoturvakulttuurin parantamisessa kuin yksityisissä organisaatioissa.
    - Miehet osoittivat enemmän huolta riskianalyysistä kuin naiset.

4.4.3 Kehittämismallien vertailu ammattiliittojen näkökulmasta

Tässä alaotsikossa mallien vertailuun (taulukko 1) on käytetty ChatGPT (OpenAI, versio 4, tammikuu 2025) -tekoälyohjelmaa. Tekoälyä hyödynnettiin analysoimaan ja vertailemaan edellä esiteltyjä kyberturvallisuuskulttuurin viitekehyksiä ammattiliittokontekstissa, erityisesti arkaluonteisen tiedon suojaamisen näkökulmasta. Tekoälylle annettiin seuraavanlaisia kehotteita (prompteja):

- "Vertaa ISCF-, ISCCM-, ENISA- ja ISCFF-malleja ammattiliitoissa työskentelevien näkökulmasta ja niiden vaikutuksia arkaluonteisen tiedon suojaamiseen."
- "Keskitä analyysi inhimillisten virheiden minimointiin ja tietoturvakulttuurin kehittämiseen ammattiliittojen työntekijöiden kannalta."
- "Laadi taulukko, jossa vertaillaan mallien soveltuvuutta ammattiliitoissa käytettäväksi."

Tekoälyä käytettiin erityisesti strukturoimaan ja jäsentämään eri mallien vahvuuksia ja heikkouksia ammattiliittojen näkökulmasta. Lopullinen vertailu on tarkistettu ja täydennetty tämän opinnäytetyön tekijän toimesta varmistaen, että se vastaa työn tavoitteita ja soveltuu akateemiseen käyttöön.

Kuten olemme tutustuneet, malleja on erilaisia ja niissä on samoja piirteitä. Mallit perustuvat tutkijoiden näkemyksiin, osin abstrakteihin käsitteisiin ei niinkään konkreettisiin asioihin. Mitä mallia pitäisi käyttää lähtökohtana kuvaamaan ammattiliiton kyberturvallisuuden tilaa tai lähteä kehittämään sitä?

Scheinin malli on usein perinteisesti lähtökohtana organisaation ainutlaatuisen kulttuurin ymmärtämisessä, painottaen ääneen lausuttuja uskomuksia ja arvoja kulttuurin mittaamisessa. Mallin taustalla olevat oletukset ovat vaikeasti arvioitavissa, mutta ne ovat keskeisiä ymmärtämään, miten ihmiset työskentelevät ja tekevät päätöksiä organisaatiossa. Vaikka Scheinin mallia on laajasti käytetty tietoturvakulttuurin tutkimusten teoreettisena perustana, sen abstraktit ulottuvuudet tekevät sen soveltamisesta yksittäisiin organisaatioihin haastavaa. (Sutton & Tompson 2024, 148.)

Uusin vertailun ulkopuolelle jätetty lähestymistapa kyberturvallisuuskulttuurin ymmärtämiseen on integroitu kyberturvallisuuskulttuurin viitekehys (CSC framework), jonka esittelivät Sutton ja Tompson (2024). Tämä malli yhdistää kolme keskeistä elementtiä: kulttuuriarvot, kulttuurin ja käyttäytymisen välisen yhteyden sekä itse käyttäytymisen. Viitekehyksen tavoitteena on tarjota kokonaisvaltainen näkemys siitä, miten organisaation arvot ja toimintaympäristö vaikuttavat työntekijöiden tietoturvakäyttäytymiseen. Toisin kuin Da Veiga & Eloff:n ISCA-malli, joka keskittyy tietoturvakulttuurin arviointiin määrällisin mittarein, uusin tarjottu viitekehys pyrkii yhdistämään sekä kulttuuriset että käyttäytymiseen liittyvät tekijät kokonaisvaltaiseksi lähestymistavaksi. Tämä tuo uuden näkökulman perinteisiin tietoturvakulttuurin arviointimenetelmiin ja voi toimia täydentävänä työkaluna esimerkiksi ISCA-mallin rinnalla. Mallin konkretia on kuitenkin tutkimuksessa melko abstraktilla tasolla, eikä siitä ole pääteltävissä tämän tutkimuksen tueksi enempää johtopäätöksiä.

Inhimillisten virheiden minimoinnissa erityisesti ammattiliittojen kontekstissa ISCCM ja ENISA-malli ovat tehokkaimpia, koska ne tarjoavat konkreettisia työkaluja työntekijöiden tietoturvakäyttäytymisen muuttamiseen. ISCCM soveltuu erityisesti siksi, koska se perustuu pitkäjänteiseen muutoksenhallintaa, jolloin työntekijät sitoutuvat tietoturvakäytäntöihin todennäköisesti paremmin. Arkaluonteisten jäsentietojen suojaamisessa ENISA askelmalli auttaa kehittämään selkeitä ohjeita ja käytäntöjä, jotka suojaavat arkaluonteisia henkilötietoja ja ehkäisevät mahdollisia tietovuotoja. ISCF ja ISCFF tunnistavat organisaation sisäiset tietoturvariskit mutta eivät suoraan ilman apuvälineitä tarjoa konkreettisia työkaluja niiden ratkaisemiseen. Jos tavoitteena on muuttaa työntekijöiden tietoturvakäyttäytymistä pitkälle aikavälillä, ISCCM on paras vaihtoehto, sillä se keskittyy kulttuurin muutoksenhallintaan ja asenteisiin. Jos taas halutaan selkeät vaiheet tietoturvan parantamiseksi, ENISA askelmallin on käytännönläheisin työkalu. Jos tietoturvakulttuurin nykytilan arviointi on tärkein vaihe, ISCF ja ISCFF voivat toimia parhaiten, joskaan ne eivät tarjoa suoria toimintamalleja jatkolle.

Taulukko 1. Kyberturvallisuuden kehittämisen viitekehysten vertailu

Malli	Keskeinen tavoite	Inhimillisten virheiden minimointi	Vaikutus jäsentietojen suojaamiseen	Soveltuvuus ammattiliittoihin
ISCF (Information Security Culture Framework)	Kokonaisvaltainen ymmärrys tietoturvakulttuurin muodostumisesta organisaatioissa.	Tunnistaa organisaatiokulttuurin vaikutuksen työntekijöiden tietoturvakäyttäytymiseen.	Auttaa ymmärtämään, miksi tietoturvapuutteet syntyvät ja miten organisaatiokulttuuri vaikuttaa arkaluonteisen tiedon käsittelyyn.	**Hyödyllinen lähtökohta**, mutta ei tarjoa konkreettisia muutosstrategioita tai käytännön ohjeita.
ISCCM (Information Security Culture Change Management)	Tietoturvakulttuurin muutoksenhallinta ja käyttäytymisen ohjaaminen.	Mahdollistaa tietoturvakäyttäytymisen kehittämisen suunnitelmallisesti, esim. koulutuksen ja kannustinjärjestelmien avulla.	Auttaa muuttamaan työntekijöiden toimintatapoja niin, että inhimilliset virheet vähenevät ja tietoturvariskit minimoidaan.	**Sopii erinomaisesti ammattiliitoille**, jos halutaan pitkäjänteisesti kehittää turvallisuuskulttuuria ja parantaa ohjeistusten noudattamista.
ENISAn askelmalli	Tietoturvakulttuurin kehittäminen vaiheittain (arviointi, suunnittelu, toteutus, seuranta).	Tarjoaa käytännönläheiset vaiheet, joilla voidaan vähentää inhimillisiä virheitä selkeillä prosesseilla ja ohjeilla.	Parantaa arkaluonteisten tietojen suojaamista strukturoimalla turvallisuuskäytännöt ja varmistamalla jatkuvan seurannan.	**Erittäin käyttökelpoinen ammattiliitoille**, koska tarjoaa selkeät askeleet tietoturvakulttuurin vahvistamiseen ja käytännön ohjeistusten laatimiseen.
ISCFF (Information Security Culture and Key Factors Framework)	Tietoturvakulttuuriin vaikuttavien keskeisten tekijöiden tunnistaminen.	Auttaa tunnistamaan, mitkä tekijät, kuten johto ja koulutus, vaikuttavat tietoturvakäyttäytymiseen.	Ei tarjoa suoria ratkaisuja tiedon suojaamiseen, mutta auttaa ymmärtämään, mitkä tekijät vaativat kehitystä.	**Hyödyllinen ammattiliitoille, jos halutaan tunnistaa tietoturvakulttuurin heikkoudet ja vahvuudet.**

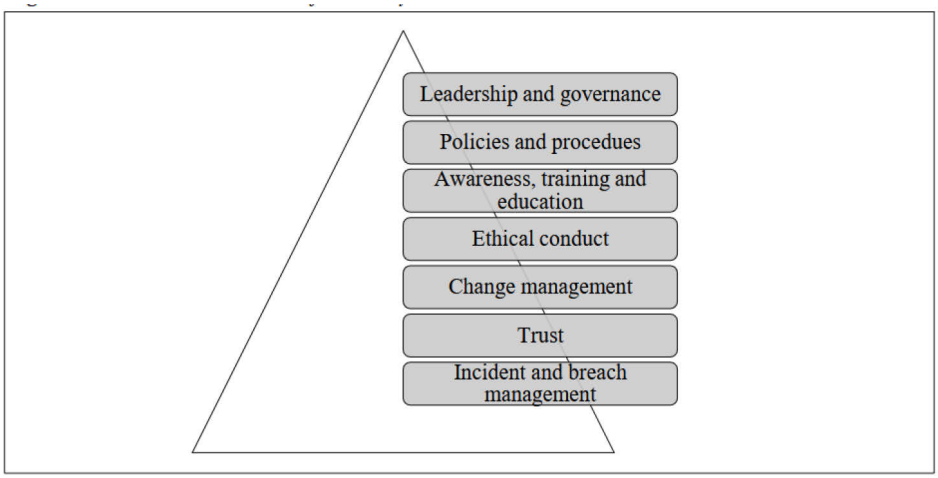
Tämän tutkimuksen tekijän loppupäätelmä mallien sopivuudesta ammattiliitoille on se, että jos tavoitteena on rakentaa ja kehittää kyberturvallisuuskulttuuria ja saada siihen tueksi selkeitä työkaluja, paras lähtökohta on ENISAn malli. Päätelmä perustuu mallin käytännönläheisiin ja selkeisiin askelmiin sekä mallin rakennus eurooppalaisesta kontekstista ajatellen EU-alueen yhteisiä toimintatapoja ja velvoitteita kuten EU yleistä tietosuoja-asetusta.

4.4.4 Kyberturvallisuuskulttuurin kehittämisen strategiset tasot

Da Veiga (2019) mukaan kyberturvallisuuskulttuurin kehittäminen edellyttää kokonaisvaltaista lähestymistapaa, jonka perustana ovat seuraavat elementit (kuva 12):

- johtajuus

- selkeät politiikat
- tehokas koulutus
- eettiset periaatteet
- muutoksen hallinta
- luottamukseen perustuva vuorovaikutus ja
- poikkeamien hallinta.



Kuva 12. Peruselementit turvallisuuskulttuurin rakentamiselle ja kehittämiselle (Da Veiga 2019)

Da Veiga (2019) avaa elementtejä niin, että johto asettaa tietoturvan strategiset linjaukset ja varmistaa resurssien sekä hallintorakenteiden avulla, että tietoturva integroidaan organisaation toimintaan. Johdon esimerkki, sitoutuminen ja selkeät vastuunjaot ovat olennaisia vahvan tietoturvakulttuurin edistämiseksi. Tietoturvakäytännöt eli politiikat ja ohjeet ohjaavat työntekijöiden käyttäytymistä, mutta pelkkä politiikkojen olemassaolo ei riitä. Koulutuksen, tietoisuuden lisäämisen ja palkitsemisen yhdistäminen parantaa sääntöjen noudattamista ja kulttuuria. Johdon ja työntekijöiden välinen luottamus on keskeistä tiedon jakamisen ja sitoutumisen edistämiseksi. Työntekijöiden tulee ymmärtää, mikä on tietoturvapoikkeama, kenelle se raportoidaan ja miten toimitaan tilanteessa. Kohdennetut interventiot (esimerkiksi alakulttuureihin) voivat merkittävästi parantaa työntekijöiden valmiuksia poikkeamien käsittelyssä.

Da Veigan (2019) mukaan tutkimukset osoittavat (Chen, Ramamurthy & Wen 2015, Whittman & Mattord 2012, Da Veigan 2019, mukaan), että sääntöjen noudattaminen riippuu ensinnäkin yrityksen kulttuurista palkita tai toisaalta rangaista sääntöjen rikkomuksista. Toisin sanoen, joissain organisaatioissa

voi toimia se, että tietoturvaohjeiden noudattaminen on osa henkilökohtaista suoriutumisen arviointia = palkitseminen. Jos sääntöjen rikkomisesta seuraa sanktio, sen pelko toimii kannustimena noudattaa ohjeita. Toisaalta Tolahin ym. (2021) tutkimuksen mukaan työntekijöiden positiivinen työtyytyväisyys vaikuttaa myönteisesti tietoturvakulttuuriin. Jos sanktiot ovat pääosassa, työtyytyväisyys ei todennäköisesti ole parhaimmillaan.

Joka tapauksessa Da Veiga (2019) toteaa, että tietoturvatietoisuutta lisäävät ohjelmat ja koulutukset ovat ratkaisevan tärkeitä työntekijöiden osaamisen lisäämiseksi ja virheiden vähentämiseksi. Ohjelmat voidaan kohdentaa organisaation tarpeisiin, ja niiden tehokkuutta tulee arvioida säännöllisesti. Tietoturva-alan ammattilaisia ohjaavat eettiset ohjeet, mutta työntekijöiden erilaiset eettiset näkemykset voivat poiketa näistä ja tämä vaatii koulutusta, jotta ne ovat linjassa organisaation arvojen kanssa.

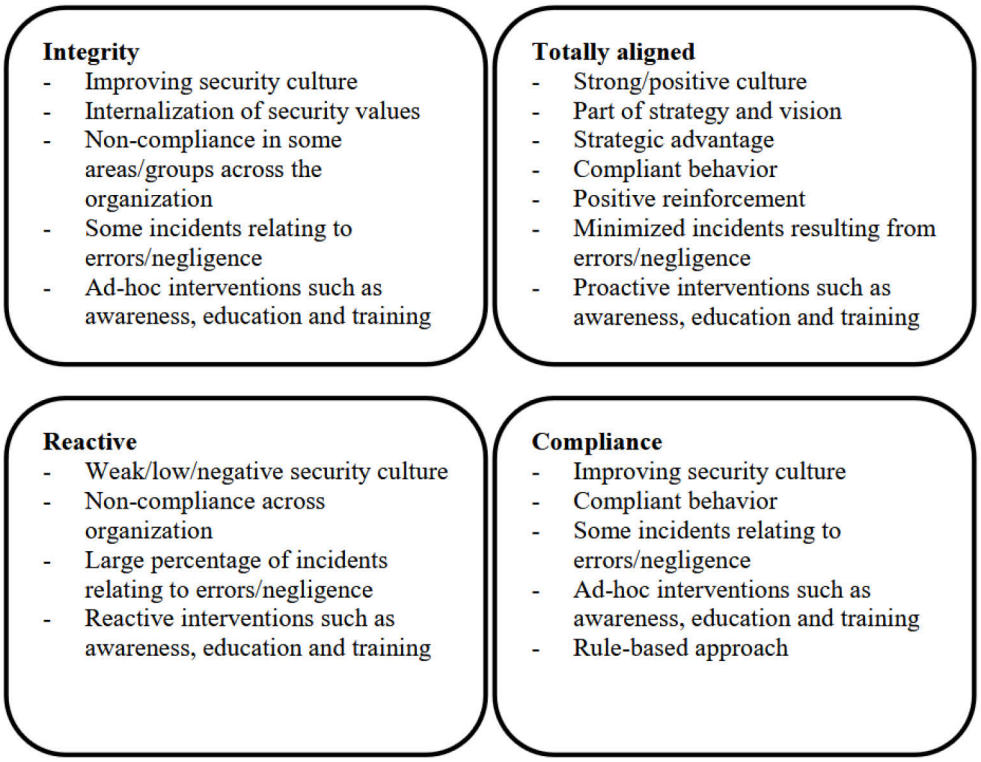
Vahva tietoturvakulttuuri vaatii systemaattista muutoksenhallintaa. Muutoksenhallintamallit (esim ADKAR) tarjoavat viitekehyksen tehokkaalle tavalle muutoksen implementoinnille ja vaikutusten seurannalle.

ENISAn (2017) viitekehys tietoturvakulttuurin kehittämiseksi mukailee edellä mainittuja elementtejä. Johdon sitoutuminen on senkin mukaan ensimmäinen askel. Seuraava askel on arvioida työntekijöiden suhtautuminen ja asenteet tietoturvaan liittyen eli toisin sanoen nykytila-analyysi, josta johdetaan tavoitetila ja määritellään tarvittavat kehitysaskeleet. Lisäksi työntekijöiden koulutus on yksi avaintekijöistä, kuten muissakin malleissa. Kehitysaskeleiden seurannan tueksi on määriteltävä mittaristo. Palaute, palkitseminen ja rangaistukset on myös suunniteltava etukäteen. ENISAn malli korostaa myös tavoitteiden jatkuvaa arviointia ja uudelleenanalysointia.

Da Veigan (2019) mukaan organisaation tietoturvakulttuurin maturiteettitasoa voidaan kuvata neljän strategisen tason avulla (kuva 13) seuraavasti:

1. Reaktiivinen
    - Toimitaan vain tapahtuneiden tietoturvaongelmien jälkeen. Työntekijöiden koulutus on satunnaista ja tilannekohtaista.

2. Sääntöihin perustuva (compliance)
    - Keskitytään sääntöjen ja määräysten noudattamiseen sekä itsearviointeihin ja auditointeihin. Tämä lähestymistapa on sääntöpohjainen, mutta ei ole kiinteä osa organisaation toimintaa.
3. Integriteettiin pohjautuva
    - Proaktiivisia toimia (esim. koulutukset ja tietoisuuden lisääminen) toteutetaan, mutta ne eivät ole täysin integroituja organisaation strategiaan.
4. Täysin linjassa oleva (totally aligned)
    - Ihanteellinen tilanne, jossa tietoturvakulttuuri on sisällytetty organisaation strategiaan ja visioon.
    - Johto toimii proaktiivisesti, käyttää resursseja tietoturvakulttuurin vahvistamiseen ja palkitsee positiivista ja sääntöjen mukaista käyttäytymistä.
    - Tuloksena vahva tietoturvakulttuuri, jossa työntekijät ymmärtävät vastuunsa ja tietoturvapoikkeamat vähenevät.



Kuva 13. Turvallisuuskulttuurin strategisen kehittämisen tasot (Da Veiga 2019)

Da Veigan (2019) mukaan organisaation tavoitteena tulisi olla täysin linjassa oleva tietoturvakulttuuri, jossa tietoturva on osa organisaation strategiaa, työntekijöiden toimintaa ohjataan proaktiivisesti, ja poikkeamat minimoidaan. Tämä eroaa heikommista strategioista, jotka ovat reaktiivisia tai sääntöihin keskittyviä mutta irrallisia organisaation kokonaisuudesta.

4.4.5 Kyberturvallisuuskulttuurin kehittäminen pienissä ja keskisuurissa yrityksissä kuten ammattiliitoissa

Euroopan unioni on maailman suurin yhtenäismarkkina-alue ja samalla maailman suurin talous. Monet saattavat ajatella, että tämä markkinakoko johtuu suurista organisaatioista ja monikansallisista yrityksistä. Vaikka nämä ovatkin tärkeitä EU:n talouden kannalta, pienet ja keskisuuret yritykset (pk-yritykset) muodostavat sen selkärangan. Pk-yritykset toimivat sekä digitaalisen muutoksen mahdollistajina että EU:n yhteiskunnallisen rakenteen keskeisenä osana. (ENISA 2021, 3.)

COVID-19-kriisi osoitti, kuinka tärkeitä internet ja tietokoneet ovat myös pk-yrityksille liiketoiminnan ylläpitämisessä ja toisaalta, juuri heille se oli haastava urakka verrattuna suuryrityksiin. Selviytyäkseen pandemiasta ja jatkaakseen toimintaansa monet pk-yritykset joutuivat ottamaan käyttöön liiketoiminnan jatkuvuutta tukevia toimenpiteitä, kuten siirtymään pilvipalveluihin, päivittämään internet-yhteyksiään, parantamaan verkkosivustojaan ja mahdollistamaan etätyöskentelyn henkilöstölleen. (ENISA 2021, 3.)

ENISA (2021,3) suoritti digitaaliturvallisuudesta kyselyn pk-yrityksille pandemian jälkeen. Kyselyyn osallistui 249 eurooppalaista yritystä. Tutkimus osoitti, että suurimmat haasteet pk-yrityksille ovat:

- Heikko tietoisuus kyberturvallisuusuhkista ja niiden vaikutuksista liiketoimintaan.
- Kyberturvallisuustoimenpiteiden korkeat kustannukset, usein yhdistettynä erillisen budjetin puutteeseen.
- ICT-kyberturvallisuusasiantuntijoiden saatavuuden rajallisuus.
- Pk-yrityksille suunnattujen selkeiden ohjeistusten puute.
- Johdon vähäinen tuki kyberturvallisuustoimille.

ENISA (2021,3) toteaa yhteenvetona, että Euroopan unionin pk-yritykset ymmärtävät kyberturvallisuuden olevan tärkeä kysymys ja ovat erittäin riippuvaisia ICT-infrastruktuuristaan. Kyselyyn vastanneista pk-yrityksistä yli 80 % ilmoitti, että kyberturvallisuusongelmilla olisi vakava negatiivinen vaikutus liiketoimintaa jo viikon sisällä niiden ilmenemisestä, ja 57 % arvioi, että ne todennäköisesti ajautuisivat konkurssiin tai joutuisivat lopettamaan toimintansa. Tästä huolimatta pk-yritykset eivät aina ymmärrä, että kyberturvallisuus ei koske vain suuria organisaatioita. Siksi niiden on tiedostettava, kuinka merkittäviä vaikutuksia kyberturvallisuusongelmilla voi olla niiden liiketoiminnalle. Monet pk-yritykset uskovat, että heidän hankkimiensa IT-tuotteiden mukana tulevat kyberturvallisuusominaisuudet ovat riittäviä, vaikka näin ei välttämättä ole.

ENISA (2021, 4) suosittelee tiivistettynä pk-yrityksille keskittymistä seuraaviin kolmeen osa-alueeseen:

1. Ihmiset
2. Prosessit
3. Teknologia

Edellä mainittuihin sisältyy muun muassa ohjelmistojen ajan tasalla pitäminen, tiukkojen pääsynhallintasääntöjen soveltaminen, pilvipalveluiden hyödyntäminen, kyberhäiriöihin varautumissuunnitelman laatiminen.

Käsiteltävän tiedon määrä on isoissa yrityksissä luonnollisesti suurempi mutta pienet ja keskisuuret yritykset (pk-yritykset) operoivat samassa kybertoimintaympäristössä kuin isommatkin. Samat inhimilliset riskit ja vaarat vaanivat niin isoja kuin pieniä yrityksiä ja toisaalta, samat tietosuojaan liittyvät vaatimukset on otettava huomioon, toimipa pienessä tai isossa yrityksessä. Pk-yrityksillä on usein kuitenkin käytössään isoja rajallisemmat resurssit, puutetta osaamisesta, rahasta ja ajasta, mikä vaikeuttaa investointeja ja panostuksia tieto- ja kyberturvaan. Da Veiga (2019) korostaa, että pk-yritysten on silti panostettava välttämättömien teknologioiden ja prosessien hallintaan sekä vahvistettava tietoturvakulttuuria koulutuksen, tietoisuuden lisäämisen ja henkilöstön opettamisen avulla.

Tässä tutkimuksessa on keskitytty havaintojen ja tulosten esittämiseen nimenomaan pienten ja keskisuurten organisaatioiden, tarkemmin ammattiliittojen näkökulmasta, joiden ydintoiminta on tarjota palveluja ja etuja henkilöjäsenille. Kyberturvallisuuden toteutuminen arkaluonteisen henkilötiedon takia on ensiarvoisen tärkeää, vaikka ydintoiminta on kaikkea muuta kuin tekniikkaa. Ammattiliittojen on syytä ymmärtää, miten kyberturvallisuus liittyy toimintaan ja miksi sen ylläpito on tärkeää, miten vaikuttaa ihmisten käyttäytymiseen tai miten kyberturvallisuuden kehittämisessä pääsee liikkeelle, esimerkiksi käyttämällä valmiita viitekehyksiä ja arviointimenetelmiä.

4.5 Kyberturvallisuus

Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan (Turvallisuuskomitea 2018, 22). Kyber tarkoittaa digitaalista maailmaa; kaikessa laajuudessaan sitä bittien maailmaa, joka ympärillämme on ja joka liittyy kaikkeen päivittäiseen elämäämme. Isommin kuin aina edes osaamme ajatella. Käsitteenä se usein rinnastuu kybertoimintaympäristöön tai kybermaailmaan. (Limnéll ym. 2014, 29.)

Kyberturvallisuus-termi tuli Suomeen vuonna 2011, jolloin valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta päätti käynnistää kansallisen kyberturvallisuusstrategian laatimisen (Järvinen 2018, 13). Kybermaailmasta ja kyberturvallisuudesta on sittemmin tullut erottamaton osa arkipäiväämme.

Maailmantalous, yhteiskuntien turvallisuus, yritysten toiminta ja elämäntapamme ovat tänä päivänä hyvin riippuvaisia bittien toimivuudesta. Limnéll ym. (2014, 13) kysyvätkin: ”Entä jos bitit eivät toimikaan tai emme voi luottaa kybermaailman toimivuuden turvallisuuteen?” Limnéll ym. jatkavat toteamalla, että merkittävimmät puutteet kyberturvallisuudessa liittyvät siihen, että sitä pidetään teknologisena asiana. Tämän päivän digitalisoituneessa maailmassa kyberturvallisuus on kuitenkin mitä suurimmissa määrin strateginen ja poliittinen asia, jossa ”ison kuvan ja suunnan määrittämisen” ymmärrys on valitettavan heikkoa. (Limnéll ym. 2014, 13.)

Kybermaailman negatiivinen puoli muodostuu uhkista ja erilaisista epävarmuuksista. Kyberturvallisuudella suojaudutaan negatiivisilta tekijöiltä, ennaltaehkäistään tai torjutaan niitä sekä lievennetään niiden vaikutuksia. Negatiivisen puolen jäsentämiseen liittyy Limnéllin ym. (2014, 105) mukaan seuraavat kolme käsitettä:

1. **Uhka**
   Kyberuhka tarkoittaa digitaalisen järjestelmän turvallisuutta vaarantavaa uhkaa.
2. **Riski**
   Kyberriski on mahdollisuus, että kyberuhka toteutuu ja aiheuttaa vahinkoa organisaatiolle, yksilölle tai yhteiskunnalle.
3. **Haavoittuvuus**
   Haavoittuvuus tarkoittaa tietojärjestelmän, ohjelmiston tai verkon heikkoutta tai puutetta, jota kyberuhat voivat hyödyntää.

On huomioitava, että uhka voi tulla myös organisaation sisältä, ihmisen tekemänä. Keskittymällä teknisiin suojauskeinoihin ei poista ihmisen aiheuttamaa uhkaa (Ejigu ym. 2021, 2). Saxena ym. (2020, 3) jakavat organisaation sisältä henkilöstöstä tulevat uhkat kolmeen eri kategoriaan, joista syntyviä uhkia on minimoitava eri tavoilla:

1. **Ilkeämielinen sisäpiiriläinen**
   Ilkeämielinen sisäpiiriläinen käyttää tahallisesti omia oikeutettuja tunnuksiaan väärin varastaakseen tietoja taloudellisen tai henkilökohtaisen hyödyn vuoksi. Esimerkiksi työntekijä, joka ei pidä työnantajastaan, voi myydä luottamuksellisia tietoja kilpailijalle.
2. **Tietojenkalastelun uhriksi joutunut sisäpiiriläinen**
   Hyväksikäytetty sisäpiiriläinen on henkilö, jonka käyttäjätunnukset on varastettu ja jota hyökkääjä käyttää hyödykseen. Hyökkääjä voi esimerkiksi kerätä sisäpiiriläisen kirjautumistiedot sosiaalisen manipuloinnin avulla ja käyttää niitä päästäkseen käsiksi arkaluonteisiin tietoihin, kuten organisaation immateriaalioikeuksiin tai henkilötietoihin.
3. **Huolimaton sisäpiiriläinen**
   Huolimattomat sisäpiiriläiset tekevät yleisimpiä virheitä ja kiinnittävät

yleensä vain vähän huomiota organisaation tietoturvakäytäntöihin. He voivat tietämättään altistaa organisaation resursseja ulkopuolisille. Esimerkiksi työntekijä voi klikata epävarmaa linkkiä tajuamatta sen tietoturvariskiä, mikä voi antaa ulkopuolisille pääsyn järjestelmään tai kriittisiin resursseihin.

Epätavallinen toiminta voi olla merkki sisäisestä uhasta. Esimerkkejä tällaisesta toiminnasta ovat järjestelmän käyttö epätavallisiin aikoihin (esim. kirjautuminen järjestelmään myöhään yöllä), suuri tietoliikennemäärä (esim. liian suuren datamäärän siirtäminen verkossa) sekä poikkeava tai epätyypillinen toiminta (esim. pääsy epätavallisiin laitteisiin tai tietokantoihin). (Saxena 2020, 3.)

Kyberturvallisuus koostuu kokonaisvaltaisesta tietoisuudesta. Kyberturvaa uhkaa erilaiset tekijät, jotka on tunnistettava ja mietittävä keinot suojautumiselle. Keinoja ovat niin tekniset, hallinnolliset kuin koulutus. Sisäisen uhkan vaaraa ei kannata unohtaa tai keskittyä vain tekniikkaan.

4.5.1 Kyberturva vs. tietoturva

Arkikielessä termit kyberturva ja tietoturva tarkoittavat usein samaa asiaa. Niillä on kuitenkin selvä ero. Tietoturva pyrkii tietojen, tiedostojen ja yksittäisten koneiden suojaamiseen (Järvinen 2018, 14). Kyberturvallisuus sisältää aina tietoturvan mutta tarkoittaa laajemmin tietoverkkojen, järjestelmien ja infrastruktuurin turvallisuutta. Järvinen (2018, 16) käyttää termiä kyberturvallisuus viittaamaan tietoturvaan, joka koskee arjen infrastruktuuria ja maanpuolustusta. Hänen mukaansa sähkö, vesi, liikenteen ohjaus, terveydenhuolto, kauppa, logistiikka ja monet muut asiat toimivat tietokoneiden ja verkkojen varassa. Jos niiden tietoturva pettää, kyse ei ole vain menetetyistä tiedostoista tai taloudellisista tappioista – vaarassa ovat ihmisten hyvinvointi ja henki.

Tietoturva ei ole vain tekniikkaa. Tietoturva mielletään usein tekniseksi, it-tuen asiaksi. Näin saattoi varmasti tietokoneiden alkuaikoina ja yleistyessä ollakin. Suurimmat ongelmat liittyivät itse fyysisiin laitteisiin ja niiden korjaamiseen tarvittiin it-tukea. Nykyään tekniikka on parempaa mutta ihminen ei ole muuttunut kuten Petteri Järvinen (2022, 32) toteaa. Verizonen 2024 tutkimuksen (2024,

2) mukaan inhimillinen tekijä on ollut mukana lähes 70 % hyökkäyksistä. Ihmiset ovat huolimattomia, väsyneitä ja joskus suorastaan piittaamattomia. On kiire, monta tehtävää samanaikaisesti hoidettavana, useita salasanoja muistettavana ym. Ihmistä on helppo erehdyttää ja huijata. Tietoturvan tärkein tavoite onkin saada ihmiset toimimaan oikein, muistamaan ohjeet ja noudattamaan niitä. (Järvinen 2022, 32.) Tästä huolimatta tietoturva on useimmiten edelleen it-osaston vastuulla, eivätkä he ole parhaita henkilöitä viestimään aiheesta muulle henkilökunnalle.

Kyberturva ei ole vain vahvojen salasanojen, anti-virus- tai palomuuriohjelmistojen käyttöä. Kyberturvallisuus ei ole tekninen asia, joka kiinnostaa alan ihmisiä. Kyberturva on prosessi, joka vaatii kaikkien toimijoiden yhteispeliä normaalista tietokoneenkäyttäjästä it-spesialistiin asti. Kyberturvallisuus on kokonaisvaltainen sarja toimintoja, jotka tähtäävät kybertoimintaympäristöä uhkaavien tekijöiden torjumiseen. Tehokkaan kyberturvallisuuden tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys kaikenlaisilta uhilta ja vahingoilta. (Sevgi 2021, 82.)

Kyberturva ja tietoturva ovat koko organisaation asioita. Kokemukset osoittavat, että kun koko organisaatio jakaa yhteisen tavan ajatella haavoittuvuuksia, tietoturvaa voidaan parantaa merkittävästi (Boehm ym. 2019, 7).

4.5.2 Kyberturvallisuuden parhaat käytännöt ja johtaminen

Henkilökunnan **kyberhygieniatietoisuuden** kasvattaminen on ensiarvoisen tärkeää. Jokainen henkilötietoja käsittelevä on saatettava tietoiseksi miten oma toiminta voi vaikuttaa koko organisaation kyberturvallisuuteen. Jo peruskyberhygienian säännöillä, kuten salasanakäytännöillä ja koneen ja laitteiden käsittelyyn liittyvillä ohjeistuksilla kasvatetaan organisaation kyberresilienssiä eli vastustuskykyä.

Kyberturvallisuuden tasoa ei nosteta pelottelemalla vaan **jatkuvalla innovatiivisella kouluttamisella**. Koulutuksien on oltava jatkuvia ja säännöllisiä. Ohjeiden on hyvä olla pureskeltu helposti ymmärrettävään muotoon, jotta aiheet ymmärretään ja pystytään omaksumaan osaksi jokapäiväisiä toimia. Inhimilli-

nen erhe voidaan karsia minimiin, kun henkilökuntaa motivoidaan ja kannustetaan positiivisesti. Kyberturvallisuuden faktat, kuten riskit ja ajankohtainen tieto, on syytä tuoda esiin mutta sillä tasolla, joka on koko henkilökunnan kannalta omaksuttavissa. Henkilökunnalle on hyvä järjestää testejä tai muita harjoituksia turvallisessa ympäristössä. On olemassa valmiita ohjelmistoja ja yrityksiä, jotka voidaan valjastaa lisäresurssiksi.

Tietoturvatiimeille **harjoittelu** on avain onnistumiseen. Säännölliset pöytäharjoitukset tai simulaatiot auttavat tunnistamaan aukkoja ja poistamaan heikkouksia kyberturvallisuuskäytännöissä. (CrowdStrike 2024, 55.)

Monesti kuulee edelleen sanottavan, että tietoturva, kyberturva tai jopa tietosuoja on ”it-hommia” tai teknisiä toimenpiteitä. Jos ammattiliitossa ajatellaan näin, on monesti puute **johtamisessa**. Johdon tulee ymmärtää, että kyberturvan tulee olla osa ammattiliiton strategisia tavoitteita, eikä vain tekninen kuluerä. Osoittamalla resursseja mm. tietosuoja- ja tietoturvavastaavalle ja hyväksymällä ja seuraamalla, että kyberturvallisuutta hoidetaan systemaattisesti niin hallinnollisesti kuin teknisesti, johto omalta osalta on luomassa kyberturvallisuuskulttuuria. Järvinen (2022, 27) muistuttaa, että tietosuojavastaava ei vastaa yrityksen tietosuojasta, vaan vastuussa ovat aina yrityksen toimiva johto ja hallitus. Sama pätee tieto- tai kyberturvaan.

Tietoturvan **hallintamalli** on strateginen kuvaus tavasta, jolla kyberturvallisuutta toteutetaan. Hallintamalli määrittelee ylätasolla elementit, tavat ja dokumentit, joilla varmistetaan organisaation kyberturvallisuuden taso. Hallintamalli on siis kattoasiakirja, joka ohjaa kaikkia tietoturvatoimia organisaatiossa. **Tietoturvastrategia, -politiikka tai -periaatteet** ovat kuvauksia konkreettisista kyberturvatoimenpiteistä ja ohjeistuksista. Tietoturvapolitiikka, englanniksi Information security policy (ISP) on dokumentti, jossa linjataan organisaation tietoturvan hallintaan liittyvät periaatteet.

Nämä kaikki edellä mainitut kokonaisuudet tähtäävät vahvan kyberturvallisuuskulttuurin rakentamiseen organisaatioon. Parhaiden käytäntöjen käyttöönoton tueksi on olemassa erilaisia viitekehyksiä ja standardeja, kuten ISO 27001-standardi tai NIST-viitekehykset.

4.5.3 Riskienhallinta osana kyberturvallisuutta

Riskienhallinta on keskeinen osa kyberturvallisuuden hallintamallia. Riskienhallinnalla pyritään tunnistamaan organisaatiota koskevat kyberturvariskit, arvioimaan niiden vaikutuksia liiketoiminnan kannalta sekä määrittelemään kontrollit, joilla riskejä pyritään alentamaan hyväksyttävälle tasolle. Kyberturvallisuuden riskit on sisällytettävä osaksi organisaation kokonaisriskienhallintaa. Organisaation on ymmärrettävä, että kyberriskit ovat lähes poikkeuksetta liiketoiminnan kannalta kriittisiä. Riskienhallinta koostuu Limnéllin ym. (2014, 110) mukaan seuraavista osatekijöistä:

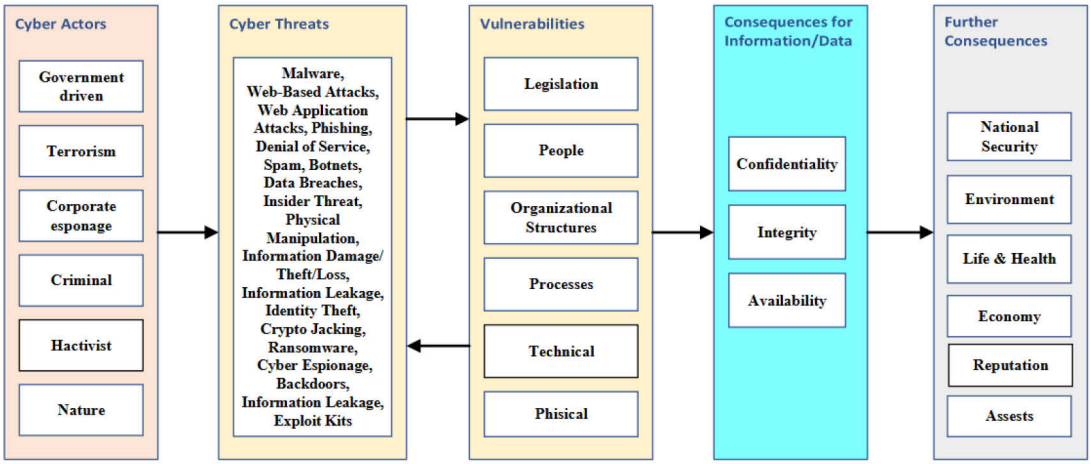
- *riskienhallinnan suunnittelusta*
- *riskien aikaisesta tunnistamisesta ja analysoinnista*
- *jatkuvasta riskien kehittymisen seurannasta ja niiden uudelleen arvioimisesta*
- *korjaavien toimien suorittamisesta*
- *riittävästä viestinnästä, raportoinnista ja muusta dokumentaatiosta sekä koordinaatiosta.*

Näin ollen riskienhallinnan täytyy olla suunnitelmallista ja koordinoitua sekä johdettua. Sitä ei voi tehdä satunnaisesti vaan säännöllisesti kytkettynä esimerkiksi johdon vuosikelloon. Riskienhallinta on siis koko yrityksen kattava johdettu toiminto, jonka osana on kyberriskien analysointi.

Riskienhallinnan yhteydessä on hyvä tunnistaa keskeiset osatekijät ja näiden väliset yhteydet. Hoffmann ym. (2020, 657) esittävät selkeästi (kuva 14), mistä osatekijöistä kyberriski muodostuu. Näitä ovat seuraavat:

- kybertoimijat
- kyberuhat
- haavoittuvuudet
- tietoon kohdistuvat seuraukset

- jatkoseuraukset.



Kuva 14. Kyberriskien osatekijät (Hoffmann 2020, 657)

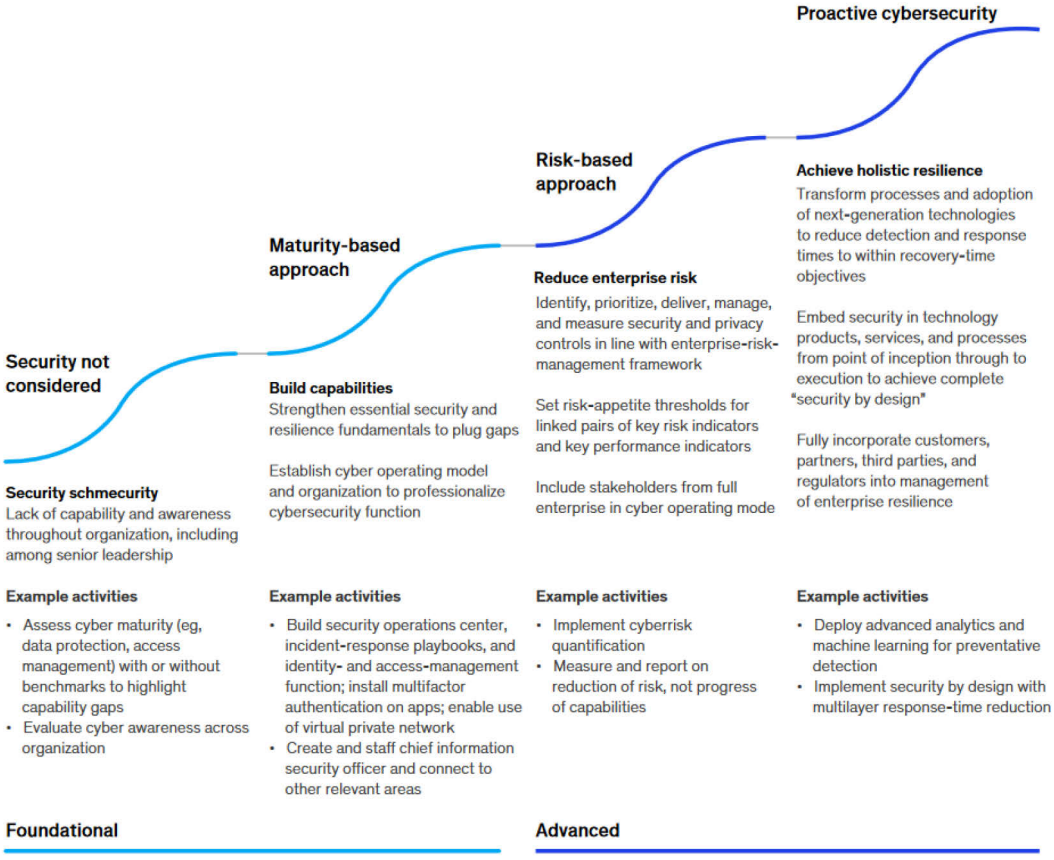
Kybertoimijat voivat aiheuttaa uhkia hyödyntämällä erilaisia haavoittuvuuksia, mikä voi johtaa vakaviin seurauksiin organisaation tiedoille ja toiminnalle. Näiden uhkien hallinta edellyttää systemaattista riskienhallintaa, joka keskittyy erityisesti kriittisten haavoittuvuuksien tunnistamiseen ja minimointiin.

McKinsey & companyn artikkeli (Boehm ym. 2019, 2) huomauttaa kyberuhan ja kyberriskin erosta. Kyberuhka on potentiaalinen vaara, joka voi mahdollistaa kyberriskin. Uhkat ovat mm. käyttöoikeuksien varastaminen, haavoittuvuuksien hyväksikäyttö tai tietojenkalastelu. Laajennettuna uhkia ovat myös petos, talousrikos, tietojen menetys tai järjestelmän saavuttamattomuus.

Organisaation kypsyystasosta kertoo se, kuinka organisaatiossa toteutetaan riskienhallintaa. Jos organisaatio yrittää varautua kaikkiin mahdollisiin uhkiin eikä tee työtä tunnistaakseen toimintansa kannalta uhkaavimpia riskejä, se käyttää resurssejaan tehottomasti ja altistaa toimintansa uhkille. Boehmin ym. (2019, 5) artikkelissa on vertailtu jopa kustannuksia, jotka aiheutuvat kaikkeen varautumisessa verrattuna riskiperusteiseen malliin: va-

rautuminen kaikkeen on kolme kertaa kalliimpaa kuin riskiperusteinen varautuminen kyberturvallisuuteen. Hoffmann (2020, 661) on samoilla linjoilla todetessaan, että kyberturvallisuuden johtavia organisaatioita ovat ne, jotka eivät ainoastaan pysty reagoimaan kyberuhkiin ennakoivasti, vaan myös ennustamaan ja estämään niitä hyödyntämällä kyberriskien hallinnan periaatteita.

Boehmin ym. (2019, 4) kuva kyberturvallisuustekemisen kypsyystasoista (kuva 15) osoittaa kyberturvallisuustekemisen eri portaat. Heidän mukaansa suurin osa yrityksistä on siirtymässä riskipohjaiseen tasoon, joka on jo hyvä. Kuitenkin moni organisaatio on vielä kyberturvatekemisessä teknisellä perustasolla tai vielä heikommalla tasolla, jossa tietoturvaa ei ole otettu huomioon ollenkaan. Kypsyystasot osoittavat hyvin sen, että tietoturva ei ole vain teknisten ohjelmistojen käyttöönottoa, sillä ei vielä pääse pitkälle tietoturvan tekemisen portaissa ylöspäin.



Kuva 15. Organisaatioiden kyberturvallisuustekemisen kypsyystaso (Boehm 2019, 4)

Kun mennään vielä syvemmälle riskienhallintaan, voidaan luoda johdolle näkymiä, joissa yhdistyy KRI (key risk indicator, suomeksi riskimittari) ja KPI (key performance indicator, suomeksi suorituskykymittari). Ammattiliitto voisi yhdistää esimerkiksi tietovuodolle alttiit järjestelmät tietoon, kuinka hyvin nämä järjestelmät on suojattu. KRI näyttäisi kuinka moni järjestelmä on ja ei ole suojattu tietovuotoja vastaan. KPI puolestaan asettaisi tavoitteen, jonka edistymistä näkymästä voisi seurata. Näin organisaatiossa (esimerkiksi johto) voisi tarkastella molempia mittareita säännöllisesti ymmärtääkseen kuinka iso riski tällä hetkellä on (KRI) ja kuinka nopeasti tai tehokkaasti riskejä pienennetään (KPI). Jos edistyminen (KPI) ei ole tarpeeksi nopeaa, johto voi esimerkiksi keskustella tiimien kanssa ja miettiä mitä pitäisi tehdä toisin tai mihin lisätä resursseja. (Boehm ym. 2019, 10.)

Riskienhallintaa ei ole kaikkien mahdollisten uhkien monitorointi tai niihin varautuminen. On keskityttävä liiketoiminnan kannalta oleellisimpien ja vaikutukseltaan kriittisimpien riskien minimointiin. Ne voivat monesti olla siellä, mihin mikään järjestelmä ei näe: henkilökunnan tietoisuus ja kouluttaminen. (Boehm ym. 2019, 3.)

Limnéll ym. (2014, 109) korostavat, että riskienhallinta ei ole vain johtamistekninen käytäntö: se sisältää ja heijastaa organisaation arvoja ja ideaaleja muun muassa luotettavuuteen ja vastuullisuuteen liittyen. Se on jatkuva ja systemaattinen ajatteluprosessi, joka koskee kaikkia mahdollisia riskejä ja ongelmia tai katastrofeja ennen kuin ne tapahtuvat.

4.6 Tietosuoja

Tietosuojalla tarkoitetaan henkilötietojen suojaamista (Järvinen 2022, 25). Tavoitteena on turvata ihmisen yksityisyys. Henkilötiedot ovat arvokkaita sekä taloudellisesti että inhimillisistä syistä. Maailmalta löytyy lukuisia esimerkkejä vahingoista, joita henkilötietojen huolimaton käsittely ja tietosuojalakien puuttuminen ovat aiheuttaneet. (Järvinen 2022, 134.) Kuten Järvinen (2022, 108) toteaa: data on uusi öljy.

Tietosuojalait asettavat yrityksille velvoitteita ja antavat henkilöille oikeuksia. Yrityksen on otettava tietosuojan vaatimukset huomioon jo silloin, kun tietojärjestelmiä suunnitellaan. Henkilötietojen tietoturva on varmistettava kaikissa olosuhteissa ja koko tiedon elinkaaren ajan. (Järvinen 2022, 26.)

Tietosuoja-asetuksessa henkilötietoja keräävää ja käsittelevää tahoa kutsutaan rekisterinpitäjäksi. Kyseessä voi olla esimerkiksi yhdistys, jonka on määriteltävä henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjällä on vastuu henkilötietojen käsittelyn suunnittelusta, toteutuksesta ja valvonnasta. Rekisterinpitäjän on laadittava sisäistä käyttöä varten seloste henkilötietojen käsittelytoimista. Siinä tulee kuvata, mitä henkilötietoja organisaatiossa käytetään, mihin tarkoitukseen, mihin maihin tietoja siirretään, mikä on tietojen käsittelyperuste ja mitä sopimuksia organisaatio on tehnyt mahdollisten käsittelijöiden kanssa. Rekisterinpitäjä voi ulkoistaa työhön liittyviä rutiinitehtäviä, kuten tietojen teknistä säilyttämistä tai tietojen käyttöä esimerkiksi postituksiin, toiselle taholle. Rekisteriin tallannettavat henkilötiedot ovat peräisin rekisteröidyiltä eli tavallisilta ihmisiltä – esimerkiksi yhdistyksen jäseniltä. (Järvinen 2022, 136.)

Tietosuoja-asetuksen määritelmä henkilötiedosta on laaja. Mikä tahansa data, joka voidaan liittää ihmiseen suorasti tai epäsuorasti jonkin toisen tiedon tai rekisterin kautta, on henkilötietoa. Henkilötietoa ovat esimerkiksi nimi, osoite, puhelinnumero, sijainti, hiusten ja silmien väri ja vaikkapa kengännumero. Myös IP-osoitteet ja jopa autojen rekisterikilvet ovat henkilötietoja, koska ne voidaan yhdistää epäsuorasti henkilöihin. Tieto on henkilötietoa silloinkin, kun data on pseudonymisoitu korvaamalla henkilöt numeerisilla tunnisteilla. Vain täydellisesti anonymisoitu tieto on vapaa tietosuoja-asetuksen vaateista. (Järvinen 2022, 137.)

4.6.1 Arkaluonteinen henkilötieto, sen suojaaminen ja käsittely

Erityisiä arkaluonteisia henkilötietoja ovat tieto rodusta ja etnisestä alkuperästä, poliittisesta kannasta, uskonnollisesta vakaumuksesta, ammattiliiton jäsenyydestä sekä terveydestä (Järvinen 2022, 137). Yhdistyksen on pidettävä jäsenistään luetteloa (Yhdistyslaki 26.5.1989/503, 3. luku 11.§ mom. 1). Am-

mattiliiton jäsenyys luokitellaan kuuluvaksi erityisten henkilötietoryhmien tietojen käsittelyyn (Tietosuojalaki 5.12.2018/1050, 2. luku 6§ mom. 1). Nämä ovat kaksi tärkeää asiaa, jotka on ymmärrettävä puhuttaessa ammattiliittojen tietosuojasta.

Rekisterinpitäjällä on lukuisia velvollisuuksia, jotka alkavat jo toiminnan suunnittelusta ja tietosuoja on otettava mukaan alusta lähtien. Vain toiminnan kannalta perusteltuja tietoja saa kerätä ja käsitellä. Käsittelyn on oltava asianmukaista ja rekisteröidyn kannalta läpinäkyvää. Tietojen on oltava oikeita ja, jos virheitä havaitaan, ne pitää oikaista ja vanhentuneet tiedot poistaa viipymättä. (Järvinen 2022, 139.) Jos vahinkoja kaikesta huolimatta sattuu, rekisterinpitäjällä tai käsittelijällä on velvollisuus ilmoittaa tapahtuneesta valvontaviranomaiselle (Järvinen 2022, 145).

Henkilötietojen käsittelyyn pitää aina olla perusteltu syy. Puhutaan käsittelyperusteesta. Ilman sitä käsittely on lainvastaista. (Järvinen 2022, 139.) Tietosuojavaltuutetun toimiston (2024a) mukaan erityisten henkilötietoryhmien tietojen käsittely on lähtökohtaisesti kielletty. Kuitenkin erityisiin henkilötietoryhmiin kuuluvia henkilötietoja saa käsitellä, kun kieltoon on säädetty poikkeus EU:n tietosuoja-asetuksessa tai erikseen unionin oikeudessa tai kansallisessa lainsäädännössä. Erityisiä henkilötietoryhmiä voi käsitellä suoraan tietosuoja-asetuksen perusteella, jos rekisteröity on antanut nimenomaisen suostumuksen kyseisten henkilötietojen käsittelyyn. Nimenomainen suostumus ammattiliiton kohdalla tarkoittaa liittymislomakkeen täyttämistä.

Tietosuoja-laki määrää, että käsiteltäessä ammattiliiton jäsenyyttä rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset ja erityiset toimenpiteet rekisteröidyn oikeuksien suojaamiseksi. Näitä toimenpiteitä ovat seuraavat:

1) *toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty;*
2) *toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista;*
3) *tietosuojavastaavan nimittäminen;*

4) *rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin;*
5) *henkilötietojen pseudonymisointi;*
6) *henkilötietojen salaaminen;*
7) *toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;*
8) *menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi;*
9) *erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen;*
10) *tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskevan vaikutustenarvioinnin laatiminen;*
11) *muut tekniset, menettelylliset ja organisatoriset toimenpiteet.*

(Tietosuojalaki 2. luku 6§ mom. 2.)

Tietosuojavelvollisuuksien laiminlyönnistä on laadittu sanktio- ja seuraamisjärjestelmä. EU:n yleisen tietosuoja-asetuksen 58 artiklan 2 kohdassa säädetään valvontaviranomaisen toimivaltuuksista. Niitä ovat rekisterinpitäjälle annettava varoitus tai huomautus siitä, että käsittelytoimet ovat asetuksen vastaisia sekä käsittelyn väliaikainen tai pysyvä rajoittaminen, mukaan lukien käsittelykielto. Sanktioista puolestaan on säädetty niin, että valvontaviranomainen voi määrätä hallinnollisen sakon toimenpiteiden lisäksi tai niiden sijaan. Sakko voi yrityksille olla korkeimmillaan 20 000 000 euroa tai neljä prosenttia edeltävän tilikauden vuotuisesta liikevaihdosta, riippuen kumpi määristä on suurempi. (Andreasson & Ylipartanen 2022, 38.) Järvinen (2022, 146) huomauttaa, että jättisakot ovat saaneet paljon julkisuutta mutta niillä on toinenkin tavoite. Ne nostavat tietosuojan yritysten johdon ja hallituksien asialistalle. Miljoonalasku tietosuojan laiminlyönneistä yhdistettynä uutisoinnista seuraavaan mainehaittaan on tekijä, joka saa varmasti jokaisen yrityksen ja yhdistyksen ottamaan tietosuojan vakavasti.

4.6.2 Tietosuojaloukkaus vs. tietoturvaloukkaus

Tietosuojaloukkaus on tapahtuma, jossa henkilötietoja tuhoutuu, häviää, muuttuu, niitä luovutetaan luvattomasti tai niihin pääsee käsiksi asiaton taho. Voidaan puhua myös henkilötietojen tietoturvaloukkauksesta, kuten tietosuojavaltuutetun toimisto (2024c) termin määrittelee:

> ”Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.”

Organisaatiolla, joka havaitsee tietosuojapoikkeaman, on ilmoitettava viipymättä (72 tunnin sisällä) tietosuojaviranomaiselle havainnosta. Lisäksi henkilöille, joita loukkaus koskee, on ilmoitettava. (Tietosuojavaltuutetun toimisto 2024c.)

Tietosuojaloukkaukseen voi liittyä tietoturvaloukkaus. Termit varsinkin yleiskielessä menevät usein sekaisin. Tietoturvaloukkauksessa voi olla vaarantuneena henkilötiedon lisäksi tietojärjestelmä tai tietoverkko. Tai tietoturvaloukkaus voi olla kyseessä ilman tietosuojaloukkausta, jolloin henkilötiedot eivät ole vaarantuneet. Organisaation on tärkeä luoda itselle selkeä prosessi mahdollisten loukkausten varalle.

4.7 Kyberuhat ja niiden vaikutukset ammattiliittojen arkaluonteisten tietojen suojaamiseen

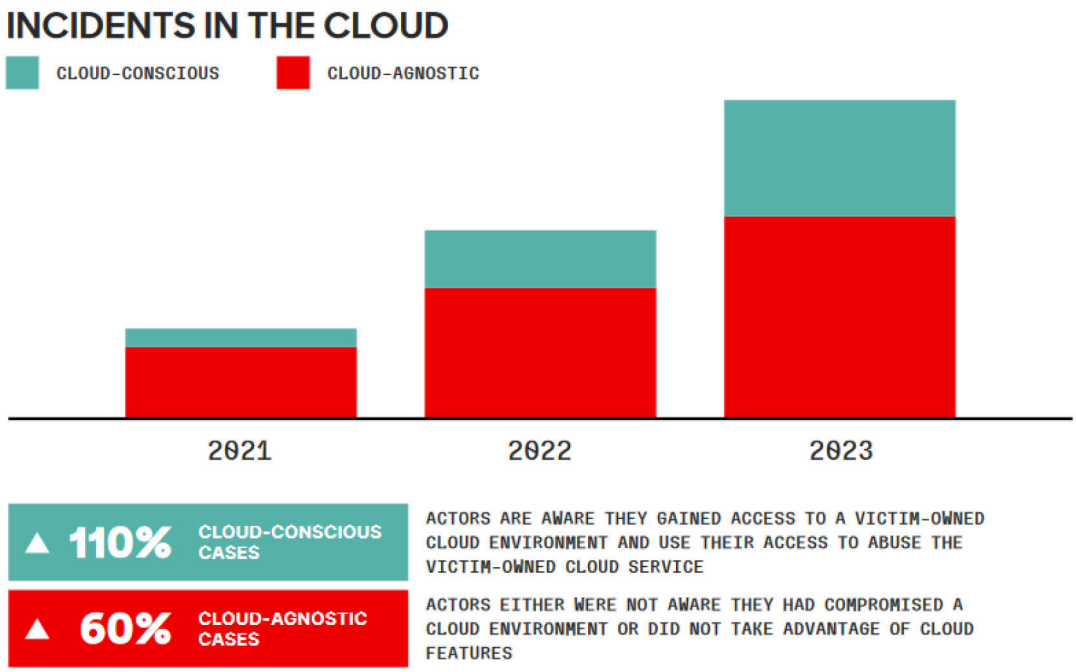
Arjen toimivuus on riippuvainen bittien maailmasta ja siksi jokaisen on oltava tietoinen kyberuhkista ja omista toimenpiteistään niihin liittyen. (Limnéll ym. 2014, 14.) Ammattiliittojen henkilökunnasta jokaisen on ymmärrettävä miten oma toiminta vaikuttaa jäsenistön tietosuojan toteutumiseen. Myös välillisten toimintojen.

Kyberuhka on Limnéllin ym. (2014, 37) sanoin tahallisesti tai tahattomasti digitaalisessa maailmassa tapahtuva turvattavan kohteen turvallisuutta heikentävä tekijä. Limnéll ym. (2014, 105) jatkavat, että uhka on pakottavaa toimintaa, jossa toteutettavaksi uhatun toimen oletetaan saavan aikaan negatiivisen

vaikutuksen kohteessa ja/tai kohteen intresseissä. Sen avulla kohde pyritään saamaan toimimaan uhkaajan haluamalla tavalla.

Hüseyin Sevgin -tutkimus (2021, 76) korostaa, että ammattiliitot ovat siirtyneet yhä enemmän digitaalisiin kanaviin, erityisesti sosiaalisen median ja sähköisten viestintäalustojen käyttöön. Tämä lisää näkyvyyttä ja tavoitettavuutta, mutta samalla altistaa ne uusille kyberhyökkäyksille. Ammattiliittojen käsittelemä tieto, kuten jäsenten henkilökohtaiset tiedot ja toisaalta vaikuttamiskeinot internetissä ja sosiaalisessa mediassa, ovat erityisen houkutteleva kohde kyberrikollisille. Digitaalisten kanavien käytön yleistyminen lisää näiden tietojen altistumista ja voi aiheuttaa toteutuessaan mittavia kustannuksia.

Pilvipalvelut ovat yleistyneet ammattiliittojenkin käytössä. Pilvipalveluita käytetään niin jäsenrekisterien kuin autentikoinnin ylläpitoon. Tämän ovat huomanneet myös hyökkääjät. Crowstriken Global Treath Reaport (2024, 17) kertoo, että pilvipalveluihin kohdistuneet iskut ovat lisääntyneet 75 % edellisen vuoden, vuoden 2023 raporttiin verrattuna (kuva 16).



Kuva 16. Pilvipalveluihin kohdistuneet hyökkäykset 2021–2023 (CrowdStrike 2024, 17)

Huijaus- ja tietojenkalasteluviestit ovat lisääntyneet ammattiliitoissakin viime vuosina merkittävästi. Vielä jokunen vuosi sitten huijausviesteistä puhuttiin

teoriatasolla ja ne kohdistuivat muihin kuin ammattiliittoihin. Tänä päivänä tietojenkalasteluyritykset ovat osa arkea. Käyttäjätunnuksen menettäminen tietojenkalastelun seurauksena voi aiheuttaa riskin jäsenrekisterin turvallisuudelle.

Kalastelu- ja huijausviestien tunnistaminen ei ole enää helppoa. ChatGPT-tyyliset tekoälysovellukset ovat parantaneet huijausviestien laatua. Kieliopista ei enää välttämättä tunnistakaan huijausta. Kiire ja mobiililaitteet tekevät oman mausteensa sosiaalisen manipuloinnin tunnistamisen vaikeuteen, vaikka tunnistaisikin teoriatasolla uhkat. Uusimpana muotona on huijauksissa käytetty äänisimulaattori. Huijauksissa voidaan käyttää esimerkiksi sosiaalisen median alustoilta löytyvää henkilön ääntä ja tekeytyä häneksi. Vishing-hyökkäyksissä huijarit soittavat uhreille ja yrittävät houkutella heidät lataamaan haittaohjelmia, avaamaan etätukiyhteyden tai syöttämään tunnistetietonsa väärennetyille sivustoille. Vuonna 2024 useimmat hyökkäykset toteutettiin esiintymällä it-tukena ja väittämällä, että soitto liittyy yhteys- tai tietoturvaongelmaan. (CrowdStrike 2025, 16.)

CrowdStrike (2024, 52) ennusti 2024, että sosiaalinen manipulointi tulee tehostumaan entisestään. Monivaiheisen tunnistautumisen (MFA) ohittamisen hyökkäykset lisääntyvät. Kasvua ennustettiin tapahtuvaksi myös kolmansien osapuolten palveluntarjoajiin kohdistuvissa hyökkäyksissä ja palvelutarjoajien ketjussa, joiden tavoitteena on hyödyntää yhtä laajempaa pääsykohtaa. Vuonna 2025 huomattiinkin, että vuoden 2024 aikana oli tapahtunut siirtymää perinteisistä tietojenkalasteluista uusiin tunkeutumistapoihin. Yritysten tiukentunut tietoturva oli vaikeuttanut perinteisiä hyökkäyksiä. Erityisesti puhelinpohjainen huijaus yleistyi, ja rikolliset hyödyntävät yhä enemmän vishingiä, takaisinsoittohuijauksia ja IT-tukihuijauksia päästäkseen yritysverkkoihin. (CrowdStrike 2025, 5.)

Kun hyökkääjät onnistuvat tunkeutumaan järjestelmään, heidän seuraava tavoitteensa on laajentaa pääsyään ja edetä alkuperäisestä sisäänpääsypisteestä kohti arvokkaita kohteita. Kuinka nopeasti tämä niin sanottu "murtautumisaika" tapahtuu, määrittää, kuinka nopeasti puolustajien on reagoitava minimoidakseen hyökkäyksen aiheuttamat vahingot ja kustannukset. Vuonna 2024 interaktiivisten verkkorikoshyökkäysten keskimääräinen murtautumisaika

lyheni 48 minuuttiin, kun se vuonna 2023 oli vielä 62 minuuttia. Huolestuttavasti nopein murtautuminen tapahtui vain 51 sekunnissa – mikä tarkoittaa, että puolustajilla voi olla alle minuutti aikaa havaita ja torjua hyökkäys ennen kuin hyökkääjät saavat laajemman hallinnan järjestelmään. (CrowdStrike 2025, 12.)

Haavoittuvuuksien hyväksikäyttö maailmanlaajuisesti kasvaa hurjaa vauhtia. Tietoturvayhtiö Verizonen 2024 Data Breach Investigation Report (2024, 7) kertoo haavoittuvuuksien hyväksikäyttöön liittyvien hyökkäysten lähes kolminkertaistuneen eli kasvaneen 180 % edellisen vuoden raporttiin verrattuna.

Haittaohjelmien levittäminen huijausviestien välityksellä on myös uhka ammattiliiton kyberturvallisuudelle. Haittaohjelman pääseminen ammattiliiton verkkoon voi aiheuttaa toiminnan pitkäaikaisen lamaantumisen. Pilvipalveluiden käytön paikallinen verkkohäiriö tai maailmanlaajuinen katkos palveluntarjoajalla aiheuttaa laajasti haittaa toiminnalle, jossa työ tapahtuu pääosin tietokoneella ja toimistosovelluksilla. Palvelunestohyökkäykset aiheuttavat ammattiliitolle uhkan, joka olisi kiusallinen ja estäisi jäsenpalveluiden tarjoamisen. Tietomurto tai tietovuoto aiheuttaisi ammattiliitoille suurimman mahdollisen haitan.

Tietoisuus näistä uhista on siis ensiarvoisen tärkeä saattaa ammattiliiton henkilökunnan tietoisuuteen. Seuraavassa kappaleessa käsittelen yleisimmät kyberturvallisuusuhat ja -haasteet, miten ne ilmenevät, leviävät ja vaikuttavat organisaatioihin.

4.7.1 Kiristysohjelmat (ransomware)

Kiristyshaittaohjelma on ohjelma, joka estää laitteen normaalin käytön ja esittää vaatimuksen lunnaiden maksamisesta rikollisille. Haittaohjelmatyypistä käytetään myös nimitystä lunnastroijalainen. Kiristyshaittaohjelma salaa laitteella olevat tiedostot salausalgoritmilla ja avaimella, joka on vain hyökkääjän tiedossa. Tiedostojen salauksen tai näytön lukitsemisen jälkeen haittaohjelma jättää uhrille yleensä viestin, jossa rikollinen kertoo palauttavansa laitteen omistajansa käyttöön lunnaita vastaan. (Kyberturvallisuuskeskus 2024a.)

Rikolliset levittävät kiristyshaittaohjelmia sekä satunnaisiin kohteisiin että kohdennettujen tietomurtojen avulla. Yksityishenkilöille ja pienille organisaatioille olennainen uhka ovat satunnaisesti suurelle vastaanottajajoukolle levitettävät haittaohjelmat. Tällaisessa hyökkäyksessä rikolliset eivät aktiivisesti edistä hyökkäystä, vaan luottavat siihen, että joku lataa ennemmin tai myöhemmin erehdyksessä haittaohjelman laitteelleen tai että haittaohjelmaan ohjelmoitu automatiikka löytää haavoittuvan laitteen. Tyypillisimpiä levityskeinoja ovat roskapostissa olevat linkit ja liitteet. Niitä levitetään myös väärennetyillä ladattavilla tiedostoilla kuten maksullisten ohjelmistojen piraattikopioilla, sekä tunnettuja ohjelmistohaavoittuvuuksia hyväksikäyttämällä. Kohdennetut tietomurrot sitä vastoin ovat keskisuurten ja suurten organisaatioiden murhe, sillä kohdennetun tietomurron yrittäminen edellyttää rikollisilta merkittävää vaivannäköä, eivätkä rikolliset voi odottaa saavansa vaivaan nähden riittävän suurta rikoshyötyä pieniltä organisaatioilta. Toimintatapaa, jossa rikolliset valikoivat kohteikseen erityisen maksukykyisiä yrityksiä, on kutsuttu termillä “big game hunting” eli suurriistan metsästys. (Kyberturvallisuuskeskus 2024a.)

Kiristyshaittaohjelmahyökkäyksen voi havaita esimerkiksi kiristysviestin saapumisella. Sen voi havaita myös mm. tietoturvatuotteen hälytyksellä tai sen myötä, että tiedostoihin pääsy estyy. Tärkeimmät onnistuneen hyökkäyksen seuraukset liittyvät siihen, että käyttäjät eivät pääse enää käsiksi tartunnan saaneessa laitteessa oleviin tietoihin. Jos tiedoista ei ole varmuuskopiota, saattavat tiedot olla lopullisesti mennyttä. Yrityksille kiristyshaittaohjelmahyökkäyksen taloudelliset vaikutukset voivat olla merkittävät, riippuen liiketoiminnasta. Yritys voi menettää suuria summia rahaa liiketoiminnan keskeytyessä, korjaustoimenpiteissä tai mainehaitassa. (Kyberturvallisuuskeskus 2024a.)

4.7.2 Tietojenkalastelu (phishing, smishing, vishing)

Tietojenkalastelun, joka kuuluu sosiaalisen manipulaation piiriin, avulla verkkorikolliset varastavat henkilötietoja kuten puhelinnumeroita sekä pankki- ja henkilötunnuksia. Tämän lisäksi verkkorikollisia kiinnostavat ihmisten kirjautumistiedot eli käyttäjätunnukset ja salasanat, joiden avulla voidaan kirjautua erilaisiin palveluihin. Yleensä tietojenkalastelu tapahtuu väärennettyjen verkkosivujen avulla, jonne uhri houkutellaan sähköpostin, tekstiviestin (smishing) tai

puhelun (vishing) avulla. Tarkoituksena saada henkilö syöttämään väärennetylle sivustolle oikea käyttäjätunnus ja salasana. Viestit lähtevät yleisimmin massana isoille joukoille. Tästä kehittyneempi versio on kohdennettu tietojenkalastelu (spear phishing), jossa räätälöidään huijausviesti vastaanottajan tai organisaation mukaan. (F-Secure 2022c.) Tekoälyn tulo rikollisienkin käyttöön on parantanut tietojenkalastelun laatua.

Huijaamalla saatuja tietoja voidaan käyttää käyttäjätilien kaappauksiin tai jopa identiteettivarkauksiin. Tietojenkalastelun avulla voidaan myös tartuttaa haittaohjelmia laitteelle. Haittaohjelmat naamioidaan kiinnostavaksi sisällöksi, kuten tärkeiksi asiakirjoiksi. (F-Secure 2022c.)

Kaksi- tai monivaiheisen tunnistautumisen yleistyminen on vaikeuttanut tunnusten kalastelua, joskaan ei tehnyt sitä mahdottomaksi. Tietojenkalastelu- ja huijausviestit kehittyvät jatkuvasti. Erilaiset teknologiat, kuten koneoppiminen ja tekoäly sekä psykologiset keinot auttavat rikollisia pyrkimyksissään voittaa uhrin luottamus. Kalastelukampanjat tuottavatkin jatkuvasti tulosta rikollisille ja Kyberturvallisuuskeskuksen kesäkuun 2023 arvion mukaan noin sadan organisaation sähköpostitilejä oli murrettu onnistuneesti lähikuukausien aikana. (Kyberturvallisuuskeskus 2023.)

4.7.3 Väsytyshyökkäys (brute-force)

Väsytyshyökkäyksessä hyökkääjä pyrkii pääsemään järjestelmään kokeilemalla eri salasanoja niin kauan, kunnes arvaus osuu oikeaan. Näiden iskujen takana ovat hakkerit, jotka pyrkivät selvittämään salasanojen lisäksi PIN-koodeja tai salausavaimia kokeilemalla erilaisia vaihtoehtoja. Tarkoituksena on saada pääsy salasanalla suojatulle tilille tai alustalle tai purkaa tietojen salaus. Väsytyshyökkäysten avulla voidaan myös selvittää erilaisten yritysten tai järjestöjen verkon turvallisuutta. (Zieniūtė 2022.)

Väsytyshyökkäys ei vaadi monimutkaista osaamista tai algoritmeja. Se vaatii vain aikaa ja tietojenkäsittelyvoimaa. Hyökkäyksen onnistumiseen vaikuttaa myös yksi tekijä: mitä monimutkaisempi salasana on, sitä vaikeampi se on murtaa. (Zieniūtė 2022.)

Nykyään tilejä luotaessa vaaditaan monimutkainen salasana, joka koostuu riittävästä määrästä eri merkkejä, ja sisältää isoja ja pieniä kirjaimia. Tällaisen salasanan arvaaminen eri vaihtoehtoja kokeilemalla on käytännössä mahdotonta, sillä vaihtoehtoja on liikaa. Hakkerit tietysti tietävät tämän, eikä väsytyshyökkäyksiä tehdäkään tietokoneen äärellä istuen, käsin erilaisia salasanoja syöttämällä. Sen sijaan hakkerit käyttäjät salasanojen arvaamiseen erillisiä ohjelmia, jotka voivat kokeilla tuhansia eri salasanoja sekunnissa. Jos salasana koostuu muutamasta merkistä, ohjelma selvittää sen sekunneissa. Jos salasana on riittävän monimutkainen ja pitkä, esimerkiksi 16 merkkiä, ohjelmaltakin sen selvittäminen voi viedä vuosia. Hakkereiden tihutöitä vaikeuttavat myös verkkosivujen salasanojen suojausmenetelmät. Salasanat salataan tai niistä säilytetään niin sanottu tiiviste, joka muodostetaan hajautusalgoritmilla. Salasanoja ei siis säilytetä selkolukuisena tekstinä. Jos salasanat vuotavat, hakkerit eivät pääse niihin käsiksi sellaisinaan, vaan ennen salasanojen selvittämistä on selvitettävä monimutkainen salausavain – ja sen selvittäminen vaatii huiman määrän arvausyrityksiä. (Zieniūtė 2022.)

Myös monivaiheiseen todennukseen voidaan kohdistaa väsytyshyökkäys. Tällöin puhutaan MFA-pommituksesta. Käyttäjän laitteelle, esimerkiksi iPhone-puhelimeen lähetetään lukuisia vilpillisiä todennuspyyntöjä. Perään voidaan vielä esimerkiksi soittaa ja väittää puhelun tulevan Applen asiakastuesta. Hyökkääjän tavoitteena on lukita käyttäjä ulos laitteelta ja saada sen kautta joko tietoa tai rahaa. Monivaiheisen todennuksen pyyntöä ei tule koskaan hyväksyä, jos ei itse sitä ole tilannut.

4.7.4 Haittaohjelma (malware)

Haittaohjelma on päätermi kaiken tyyppisille haitallisille ohjelmistoille, joiden tarkoitus on vahingoittaa ohjelmoitavaa laitetta, palvelua tai verkkoa. Haittaohjelmat keksittiin vuosikymmeniä sitten. Hyökkäystapoja ovat esimerkiksi sähköpostin liitteet, haittamainonta suosituilla sivustoilla, ohjelmistojen väärennetyt asennukset, USB-muistitikkujen ja sovellusten tartuttaminen sekä tietojenkalasteluviestit sähköpostin ja tekstiviestien välityksellä. (McAfee 2024.)

Laitetta voidaan myös hyödyntää esimerkiksi tietojenkalasteluun tai palvelunestohyökkäykseen tai tartuttaa haittaohjelma, jotta koneella voidaan louhia kryptovaluuttoja. Haittaohjelmien avulla kyberrikolliset keräävät yleensä tietoja, joilla he yrittävät kiristää uhreilta taloudellista hyötyä. Tällaisia tietoja voivat olla esimerkiksi raha-asioihin liittyvät tiedot, potilasasiakirjat, sähköpostit tai salasanat – nykyisin vaaraan voivat joutua minkä tyyppiset tiedot tahansa. (McAfee 2024.)

Haittaohjelmia on useita erilaisia, joiden ilmenemismuodot on hyvä tunnistaa, jotta niiden varalta voi suojautua. Seuraavassa on F-Securen (2022b) mukaan esitelty haittaohjelman eri muodot:

- **Virus**
  Tietokonevirus on tyypillinen haittaohjelma, jota käytetään esimerkiksi kyberhyökkäysten yhteydessä. Virus käyttää hyväkseen aukkoja ohjelmien tietoturvassa ja ujuttaa uutta koodia ohjelmaan. Kun ohjelma seuraavan kerran käynnistetään, voi virus esimerkiksi tuhota laitteen tiedostoja tai estää sitä käynnistymästä.
- **Troijalainen**
  Troijalainen näyttää tavalliselta ohjelmistolta tai tiedostolta, mutta todellisuudessa se on naamioitu virus. Se varastaa luottamuksellisia tietoja, kaappaa laitteen tai vakoilee sen toimintaa. Troijalainen voi piileksiä vaikkapa huijausviesteissä ja pystyy tartuttamaan laitteet monilla haittaohjelmilla samanaikaisesti.
- **Tietokonemato**
  Tietokonemato kopioi itsensä helposti laitteelta toiselle ja leviää siksi nopeasti. Mato ei vaadi vuorovaikutusta käyttäjän kanssa aiheuttaakseen tuhoa, vaan se hyödyntää puutteita tai aukkoja käyttöjärjestelmässä.
- **Mainosohjelma**
  Mainosohjelmat tunnetaan myös englanninkielisestä termistä adware. Nämä haittaohjelmat voi tunnistaa odottamattomista mainoksista tai ponnahdusikkunoista. Laite voi saada mainosohjelman esimerkiksi hyväksyessä haitallisen ohjelmiston tai sovelluksen käyttöehdot.
- **Ransomware**

Termillä viitataan kiristysohjelmiin, jotka salaavat tai lukitsevat tiedostoja, käyttäjätilejä ja laitteita. Verkkorikolliset vaativat uhreiltaan lunnaita lukituksen purkamiseksi. Usein lunnaat vaaditaan kryptovaluuttana, sillä niiden jäljittäminen on vaikeaa.

- **Vakoiluohjelma**
  Vakoiluohjelman avulla rikollinen seuraa laitteesi viestintää, selaustietoja ja muuta tietoliikennettä. Vakoiluohjelma voi myös muuttaa laitteen asetuksia mahdollistaen muiden haittaohjelmien asentamisen uhrin tietämättä. Vakoiluohjelmat tunkeutuvat laitteelle muun muassa haitallisten linkkien kautta.

4.7.5 Tietosuojaloukkaus (data breach)

Kuten kappaleessa Tietosuojaloukkaus vs. tietoturvaloukkaus kuvattiin, henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. (Tietosuojavaltuutetun toimisto 2024c.)

Tietosuojavaltuutetun toimisto (2024c) luettelee verkkosivustollaan esimerkkejä minkälaiset erilaiset tapahtumat voivat olla henkilötietojen tietosuojaloukkauksia. Niitä ovat seuraavat:

- hävinnyt USB-tikku
- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa tai
- tiliotteen postitus väärälle henkilölle.

Tietoturvaloukkauksesta voi seurata esimerkiksi henkilötietojen valvomiskyvyn menettäminen, identiteettivarkaus tai petos, maineen vahingoittuminen tai pseudonymisoitujen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen (Tietosuojavaltuutetun toimisto 2024c).

Henkilötietojen tietoturvaloukkaus on varsinkin ammattiliittojen näkökulmasta kriittinen. Ammattiliiton tärkein suojattava omaisuus ovat jäsenten henkilötiedot, jotka on annettu ammattiliiton käsiteltäväksi perustuen oikeutettuun etuun. Jos ammattiliitto menettää jäsentietoja, täytyy sen tietää tarkasti, kuinka toimia, kun se saa tiedon tapauksesta.

4.7.6 Palvelunestohyökkäys (denial-of-service, DoS)

Palvelunestohyökkäyksellä tarkoitetaan tilannetta, jossa hyökkääjä ylikuormittaa palvelua tahallisesti ja estää sen normaalin toiminnan. Dos-hyökkäyksessä lähteenä on yksi internetiin kytketty laite. Kaiken muistin ja levytilan loppuessa palvelin kaatuu ja pahimmillaan sen uudelleenkäynnistäminen vaatii ylläpidolta aktiivisia toimia (Järvinen 2018, 344).

Hyökkäyksistä saadaan tehokkaita hajauttamalla ne jopa kymmeniin tuhansiin tietokoneisiin eri puolille maailmaa. Tällaista hyökkäystä kutsutaan hajautetuksi palvelunestohyökkäykseksi (DDoS, Distributed Denial of Service), lyhyemmin DDos-hyökkäykseksi. (Järvinen 2018, 338). Näin hyökkäyksen lähdettä on hankalampi tunnistaa ja pysäyttää esimerkiksi automaattivalvonnan avulla. DDos hyökkäykset tekevät myös tuhoisampaa jälkeä suuremman liikennemäärän takia. Välittäjäkoneet ovat tavallisia koti- ja yrityskoneita, joihin on ujutettu haittaohjelma verkon tai tietomurtojen avulla. (Järvinen 2018, 338.)

Tietyt haittaohjelmat voivat kaapata minkä tahansa tietokoneen tai verkkoon kytketyn laitteen osaksi niin sanottua botnetiä. Botnet on verkosto kaapattuja laitteita, joita hyökkääjä voi käyttää DDoS-hyökkäyksen suorittamiseen. Tällöin kaikki botnetiin kuuluvat laitteet kohdistavat pyyntöjä ja verkkoliikennettä samaa verkkosivua tai palvelua kohtaan. Muun muassa reitittimiä, erilaisia mobiililaitteita sekä verkkoon yhdistettyjä kameroita voidaan käyttää hajautetun palvelunestohyökkäyksen suorittamiseen. (F-Secure 2022a.)

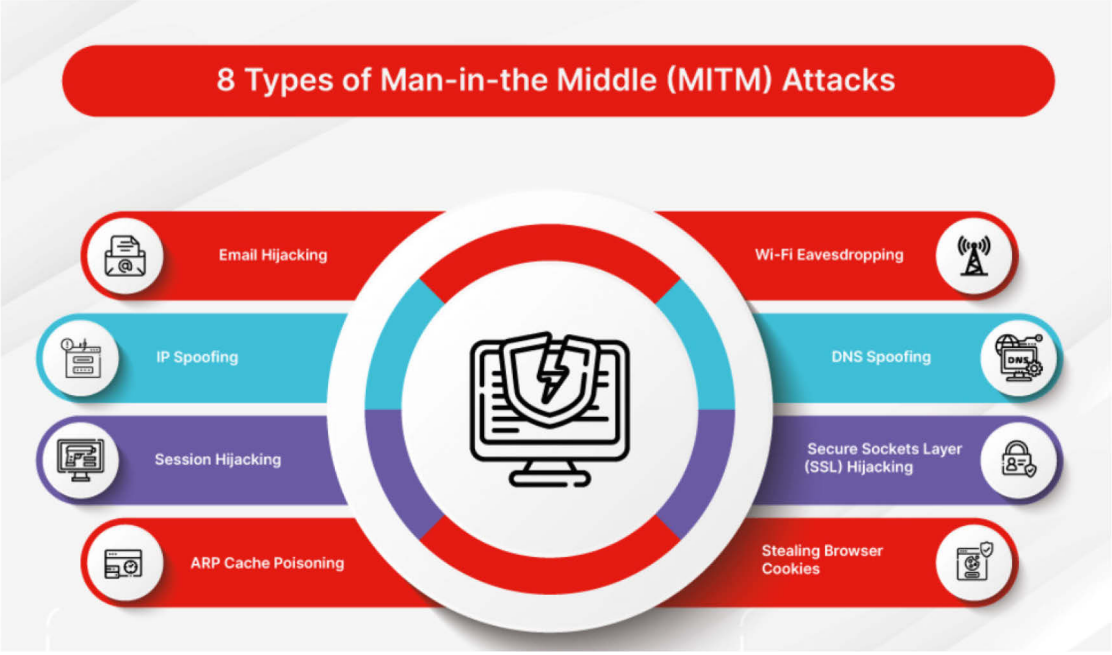
Kyberturvallisuuden näkökulmasta vaarallisiksi ddos-hyökkäykset muuttuvat silloin, kun niillä lamautetaan viranomaisten viestintää tai yhteiskunnalle tärkeiden palveluiden toimintaa (Järvinen 2018, 345).

4.7.7 Man-in-the-Middle (MitM)

Man-in-the-Middle-hyökkäyksessä hyökkääjä asettuu kahden viestivän osapuolen väliin kaapaten tieto- tai maksuliikennettä ilman, että kukaan huomaa sitä. Yleisimmin hyökkääjä kuuntelee ja odottelee liikennettä, kunnes iskee.

Hakkerit etsivät erilaisia tapoja käyttää hyväksi ohjelmistojen haavoittuvuuksia asettuakseen käyttäjän ja verkkosivuston väliin. Verkkorikollinen saattaa esimerkiksi luoda ansaksi tarkoitettuja Wi-Fi-verkkoja ja naamioida sen näyttämään vaikkapa läheisen kahvilan verkolta. Niitä ei suojata salasanoilla, vaan kuka tahansa voi yhdistää tällaiseen verkkoon. Kun uhri yhdistää tällaiseen verkkoon, kaikki hänen verkkoliikenteensä paljastuu. (Zieniūtė 2024.)

Fortinet (2024) kuvaa kahdeksan erityyppistä MITM-hyökkäystä (kuva 17).



Kuva 17. MITM hyökkäysten eri tyypit (Fortinet 2024)

Fortinet (2024) mukaan MITM-hyökkäyksissä hyödynnetään viestintäprotokollien haavoittuvuuksia tai turvattomia verkkoyhteyksiä. Perusidea niissä on kuitenkin kaikissa sama, hyökkääjä asettuu uhrin ja vastaanottajan väliin kaapatakseen liikennettä.

4.8 Ammattiliittoihin liittyvät lait ja asetukset

Ammattiliitot ovat yhdistyksiä. Yhdistyslaki määrittelee säännöt ja periaatteet, kuinka yhdistys perustetaan, kuinka se toimii ja miten toiminta lakkaa. EU:n yleinen tietosuoja-asetus asettaa yhtenäiset ehdot henkilötietojen suojaamiselle ja käsittelyllä kaikissa EU-jäsenvaltioissa. Kansallinen tietosuojalaki täydentää tietosuoja-asetusta. Laki sähköisen viestinnän palveluista koskettaa ammattiliittoja mm. sähköpostin käytössä tai muiden viestintävälineiden käytössä. Rikoslakiin sisältyy säädöksiä tietosuoja- ja tietoturvaloukkauksista ja tulee kyseeseen, jos ammattiliiton käsittelemät henkilötiedot päätyvät vääriin käsiin. Jokaisen kansalaisen viestintäsalaisuus on puolestaan asetettu perustuslaissa. Seuraavissa osioissa käsitellään ammattiliittojen toimintaan liittyvät lait ja asetukset lyhyesti.

4.8.1 Yhdistyslaki

Yhdistyksen toimintaa Suomessa säätelee yhdistyslaki, joka turvaa suomalaisten yhdistysten tasa-arvoisen aseman yhteiskunnassa. Yhdistyslaki säätelee yhdistysten perustamista, toimintaa, hallintoa ja purkamista. Se määrittelee muun muassa jäsenten oikeudet ja velvollisuudet, päätöksenteon säännöt sekä yhdistyksen rekisteröinnin ja oikeuskelpoisuuden. Yhdistyslain (1989/503) 1 §:n mukaan yhdistyksen saa perustaa aatteellisen tarkoituksen yhteistä toteuttamista varten. 8 §:n mukaan rekisteröitäväksi tarkoitetun yhdistyksen säännöissä on mainittava mm. yhdistyksen nimi, kotipaikka, yhdistyksen tarkoitus ja toimintamuodot. Yhdistyslaki määrittää myös mm. jäsenluettelon pitämisestä (8 §), jäseneksi liittymisestä (12 §) ja eroamisesta (13 §).

4.8.2 EU:n yleinen tietosuoja-asetus

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 eli yleinen tietosuoja-asetus (GDPR) säätelee henkilötietojen käsittelyä Euroopan unionissa. EU:n yleinen tietosuoja-asetus on suoraan sovellettavaa oikeutta. Se pätee yleisesti, se on kaikilta osiltaan velvoittava ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa, ellei kansallisesti ole säädetty asetuksen sallimista poikkeamista. (Andreasson & Ylipartanen 2022, 30.) Asetus on siis sama kaikissa EU-maissa, mikä takaa yhtenäiset oikeudet EU-kansalaisille. (Järvinen 2022,

132). Asetus astui voimaan vuonna 2016 ja sitä alettiin soveltaa kansallisesti Suomessa 2018.

EU:n yleisen tietosuoja-asetuksen tarkoitus on suojata yksityishenkilöitä, kun heidän tietojaan käsitellään yksityisellä sektorilla ja suurimmalla osalla julkista sektoria. Tietosuoja-asetus auttaa yksilöitä hallitsemaan paremmin henkilötietojaan. Asetuksen päämäärä on myös parantaa luottamusta online-palveluihin ja näin edistää EU:n digitaalisten sisämarkkinoiden kehittämistä (Andreasson & Ylipartanen 2022, 30).

Yleisellä tietosuoja-asetuksella osoitetaan yksilön oikeuksia ja autetaan yksilöitä hallitsemaan paremmin henkilötietojaan. Se sisältää seuraavat osat:

- *Helpompi pääsy omiin tietoihin.*
- *Uusi oikeus siirtää tiedot järjestelmästä toiseen.*
- *Selkeämpi oikeus tietojen poistamiseen (oikeus tulla unohdetuksi). Kun henkilö ei enää halua, että hänen tietojaan käsitellään, tiedot poistetaan, paitsi jos on olemassa jokin laillinen peruste säilyttää ne.*
- *Oikeus saada tietoa henkilötietojen tietoturvaloukkauksesta. Yritysten ja organisaatioiden on ilmoitettava asiasta asianomaiselle tietosuojaviranomaiselle ja vakavien tietoturvaloukkausten tapauksessa myös asianomaisille henkilöille.*

(EUR-Lex 2022.)

EU-yleisellä tietosuoja-asetuksella asetetaan kaikille EU sisämarkkinoilla toimiville yrityksille seuraavat säännöt:

- *Yhteiset EU:n laajuiset säännöt. Yksi EU:n laajuinen tietosuojalainsäädäntö lisää oikeusvarmuutta ja vähentää hallinnollista taakkaa.*
- *Tietosuojavastaavat. Tietosuojasta vastaavan henkilön nimeävät viranomaiset ja yritykset, jotka käsittelevät tietoja laajamittaisesti tai joiden ydintehtävänä on erityisten tietoryhmien, kuten terveyteen liittyvien tietojen, käsittely.*
- *Yhden luukun periaate. Yritysten on asioitava vain yhden valvontaviranomaisen kanssa (siinä EU:n jäsenvaltiossa, jossa niillä on päätoimipaikka).*

- *EU-säännöt, jotka koskevat EU:n ulkopuolisia yrityksiä. Euroopan ulkopuolelle sijoittautuneiden yritysten on sovellettava samoja sääntöjä, kun ne tarjoavat tavaroita tai palveluja tai seuraavat henkilöiden käyttäytymistä EU:ssa.*
- *Innovaatioille suotuisat säännöt. Tietosuojatakeet otetaan huomioon tuotteissa ja palveluissa jo suunnitteluvaiheessa (sisäänrakennettu ja oletusarvoinen tietosuoja)*
- *Yksityisyydensuojaa parantavat tekniikat. Pseudonymisoiminen (kun tietojen tunnistuskentistä korvataan yksi tai useampi keinotekoisilla tunnisteilla) ja salaus (kun tiedot koodataan niin, että vain valtuutetut osapuolet voivat lukea niitä).*
- *Ilmoitusten poistaminen. Yleisessä tietosuoja-asetuksessa poistettiin useimmat ilmoitusvelvollisuudet ja niihin liittyvät kustannukset. Yksi sen tavoitteista on poistaa esteitä, jotka vaikuttavat henkilötietojen vapaaseen liikkuvuuteen EU:ssa. Tämä helpottaa yritysten laajentumista digitaalisilla sisämarkkinoilla.*
- *Tietosuojaa koskevat vaikutustenarvioinnit. Yritysten on tehtävä vaikutustenarviointeja, jos tietojenkäsittely voi aiheuttaa henkilön oikeuksien ja vapauksien kannalta korkean riskin.*
- *Tietojen kirjaaminen. Pienten ja keskisuurten yritysten ei tarvitse pitää kirjaa käsittelytoimista – paitsi jos käsittely on säännöllistä tai todennäköisesti vaarantaa sen henkilön oikeudet ja vapaudet, jonka tietoja käsitellään, tai sisältää arkaluonteisia tietoryhmiä.*
- *Nykyaikainen työkalupakki kansainvälisiin tiedonsiirtoihin. Yleisessä tietosuoja-asetuksessa tarjotaan erilaisia välineitä tietojen siirtämiseksi EU:n ulkopuolelle, mukaan lukien Euroopan komission tekemät tietosuojan riittävyyttä koskevat päätökset, joissa EU:n ulkopuolinen maa tarjoaa riittävän suojan tason, ennalta hyväksytyt (vakiomuotoiset) sopimuslausekkeet, sitovat yrityssäännöt, käytännesäännöt ja sertifiointi.*

(EUR-Lex 2022.)

4.8.3 Tietosuojalaki

Tietosuojalaki (1050/2018) täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta ja sen kansallista soveltamista. Laissa säädetään muun muassa tietosuoja-asioita valvovan viranomaisen nimittämisestä ja organisaatiosta sekä sen toimivaltuuksista. Lisäksi tietosuojalaissa säädetään seuraavista:

- *lapsiin sovellettavasta ikärajasta tietoyhteiskunnan palveluita tarjottaessa*
- *erityisten henkilötietoryhmien käsittelystä*
- *henkilötietojen käsittelystä journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten*
- *henkilötunnuksen käsittelemisestä*
- *eräistä tilanteista, joissa yleinen etu on oikeusperuste henkilötietojen käsittelylle ja*
- *rajoituksista rekisteröidyn oikeuksiin.*

(Tietosuojavaltuutetun toimisto 2024b.)

Tietosuojalailla kumottiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Tietosuojalaki on henkilötietojen käsittelyyn sovellettava yleislaki, joka ei muodosta itsenäistä ja kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan rinnakkain EU:n yleisen tietosuoja-asetuksen kanssa. (Andreasson & Ylipartanen 2022, 30.)

4.8.4 Rikoslaki

Rikoslaki (19.12.1889/39) tunnistaa mm. tietomurron ja jo sen yritys on tuomittava. Rikoslain 38 luvun 8 §:n mukaan:

> ”Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen

> osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetusta tietojärjestelmässä olevasta tiedosta. Yritys on rangaistava.”

Rikoslaissa säädetään myös rikkomuksiin liittyvistä rangaistuksista. Esimerkiksi 38 luvun 9 § säätää mm.:

> ”Joka muutoin kuin luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus), tarkoitettuna rekisterinpitäjänä tai henkilötietojen käsittelijänä tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin:
>
> 1) yleisen tietosuoja-asetuksen
> 2) tietosuojalain (1050/2018)
> 3) henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) tai
> 4) henkilötietojen käsittelyä koskevan muun lain
>
> henkilötietojen käyttötarkoitussidonnaisuutta, luovuttamista tai siirtämistä koskevaa säännöstä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava *tietosuojarikoksesta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.”

Tilin kaappaaminen on tietomurto. Mikäli tekoon liittyy taloudellisen hyödyn tavoittelu uhrin kustannuksella, kyse on petoksesta. (Järvinen 2022, 168.) Identiteettivarkaus lisättiin Järvisen (2022, 168) mukaan rikoslakiin 2015. Lain 38. luvun 9 a § määrittelee identiteettivarkauden näin:

> ”Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.”

4.8.5 Perustuslaki

Viestintäsalaisuus on turvattu perustuslaissa (11.6.1999/731). Perustuslain 2. luvun 10 §:n mukaan:

> ”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.”

Perustuslain takaama viestintäsalaisuus koskee myös ammattiliittoja siltä osin, että työnantajat eivät saa ilman lainmukaista perustetta tarkastella työntekijöidensä yksityistä viestintää, kuten sähköposteja tai muita luottamuksellisia viestejä. Suomessa yksityisyyden suojaan liittyviä asioita valvoo, käsittelee ja ohjeistaa tietosuojavaltuutetun toimisto.

Perustuslaki antaa siis yksityisyydelle suojan perusoikeutena, mutta työntekijöiden yksityisyyden suojaa ja henkilötietojen käsittelyä työelämässä säätelee tarkemmin laki yksityisyyden suojasta työelämässä.

4.8.6 Laki yksityisyyden suojasta työelämässä

Laki yksityisyyden suojasta työelämässä (13.8.2004/759) määrittelee työntekijän yksityisyyden suojan tarkemmat säännöt. Lain 1 luvun 2 §:ssä todetaan:

> ”Tässä laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta”.

Tämä tarkoittaa, että työnantajan on noudatettava säännöksiä työntekijöiden henkilötietojen käsittelyssä ja työpaikan teknisessä valvonnassa, kuten kameravalvonnassa tai sähköpostin käytön seurannassa. Lain tarkoituksena on turvata työntekijöiden yksityisyys työelämässä ja varmistaa, että työnantajan toimet ovat oikeasuhtaisia ja perusteltuja.

5 KYSELYTUTKIMUS AMMATTILIITTOJEN TIETOSUOJAVERKOSTOLLE

Tutkimuksen primääriaineisto kerättiin kyselytutkimuksella, jonka kohderyhmäksi löytyi sopiva ryhmä: Akavalaisten liittojen tietosuojaverkosto. Tietosuojaverkosto koostuu noin neljästäkymmenestä eri liitoissa työskentelevistä henkilöistä, joiden työhön kuuluu joko tietosuoja- tai tietoturva-asiat omassa liitossaan.

Kysely lähetettiin sähköpostitse vastaajajoukolle 18.9.2024 ja vastausaikaa annettiin 30.9.2024 asti. 26.9.2024 lähetettiin vastaajille muistutussähköposti, jossa kerrottiin olevan pari viimeistä päivää aikaa vastata. Sähköpostin ja kyselyn aiheen oli ”Ammattiliittojen kyberturvallisuuskulttuurin vaikutus arkaluonteisen tiedon suojaamiseen”. Sähköpostin lähettäjänä toimi tämän opinnäytetyön tekijä, Suomen Ekonomien tietohallintopäällikkö. Sähköpostissa kerrottiin kyselyn olevan osa tutkimuksen tekijän opinnäytetyötä.

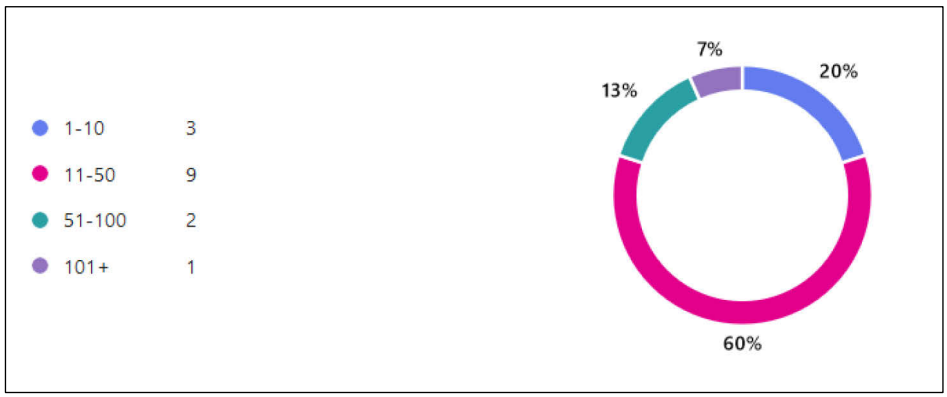
Kysely oli jaettu viiteen eri osa-alueeseen vastaamisen helpottamiseksi ja rytmittämiseksi. Kyselyn eri osa-alueet kysymyksineen ja vastauksineen on esitetty seuraavissa alaotsikoissa. Kyselyn vastauksista johdetut johtopäätökset on esitelty omassa luvussaan tämän luvun jälkeen.

Kyselyyn vastattiin anonyymisti yksilöiden ja organisaatioiden suojaamiseksi. Kyselyn lopuksi tiedusteltiin halukkuutta osallistua haastattelututkimukseen, joten siltä osin nimitiedot sai antaa halutessa. Haastatteluun suostui kaksi henkilöä. Haastattelut suoritettiin mutta niiden vähäisen määrän vuoksi tuloksia ei hyödynnetty tässä opinnäytetyössä.

Haastattelun vastausprosentti oli 37,5. Vastausprosentti oli heikompi kuin ennakkoon odotettiin. Odotukset olivat korkeammat johtuen siitä, että vastaanottajien verkosto koostui nimenomaan aiheeseen liittyen. Toisaalta matala vastausprosentti voi kieliä siitä, että aiheeseen liittyvään kyselyyn vastaaminen tuntuu haastavalta eikä omaa tietämättömyyttä haluta paljastaa. Siitäkin huolimatta, että kyselyyn vastattiin anonyymisti. Vastauksien määrässä voi heijastua myös ammattiliittojen henkilöstön keskuudessa yleinen kiire ja ajanpuute. Tietosuoja- ja tietoturvavastaavan töitä tehdään oman työn ohessa, joten voi olla, että yleisesti Akava-yhteisöä hyödyttäviä asioita ei koeta tai ehditä kokea tärkeäksi.

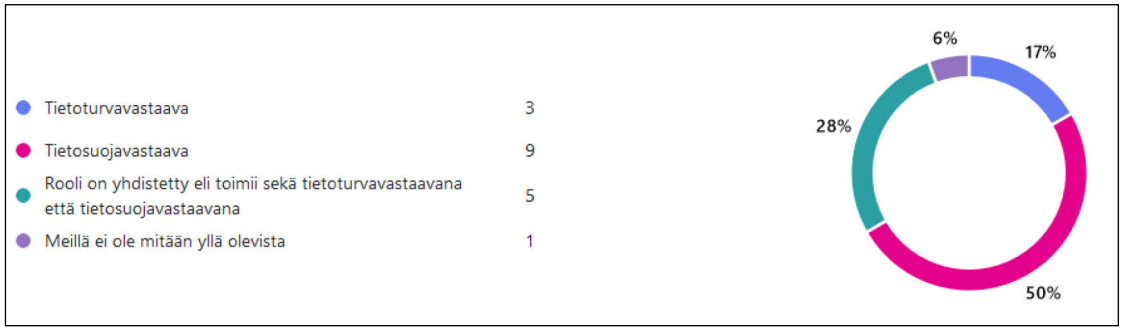
5.1 Taustatiedot

Kyselyn aluksi kysyttiin taustatietoja vastaajan organisaatiosta (kuva 18). 60 % vastaajista oli organisaatiossa, jossa on 11–50 työntekijää. 20 % vastaajista tuli organisaatiosta, jossa on alle 10 työntekijää. 13 % vastaajista tuli 51–100 henkilön organisaatiosta.



Kuva 18. Kyselyyn vastanneiden organisaatioiden koot henkilömäärän mukaan

Seuraavaksi taustatietona kysyttiin, onko organisaatiossa tietoturva- ja tietosuojavastaavia tai onko roolit yhdistetty (kuva 19). 50 %:ssa organisaatioista oli nimetty tietosuojavastaava. Tietoturvavastaava oli 17 %:lla organisaatioista. 28 %:sta organisaatioista roolit olivat yhdistettyjä eli sama henkilö toimii sekä tietosuoja- että tietoturvavastaavana. Yksi organisaatio kertoi, että heillä ei ole kumpaakaan roolia. Kyselyssä kysyttiin myös, onko edellä mainitut roolit organisaation omia työntekijöitä vai ulkoistettuja resursseja. 93 % kertoi roolien olevan omia työntekijöitä. Yksi organisaatio ilmoitti, että roolit ovat sekä omia että ulkoistettuja.



Kuva 19. Onko organisaatiossa tietoturva- ja tietosuojavastaava

5.2 Kyberturvallisuuskulttuuri

Varsinainen tutkimuksellinen osio aloitettiin kartoittamalla kyberturvallisuuskulttuuriin liittyviä asioita. Ensimmäisenä kysyttiin kuinka tärkeänä organisaation johto pitää kyberturvallisuutta. Erittäin tärkeänä pitää 33 %, 53 % tärkeänä ja 13 % neutraalina. Kukaan vastaajista ei ilmoittanut, että johto pitäisi kyberturvallisuutta jonkin verran tai ei lainkaan tärkeänä.

Seuraavana kysyttiin miten hyvin henkilöstö noudattaa tietoturvakäytäntöjä, kuten salasanojen käyttöä ja monivaiheista tunnistautumista vastaajan havaintojen mukaan. Vastaukset jakaantuivat seuraavasti: 13 % erittäin hyvin, 67 % hyvin, neutraalisti 7 % ja jonkin verran 13 %.

Kyberuhkien tietoisuudesta kysyttiin: ”Kuinka hyvin mielestäsi henkilöstö on tietoinen kyberuhista, kuten tietojenkalastelusta ja haittaohjelmista?” Erittäin tietoinen vastasi 13 %, tietoinen 73 % ja neutraali 13 %. Kukaan ei vastannut, että uhkien tietoisuus olisi tasolla jonkin verran tietoinen tai ei lainkaan tietoinen. Tämä kysymys oli mielenkiintoinen, jos vertaa sitä kysymykseen, jossa kysyttiin: ”Kuinka usein järjestätte koulutuksia kyberturvallisuustietoisuuden lisäämiseksi?” Siihen 20 % vastasi, että koulutuksia ei ole ollenkaan käytössä. 53 % ilmoitti, että koulutuksia järjestetään kerran vuodessa tai harvemmin. Kukaan ei järjestä koulutuksia kuukausittain. Koulutuksia siis järjestetään suhteellisen harvoin, mutta vastaajien mielestä henkilöstö on tietoisia kyberuhista. Tästä voisi päätellä, että jos on kerran saanut koulutuksen, oletetaan, että homma on hallussa ja tilanne hyvä. Uhkat vaan eivät ole stabiileja, ne muuntuvat ja muuttuvat nopeallakin syklillä.

Seuraavaksi kysyttiin, onko vastaajan mielestä henkilöstöllä tarvittava tieto siitä, miten toimia tietoturva- tai tietosuojaloukkauksen sattuessa omien havaintojen pohjalta. 73 %:lla tietoisuus on tasolla osittain ja 27 % on tasolla tietoinen. Kukaan ei vastannut, että henkilöstöllä ei olisi tarvittavaa tietoa. Kuitenkin 20 % vastaajista kertoi, että organisaatiossa ei järjestetä mitään koulutusta aiheesta. Tästä herää epäilys, miten henkilöstöllä voi olla tieto, jos heille ei tarjota koulutusta. Odotetaanko henkilöstön imevän tarpeelliset tiedot itse jostain?

Henkilöstön suhtautumista kyberturvallisuuskäytäntöihin ja niiden noudattamiseen vastattiin niin, että negatiivinen suhtautuminen ei ollut kellään. Positiivisesti suhtautui 53 % organisaatiosta ja neutraalisti 47 %. Henkilöstö suhtautuu siis kyberturvallisuusasioihin vähintäänkin neutraalisti, yli puolet positiivisesti. Näin ollen maaperä kyberturvallisuutta lisäävälle tietoisuudelle on otollinen. Kun jatkettiin kysymyksellä, ”Miten arvioisit henkilöstön asenteita ja motivaatioita kyberturvallisuuskäytäntöjen noudattamisessa” yleisin vastaus oli jonkin verran motivoitunut 73 %, 7 % ilmoitti erittäin motivoitunut ja ei erityistä motivaatiota 20 %.

Seuraavaksi kysyttiin, onko organisaatiossa selkeä roolitus ja vastuunjako kyberturvallisuuden osalta. Erittäin selkeä tai osittain selkeä vastasi 73 %, kun taas epäselvästä vastuunjaosta kertoi 27 % vastaajista. Kysyttäessä kuinka paljon aikaa käytetään organisaatiossa kyberturvallisuuteen liittyvien tehtävien toteuttamiseen, liian vähän vastasi 60 %, riittävästi 33 % ja 7 % ei osannut sanoa.

Kyberturvallisuuskulttuurin avoimissa vastauksissa vastattaessa kysymykseen ”Mitä konkreettisia vaikeuksia olet huomannut kyberturvallisuuskulttuurin jalkauttamisessa?” korostuu ajan, resurssien ja osaamisen puute. Esimerkkisitaatti:

> *”Ajan ja resurssien puute. Kun on kiire, ei ole liioin aikaa perehtyä, vaikka asia olisikin tärkeä.”*

Muita havaintoja kuvaavia sitaatteja seuraavassa:

”Kyberturvallisuus saatetaan kokea it:n asiana, eikä se järjestöllisten tai edunvalvonnallisten asioiden ohella saavuta riittävää keskustelua hallinnossa, vaikka loppupelissä vastuu olisi siellä.”

” Asia on arka, joka vaikeuttaa ymmärtämään turvallisuuden tason koko tston osalta.”

Kysyttäessä selkeistä puutteista kyberturvallisuuden nykykäytännöistä, ei vastaajat ole havainneet mielestään suuria puutteita. Ajanpuute kuitenkin heijastuu näissäkin vastauksissa, sekä yksittäisiä havaintoja, esimerkiksi seuraavat:

”Esillä hallinnossa liian vähän.”

”Emme ole havainneet. Olemme luottaneet ulkopuoliseen IT-tukeemme.”

”Jatkuvuus, henkilöstön valvonta/tukeminen.”

Kysyttäessä suoraan, kuinka vahvana vastaajat pitävät oman organisaation kyberturvallisuuskulttuurin tasoa, vahvana tai erittäin vahvana piti 53 % ja neutraalina 47 %.

Avoimissa vastauksissa, miten organisaatioissa kasvatetaan kyberturvallisuuskulttuuria, korostuu (53 %) epäsäännöllisten koulutusten järjestäminen. Eli tyydytään siihen, että kyberturvallisuudesta silloin tällöin järjestetään koulutus tai perehdytys. Alla muutama vastaus, josta on luettavissa, että organisaatio on ottanut kyberturvallisuuskulttuurin vakavasti:

”Kyberturvapolitiikan käyttöönotto. Politiikka perustuu iso27001:een. Henkilökunnan jatkuva koulutus. Tilannekuvasta tiedottaminen johtoryhmälle ja henkilökunnalle.”

”Koulutamme henkilöstä säännöllisesti. Lisäksi nostamme ajankohtaisia aiheita esille. Teemme tietoturvatestejä.”

Avoimissa vastauksissa, joista käy ilmi, että kyberturvallisuuskulttuuria ei ole otettu tekemiseen mukaan, löytyy mm. seuraavia kommentteja:

”IT-tukemme kiinnittää tarvittaessa huomiotamme riskitekijöihin.”

”Satunnaisesti esillä toimistopalavereissa.”

” Ei suunniteltua ohjelmaa.”

5.3 Kyberturvallisuustietous

Kolmannessa osiossa kysyttiin kyberturvallisuustietouteen liittyviä asioita. Eniten käytössä oli säännölliset koulutukset, tiedotuskampanjat sekä tietoturva- ja tietosuojatestit, kaikissa 40 %. On huomattavaa kuitenkin, että 20 % vastasi, että mikään annetuista menetelmistä ei ole käytössä. Verkkokoulutukset olivat vähiten käytössä, 7 % organisaatioista. 13 % vastasi menetelmänä olevan joku muu kuin edellä mainitut.

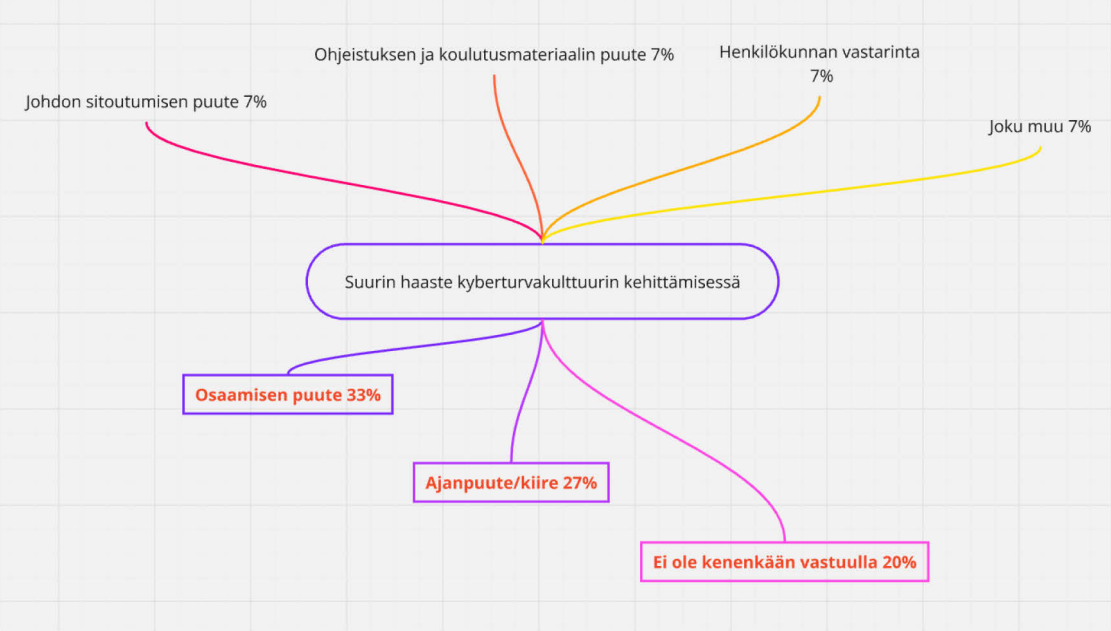
Kun kysyttiin kuinka usein organisaatio tiedottaa henkilökuntaa kyberturvallisuusasioista, yleisin vastaus oli kerran vuodessa tai harvemmin (27 %). Jälleen huomioitavaa on se, että 20 % ilmoitti, ettei tiedota henkilökuntaa miten-kään kyberturvallisuusasioista. 20 % kertoi kouluttavansa henkilökuntaa kerran kvartaalissa tai kerran puolessa vuodessa. 13 % kertoi kouluttavansa kerran kuukaudessa tai useammin.

Tietoturvatestit eivät ole kyselyn mukaan pääsääntöisesti käytössä. Organisaatiot, joissa mitään testejä ei tehdä oli 47 %. 20 % vastasi, että testejä järjestetään kvartaaleittain tai kuukausittain.

5.4 Esteet ja haasteet kyberturvallisuuskulttuurin kehittämisessä

Neljännessä osiossa kysyttiin haasteista ja esteistä liittyen kyberturvallisuuskulttuurin kehittämiselle. Kysyttäessä yhtä suurinta haastetta organisaation kyberturvallisuuskulttuurin kehittämisessä, suurin haaste oli kyberturvallisuusosaamisen puute (33 %), seuraavaksi yleisin haaste oli ajanpuute / kiire (27 %) ja kolmanneksi yleisin haaste oli, että se ei ole kenenkään vastuulla / osoittaa resurssia (13 %).

Haasteet koottiin mindmap-muotoon paremman visuaalisen havainnoinnin mahdollistamiseksi. Suurimmat haasteet -mindmap löytyy kuvasta 20.



Kuva 20. Suurimmat haasteet kyberturvallisuuden kehittämisessä

Mielenkiintoista oli, kun tämän kysymyksen rinnalle otettiin tekoälyn (ChatGPT 4) avulla kysymys: ”Kuinka usein organisaatiossa tehdään tietoturvariskien kartoitusta verrattuna suurimpiin haasteisiin?” Säännöllisesti riskikartoitusta tekee vain 27 % organisaatioista eli hieman yli joka neljäs organisaatio. Organisaatiot, jotka tekevät riskien kartoitusta säännöllisesti, nimesivät haasteikseen mm. resurssien puutteen, johdon esimerkin tarpeen sekä kyberturvan hallintapalvelun käyttöönoton tarpeen**.** Epäsäännöllisesti kartoitusta tekevät (53 %) organisaatiot puolestaan kokivat suurimmiksi haasteiksi ajan ja osaamisen puutteen, koulutuksen säännöllisyyden puutteen ja selkeiden toimintamallien puutteen. Organisaatioista 20 % ilmoitti, ettei tietoturvariskien kartoitusta tehdä lainkaan. Näissä organisaatioissa suurimmaksi haasteeksi nousi IT-tuen vaihtuvuus ja selkeän johdon tuen ja vastuunjaon puute. Tulokset osoittavat, että ajan puute korreloi selvästi epäsäännöllisen riskienhallinnan kanssa – kun aikaa ei ole varattu, riskien kartoitus jää tekemättä tai sitä tehdään satunnaisesti. Toisaalta organisaatiot, jotka tekevät kartoitusta säännöllisesti, kohtaavat enemmän haasteita resurssien ja vastuunjaon selkeydessä. Riskien kartoitusta tekemättömillä organisaatioilla ongelma näyttää liittyvän perusrakenteiden ja johdon roolin epäselvyyteen.

Muita haasteita kysyttäessä ajanpuutteen rinnalla nousivat suurimmaksi vähäinen kyberuhkien ymmärrys (53 %), ei ole kenenkään vastuulla / osoittaa resurssia (47 %) ja kyberturvallisuusosaamisen puute (40 %). 33 % organisaatioista kertoi haasteeksi ohjeistuksien ja koulutusmateriaalien puutteen, taloudelliset tekijät ja kiinnostuksen puute. 13 % ilmoitti haasteeksi johdon sitoutumisen puutteen. Huomioitavaa tämän kysymyksen osalta, että vastaajat saivat valita niin monta haastetta kuin halusivat.

Suurimpia uhkia kyberturvallisuuden kehittämiselle omassa organisaatiossa mainittiin suurimmiksi 40 % ajanpuute, resurssien puute 27 % ja kiinnostuksen puute 20 %. Yksittäinen mielenkiintoinen uhka nähtiin myös it-kumppanin osaamattomuudessa ja yksi nimesi uhkaksi kehittämiselle ihmiset.

Johdon sitoutuminen nähtiin pääsääntöisesti hyvänä, 53 % vastauksista. Hyvän sitoutumisen merkkeinä tutkimuksessa pidettiin, jos johto on sitoutunut ja kiinnostunut kyberturvallisuudesta, on ymmärtänyt oman roolinsa vastuunkantajana ja asiasta keskustellaan säännöllisesti johtoryhmässä sekä kyberturva on osana toimintasuunnitelmaa. Vastakkaisiakin vastauksia löytyi. Täysin negatiivinen suhtautuminen tai suhtautumista ei juurikaan näy, vastasi 13 % organisaatioista. Yksi vastauksista oli esimerkiksi seuraava:

> *”Sitoutumista ei näy oikein mitenkään. Kyberturvallisuudesta ei puhuta, sitä ei seurata sen kummemmin.”*

Loput 34 % vastasi sitoutumisen olevan joko neutraalia tai jotain siltä väliltä. Näissä vastauksissa korostuivat ns. näennäiset sitoutumiset eli johto on antanut esim. jonkin yksittäisen ohjelman hankintaan rahat tai kirjauksen toimintasuunnitelmaan, mutta asian eteen ei muuta tehdä. Herättäviä vastauksia olivat seuraavat:

”Operatiivinen johto pyrkii edistämään, luottamushallinto ei koe omakseen.”

”Johto pitää asiaa tärkeänä, muttei varsinaisesti ajattele asiaa.”

”Mainintana toimintasuunnitelmassa, suunnitelmana vaihtaa it-tukifirmaa.”

”Kuinka hyvin organisaatioissa on varauduttu tietoturva- ja tietosuojaloukkauksiin?” Tähän kysymykseen vastasi hyvin 40 %, neutraali 33 %, huonosti 13 % ja erittäin hyvin 13 %. Kukaan vastaajista ei vastannut varautumisen olevan todella huonosti. Toisin sanoan, huonosti ja erittäin hyvin varautuneita oli täsmälleen saman verran. Jos lasketaan neutraalien ja hyvin varautuneiden vastaukset yhteen, hyvin tai neutraalisti varautuneita organisaatioita on kolme neljästä ammattiliitosta.

Kun sitten kysyttiin, onko ammattiliitolla ollut kahden edellisen vuoden aikana tietoturvaloukkauksia (sisältäen tietosuojaloukkaukset), vastasi 53 % kyllä. 47 % vastasi, että tietoturvaloukkauksia ei ole ollut. Tästä herää mielenkiintoinen jatkokysymys, onko todella näin, että lähes puolella ei loukkauksia ole ollut, vai eikö niitä ole havaittu? Varsinkin, jos verrataan varautumisen tasoon, joka osalla oli verrattain matala.

Mielenkiintoista oli verrata tekoälyn avulla (ChatGPT 4) tietoturvapoikkeamien havaitsemista verrattuna organisaation kokoon ja tietoturva- ja tietosuojavastaavien roolin olemassaoloa sekä kyberturvallisuuden organisointia. Pienissä organisaatioissa (1 –10 työntekijää) ei raportoitu havaittuja tietoturvapoikkeamia, keskisuurissa (11–50 työntekijää) tietoturvaloukkauksia raportoitiin useimmin, kun taas suurissa (101+ työtekijää) tietoturvaloukkauksia raportoitiin harvemmin mutta niitä kuitenkin oli. Organisaatioita, joissa vastuunjako oli epäselvä, tietoturvaloukkauksia oli useammin kuin organisaatioissa, joissa vastuut ovat selkeämmin määriteltyjä. Niissä loukkausten määrä oli alhaisempi, erityisesti silloin, kun vastuunjako oli erittäin selkeä. Nämä tulokset viittaavat siihen, että selkeä roolitus ja vastuunjako voivat vähentää tietoturvaloukkausten määrää.

Pureuduin tarkemmin organisaatioihin, joissa tietoturvapoikkeamia ei ollut havaittu, verrattuna organisaatioihin, joissa niitä havaittiin. Analysoinnin apuna käytin tekoäly (ChatGPT 4). Vertailin seuraavia tekijöitä havaitsemattomuuteen ja tulkitsin seuraavia asioita:

1. Osaamisvaje: Organisaatiot, joissa koetaan puutteita kyberturvallisuusosaamisessa, voivat jäädä heikommiksi havaitsemaan tietoturvaloukkauksia.
2. Koulutusten puute: Jos koulutuksia ei järjestetä tai niitä on harvoin, henkilöstön kyky havaita loukkauksia voi olla heikko.
3. Vastuunjako: Epäselvä vastuunjako voi johtaa siihen, ettei kukaan seuraa aktiivisesti tietoturvapoikkeamia.
4. Seuranta- ja valvontakäytännöt: Organisaatiot, joissa on selkeämmät valvontakäytännöt, havaitsevat todennäköisesti enemmän loukkauksia.

Vertasin kyberturvaosaamisen puutetta ja tietoturvaloukkausten raportointia edelleen tekoälyn avulla. Havaitsin että osaamisvaje on yhteydessä tietoturvaloukkausten raportoinnin vähyyteen. Analyysin perusteella organisaatiot, jotka kokevat kyberturvallisuusosaamisen puutteen olevan suuri haaste (20 %), raportoivat vähemmän tietoturvaloukkauksia (13 %). Tämä voi viitata siihen, että osaamisvaje saattaa johtaa havaitsemattomiin tietoturvaloukkauksiin. Organisaatiot, joissa osaamista ei koeta merkittäväksi ongelmaksi (27 %), raportoivat enemmän tietoturvaloukkauksia (40 %), mikä voi viitata parempaan valmiuteen havaita ja käsitellä näitä tapauksia. Tämä analyysi tukee hypoteesia, jonka mukaan osaamisvaje voi estää tietoturvaloukkausten havaitsemisen.

5.5 Tietoturvariskien hallinta ja tietosuojakäytännöt

Neljännessä osiossa kysyttiin tietoturvariskien hallinnasta ja tietosuojakäytännöistä. Kysymykseen, onko organisaatiolla käytössä virallinen tietoturvariskien hallintasuunnitelma, suurin osa eli 60 % vastasi ei. Riskienhallintasuunnitelman olemassaolon tunnisti 27 % ja 13 % ei tiennyt, onko organisaatiolla sellaista.

Tietoturvariskien arviointeja tehdään pääsääntöisesti epäsäännöllisesti, 53 %. Säännöllisesti niitä tehdään 27 % organisaatioista. 13 % organisaatioista riskejä ei arvioida koskaan. 7 % ei tiennyt kuinka usein riskejä arvioidaan. 80 % ammattiliitoista riskejä siis arvioidaan vähintäänkin epäsäännöllisesti, mutta riskienhallintasuunnitelma on vain vajaa joka kolmannella ammattiliitolla. Yli puolella ammattiliitoista riskienhallintasuunnitelmaa ei ole ollenkaan.

Vertailin tekoälyn avulla (ChatGPT 4) kysymyksiä, joissa kysyttiin organisaation johdon sitoutumista ja virallisen riskienhallintamallin käyttämistä. Tuloksista näkyy, että organisaatiot, joissa johto pitää kyberturvallisuutta tärkeänä ja on selvästi sitoutunut sen edistämiseen, ovat todennäköisemmin ottaneet käyttöön virallisen tietoturvariskien hallintasuunnitelman. Johto, joka on sitoutunut ja ymmärtää kyberturvan tärkeyden, liittyy useammin virallisiin riskienhallintakäytäntöihin, kun taas niissä organisaatioissa, joissa johdon sitoutuminen ei ole selkeää, riskienhallintaa ei useinkaan ole. Tämä viittaa siihen, että johdon aktiivinen sitoutuminen kyberturvallisuuteen on tärkeä tekijä riskienhallintakäytäntöjen kehittämisessä ja ylläpitämisessä.

Kysyttäessä selkeitä käytäntöjä arkaluonteisen tiedon suojaamiseksi, 80 % ilmoitti olevan selkeät käytännöt. 13 % ilmoitti, että selkeitä käytäntöjä ei ole ja 7 % ilmoitti, ettei tiedä.

Kysyttäessä kuinka hyvin henkilökunta tuntee tietosuojalainsäädännön vaatimukset työssään, 80 % vastasi hyvin. Neutraaliksi ilmoitti 40 % vastaajista. Mielenkiintoinen huomio on, että kukaan ei vastannut erittäin hyvin eikä puolestaan kukaan huonosti tai erittäin huonosti. Tästä voi päätellä, että GDPR:n olemassaolo tunnetaan vähintäänkin neutraalisti tai hyvin.

Kysyttäessä, onko tietosuoja otettu huomioon organisaation kaikissa toiminnoissa, hieman yli puolet eli 53 % vastasi osittain, 47 % vastasi kyllä on otettu huomioon.

5.6 Parannusehdotukset ja avoin palaute

Viimeisessä osiossa kysyttiin vapaata palautetta ja parannusehdotuksia omaan organisaatioon. Vastaajia pyydettiin kertomaan mitä parannuksia toivottaisi kyberturvallisuuskulttuurin edistämiseksi organisaatiossa ja pyydettiin pohtimaan nimenomaan kulttuurin kehittämistä. Eniten vastauksissa toivottiin säännöllisyyttä 33 %. Tämä näkyi vastauksissa mm. seuraavasti:

> *”Aiheesta kouluttaminen olisi säännöllistä ja jonkun ulkopuolisen ammattilaisen toteuttamaa.”*

> *”Selkeämmät käytännöt, säännölliset läpikäynnit.”*

> *”Säännöllinen käsittely, ohjeistuksen tarkastaminen, valvonta.”*

Myös aikaisemmissa kysymyksissä esiin tulleet asiat kuten resurssit, aika ja osaamisen lisääminen nousivat esiin.

Viimeinen kysymys oli miten organisaationne voisi parhaiten kehittää kyberturvallisuutta tulevaisuudessa? Tässä kysymyksessä vastaukset hajautuivat eniten. 40 %:ssa vastauksista nousi esiin jollain tavalla kyberturvallisuuden nostaminen kiinteäksi osaksi tekemistä. Hallintamalli, hallituksen agendalle säännöllisenä elementtinä lisääminen, auditoinnit ja osaamisen kartuttaminen näkyivät kehittämistoiveina. Seuraavien vastausten myötä näkyy kehittämiskohteet, jotka tämänkin tutkimuksen tekemisen myötä ovat nousseet:

> *”Kehittämisessä yleisesti puuttuu kyberturvallisuuden huomioiminen. Projekteissa saattaa tulla muutoksia ja tällöin pitäisi tiedottaa myös kyberturvallisuudesta vastaavia.”*

> *”Saada lisää rahaa kunnollisten tietoturvajärjestelmien hommaamiseen, jolloin saataisiin kaikki dokumentoinnit ym. hallitusti sinne ja tiedämme mitä puuttuu ja mitä pitää milloinkin päivittää.”*

> *”Lisäämällä tietoisuutta, tekemällä auditointeja, lisäämällä koulutusmahdollisuuksia.”*

5.7 Kyselytutkimuksen löydökset

Tutkimuksen primääriaineiston vastausten perusteella voidaan päätellä selkeästi muutamia tärkeitä havaintoja tutkimuksen kohteena olevista ammattiliitoista. Löydökset on esitetty kootusti seuraavien alaotsikoiden alla.

5.7.1 Riskienhallinnan ja vastuiden merkitys

Tutkimuksen primääriaineiston vastauksista voidaan päätellä, että suurin osa ammattiliitoista pitää kyberturvaa tärkeänä asiana ja liitot sanovat kiinnittävänsä siihen huomiota mutta läheskään kaikilla ei ole riskienhallintaan vakiintunutta tapaa, joka on perusasia kyberturvan hallinnan kannalta. Tämä voi johtua useista syistä:

1. **Johdon sitoutuminen on puutteellista**: Johto saattaa ilmaista yleistä huolta kyberturvasta ja pitää sitä tärkeänä, mutta käytännön toimenpiteet, kuten riittävä resursointi, puuttuvat.
2. **Osaamisvaje**: Ammattiliitoilla ei välttämättä ole tarvittavaa asiantuntemusta tai resursseja kehittää ja ylläpitää kyberturvallisuuteen liittyviä tehtäviä.
3. **Kulttuurin ja toiminnan välinen kuilu**: Ammattiliitot saattavat nähdä kyberturvan tärkeänä, mutta eivät ole vielä konkretisoineet tätä sitoutumista muodollisten prosessien tai käytäntöjen kautta.
4. **Kyberturvan "pinnallinen" huomiointi**: Monissa ammattiliitoissa saatetaan puhua kyberturvallisuudesta, mutta syvällinen analyysi ja jatkuvat toimet voivat puuttua. Tämä voi johtaa siihen, että varotoimet eivät ole riittäviä käsittelemään todellisia tai alakulttuureissa piileviä riskejä.

Nämä asiat viittaavat siihen, että vaikka tietoisuus kyberturvasta on korkea, käytännön toimenpiteiden, kuten riskienhallinnan implementoinnissa on selkeitä puutteita. Vertailtaessa tutkimuksen tuloksia Boehmin ym. (2019, 4) esittämään malliin kyberturvatekemisen portaikosta voidaan positiivisimmankin mielipiteen pohjalta sanoa pienen osan olevan edistyneessä riskiperusteisessa kyberturvatekemisessä, suurin osa on perustasolla joko niin, että kyber-

turvaa ei ole otettu huomioon tai tekeminen on teknisperusteista. Mikään ammattiliitto ei ole tämän tutkimuksen perusteella edistyneimmällä proaktiivisella kyberturvatekemisen tasolla.

Tämän tutkimuksen tulokset osaajapulasta heijastelevat samaa mitä mm. tämän työn alussa mainittu DNA:n Tietoturvatutkimus (2024). Osaajapula on yrityksille valtava haaste. Saman haasteen kanssa kamppailevat yritykset koosta riippumatta. Kukaan ei pärjää yksinään.

Kun syvennetään analyysia kyberturvavastuiden selkeyden ja epäselvyyden kautta siihen, miten nämä vaikuttavat riskienhallinnan käytäntöihin löydetään selkeä yhteys. Ammattiliitoissa, joissa vastuunjako on epäselvä, virallista tietoturvariskien hallintasuunnitelmaakaan ei pääsääntöisesti ole käytössä. ammattiliitoissa, joissa vastuunjako on osittain tai erittäin selkeä, virallinen riskienhallintasuunnitelma on yleisempi. Tämä viittaa siihen, että selkeä vastuunjako on tärkeä tekijä kyberturvallisuuskulttuurin edistämisessä. Epäselvät vastuut voivat johtaa mm. riskienhallinnan laiminlyöntiin, mikä puolestaan lisää tietoturvariskejä.

5.7.2 Tietoisuuden ja koulutuksen merkitys

Kyberturvallisuuskulttuurin ylläpitäminen ja arkaluonteisen tiedon suojaaminen edellyttävät jatkuvaa tietoisuuden lisäämistä ja henkilöstön kouluttamista. Tässä tutkimuksessa ilmeni, että vaikka useimmat ammattiliitot kokevat kyberturvallisuuden tärkeäksi osaksi toimintaansa, säännöllisiä koulutuksia ei läheskään aina järjestetä. Erityisesti verkkokoulutuksia ja muita jatkuvaa oppimista tukevia menetelmiä puuttui monista organisaatioista, mikä lisää riskiä, että henkilöstö ei ole täysin tietoinen oikeista toimintatavoista arkaluonteisen tiedon käsittelyssä. Erilaisia tietoisuuden lisäämisen tapoja on lukuisia mutta niitä ei joko osata hyödyntää tai kukaan ei koordinoi niiden toteutusta.

Koulutuksen puute voi johtaa inhimillisiin virheisiin, jotka ovat merkittävä tietoturvariskin lähde. Kyberturvallisuuskoulutuksen tulisi olla jatkuvaa ja se tulisi räätälöidä organisaation tarpeiden mukaan. Säännölliset tietoisuuskampanjat ja käytännönläheiset harjoitukset voisivat auttaa henkilöstöä ymmärtämään

paremmin kyberturvan periaatteita ja soveltamaan niitä päivittäisessä työssään. Tämä olisi myös tehokas tapa vähentää riskiä, että arkaluonteista tietoa käsitellään huolimattomasti tai väärin.

Luovuuden ja työntekijöiden innovoinnin tukeminen on uudenlainen tapa lisätä kyberturvallisuustietoisuutta. Sen käyttö keinona on mahdollista vain keskustelevassa, tasa-arvoisessa ja epä-hierarkkisessa kulttuurissa. Luovuuden ja innovoinnin tulee tapahtua vallitsevien tietoturvaohjeiden rajoissa mutta innovoinnin tukeminen voi vahvistaa sekä työntekijöiden tietoisuutta että organisaation tietoisuutta kyberturvallisuutta vahvistavista tai heikentävistä keinoista. Organisaatiot, jotka mahdollistavat joustavan ja avoimen kulttuurin, rohkaisevat työntekijöitä löytämään luovia ratkaisuja tietoturvankin haasteisiin. Tämä lisää edelleen sitoutumista ja innovaatiokykyä. Tässä tutkimuksessa ei löytynyt viitteitä kyberturvan uusista, innovatiivisista tavoista kyberturvallisuuskulttuurin ympäriltä. Toisaalta tätä ei suoraan tutkimuksessa edes kysytty.

Tutkimuksessa ei tullut ilmi mitään viitteitä tahallisesta sisäisestä inhimillisestä uhkatekijästä. Toisaalta tutkimuksessa ei tätä suoraan kysyttykään. Voidaan olettaa tämän kuitenkin olevan häviävän pieni mahdollisuus, eikä kuulu pohjoismaiseen kulttuuriin mutta toisaalta, sen olemassaolo on hyvä tiedostaa.

5.7.3 Tietoturvaloukkausten havaitseminen ja reagointikyky

Tutkimuksen perusteella kävi ilmi, että monilla ammattiliitoilla, varsinkin pienimmillä, on puutteita kyvyssä havaita ja reagoida tietoturvaloukkauksiin. On täysin mahdollista, että ammattiliitoissa, joissa tietoturvaloukkauksia ei raportoida, kyse ei välttämättä ole loukkausten puuttumisesta, vaan siitä, että ne jäävät havaitsematta. Tämä voi johtua selkeiden toimintatapojen puutteesta tai siitä, että valvontajärjestelmiä ja hälytysmekanismeja ei ole otettu käyttöön.

Vaikka organisaatiot tunnistavat kyberturvallisuuden tärkeyden, havaitsemisen ja reagoinnin prosessit eivät aina ole riittävän selkeitä tai vakiintuneita. Tämä lisää riskiä, että tietoturvapoikkeamat jäävät huomaamatta tai niihin reagoidaan myöhässä, mikä voi johtaa vakavampiin seurauksiin. Havaitsemis- ja reagointikyvyn parantaminen on keskeinen osa tehokasta kyberturvakulttuuria.

Havaitsemisen ja reagoinnin prosessien puute ei ole yllätys vertailtaessa muihin yrityksiin. Vastaavaan havaintoon päätyi myös DNA:n Tietoturvatutkimus 2024. Yli 10 henkilön yrityksistä vain reilulla kolmanneksella (36 %) on ajantasainen kyberturvallisuusstrategia. Sellainen on 250 henkilön yrityksistäkin vain noin puolella. Useammalla yrityksellä on varautumissuunnitelma, mutta niiden määrä jää alle puoleen yrityksistä. 29 % yrityksistä ilmoittaa, ettei heillä ole kyberturvallisuusstrategiaa, eikä varautumis- tai palautumissuunnitelmaa. Nämä yritykset ovat pääsääntöisesti (72 %) pieniä, 10–50 henkilön yrityksiä.

5.7.4 Tiedonhallintakäytännöt ja dokumentaatio

Tutkimuksen tulokset paljastivat, että monilla ammattiliitoilla on puutteita selkeissä käytännöissä arkaluonteisen tiedon käsittelyn osalta. Tämä voi tarkoittaa, että vaikka yleiset tietoturvasäännöt olisivat olemassa, niiden käytännön toteutus jää epäselväksi, mikä lisää riskiä tietoturvaloukkauksiin. Dokumentoidut ja hyvin viestityt prosessit auttavat varmistamaan, että kaikki organisaation jäsenet tietävät tarkasti, miten arkaluonteista tietoa tulisi käsitellä, suojata ja miten poikkeamat ilmoitetaan. Ohjeet tulisi olla aina saatavilla ja päivitettyinä. Myös vastuu dokumenttien ylläpidosta on oltava jollain. Tämän tulisi olla osa laajempaa kyberturvallisuuskulttuuria, jossa tiedonhallinta nähdään yhtenä keskeisenä osatekijänä, ei vain sanana paperilla.

5.7.5 Kulttuurin ja käytännön välinen kuilu

Vaikka ammattiliitot tunnistavat kyberturvallisuuden tärkeyden ja puhuvat aktiivisesti sen merkityksestä, käytännön toteutus ei aina vastaa tavoitteita. Tässä tutkimuksessa havaittiin, että monissa ammattiliitoissa kyberturvakulttuuri ei konkretisoitunut selkeiksi, johdonmukaisiksi käytännöiksi, jotka ohjaisivat arkaluonteisen tiedon suojaamista.

Erityisesti resurssien puute nousi keskeiseksi haasteeksi. Useat ammattiliitot kamppailevat rajallisten taloudellisten ja henkilöstöresurssien kanssa, mikä vaikeuttaa kyberturvallisuuden jalkauttamista käytännön tasolle. Vaikka strategisella tasolla kyberturvallisuus olisikin priorisoitu, konkreettisten toimien to-

teuttaminen jää usein vajaaksi, kun aikaa ja osaavia resursseja ei ole riittävästi. Tämä luo "kulttuurin ja käytännön välisen kuilun", jossa hyvät aikomukset eivät riitä ilman toimivia prosesseja ja selkeitä käytäntöjä.

Tulokset osoittavat, että selkeämmät käytännöt ja systemaattinen jalkauttaminen ovat välttämättömiä, jotta kyberturvakulttuuri voi olla aidosti osa organisaatiokulttuuria. Johdon sitoutuminen ja aktiivinen rooli ovat avainasemassa, sillä ne voivat varmistaa, että tarvittavat resurssit ja tuki ovat käytettävissä. Vasta silloin voidaan rakentaa pohja, jolle toimivat, selkeät ja kestävät käytännöt voidaan perustaa.

5.7.6 Kyberturvallisuuskulttuurin käsite ja sen ymmärtäminen

Tämän tutkimuksen aikana nousi esiin kiinnostava havainto siitä, että vaikka "kyberturvallisuus" terminä tunnetaan, käsitys siitä, mitä "kyberturvallisuuskulttuuri" tarkoittaa, on monille ammattiliitoille epäselvä. Vastaajat tunnistavat, että kyberturvallisuus on tärkeää, mutta eivät aina tiedä, mistä kulttuuriset tekijät – kuten johdon sitoutuminen, jatkuva koulutus, tietoisuuden lisääminen ja selkeät käytännöt – koostuvat tai miten ne toteutuvat käytännössä.

Tämä käsitteellinen epätietoisuus voi vaikuttaa siihen, että ammattiliitot eivät kehitä tai ylläpidä tarvittavia käytäntöjä ja prosesseja, jotka tukisivat kattavan kyberturvakulttuurin syntymistä. Jotta organisaatioiden kyberturvallisuuskulttuuri voisi kehittyä, on tärkeää ensin ymmärtää siihen liittyvät elementit ja toimenpiteet ja miten ne tukevat koko organisaation turvallisuutta. Tämä puute voi johtaa siihen, että yksittäisiä toimenpiteitä toteutetaan, mutta ne eivät muodosta kattavaa ja johdonmukaista kulttuuria, joka suojaisi organisaatiota pitkäjänteisesti. Kyberturvallisuuskulttuurin kehittäminen vaatii tietoista ja kokonaisvaltaista lähestymistapaa, jossa eri tekijät tukevat toisiaan.

6 JOHTOPÄÄTÖKSIÄ TUTKIMUKSEN PERUSTEELLA

Tässä tutkimuksessa tavoitteena oli selvittää, minkälainen kyberturvallisuuskulttuuri ammattiliitoissa vallitsee ja miten kyberturvallisuuskulttuuria voisi kehittää. Tutkimusongelmana oli se, että ammattiliittojen käytössä ei ole kyberturvallisuuskulttuurin yhtenäisiä käytäntöjä eikä koulutusta ja tämä vaikuttaa arkaluonteisen tiedon suojaamiseen. Tutkimuskysymykset olivat seuraavat:

1. Mitä on kyberturvallisuuskulttuuri ja miten sitä kehitetään?
2. Minkälainen kyberturvallisuuskulttuuri ammattiliitoissa on?
3. Mitkä ovat suurimmat esteet ja haasteet kyberturvallisuuskulttuurin kehittämiselle ammattiliitoissa?

Tutkitun teorian pohjalta voidaan todeta, että kyberturvallisuuskulttuuri tarkoittaa organisaation yhteisiä arvoja, asenteita, käyttäytymismalleja ja käytäntöjä, jotka edistävät kyberturvallisuuden toteutumista ja tukevat organisaation toimintaa digitaalisen turvallisuuden näkökulmasta. Kyberturvallisuuskulttuuria voi ja kannattaa arvioida ja kehittää säännöllisesti. Arviointiin ja kehittämiseen on olemassa tutkittuja valmiita malleja, joista organisaatio voi ottaa omaan toimintaan sopivat osat. Säännöllinen arviointi voi paljastaa dominoivan kulttuurin alle piilottamat alakulttuurit, joissa voi piillä riskeille alttiita käyttäytymismalleja ja -tapoja. Kyberturvallisuuskulttuuri vaati pohjalle johdon sitoutumisen sekä työlle varatut resurssit.

Keskeiset elementit, joista kyberturvallisuuskulttuuri rakentuu, ovat seuraavat:

1. **Johdon sitoutuminen:** Kyberturvallisuuskulttuurin rakentaminen alkaa ylimmän johdon vahvasta tuesta. Tämä tarkoittaa kyberturvallisuuden integroimista organisaation strategiaan ja toimintatapoihin. Johdon esimerkki ja resurssointi ovat ratkaisevia kulttuurin juurtumisessa.
2. **Tietoisuus ja koulutus:** Henkilöstön ymmärrys kyberuhkista ja turvallisista toimintatavoista on avainasemassa. Jatkuva koulutus ja valistus tukevat työntekijöiden kykyä tunnistaa ja reagoida uhkiin tehokkaasti.
3. **Prosessit ja politiikat:** Selkeät ohjeet, toimintamallit ja politiikat ohjaavat organisaation jäsenten päivittäistä toimintaa, mikä vähentää virheiden ja haavoittuvuuksien riskiä.
4. **Teknologian hyödyntäminen:** Teknologiset ratkaisut, kuten tietoturvaohjelmistot, monitorointijärjestelmät ja varautumissuunnitelmat, ovat tärkeitä uhkien havaitsemisessa, estämisessä ja hallinnassa.

5. **Jatkuva kehitys:** Kyberturvallisuus ei ole staattinen tila. Organisaatioiden on kyettävä oppimaan menneistä tapahtumista, seuraamaan muuttuviin uhkakuviin liittyvää kehitystä ja päivittämään toimintatapojaan proaktiivisesti.

Ammattiliitoissa otetaan kyberturvallisuus tärkeänä asiana. Johdon sitoutuminen ei ole ongelma, mutta osaamisen ja vastuiden selkeys on puutteellista. Kyberturvallisuus tiedostetaan strategisena painopisteenä, mutta siihen ei resursoida tarpeeksi aikaa tai rahaa ja osaaminen on puutteellista. Kyberturvallisuuden johtaminen ei ole kenenkään vastuulla. Tietoturva- ja tietosuojavastaava on, mutta monesti nämä roolit hoitavat vain pienen siivun kokonaiskyberturvallisuudesta. Kyberturvallisuuskulttuuri sanana on tuntematon. Pääpaino on teknisissä ratkaisuissa ja tietosuojan lakisääteisissä dokumentaatioissa. Pahimmillaan työhöntuloperehdytys vastaa henkilökunnan säännöllisen informoinnin osuuden.

Tutkimuksen tulokset osoittavat, että ammattiliitoissa kyberturvallisuuskulttuurin kehittäminen on moniulotteinen haaste, jossa useat tekijät vaikuttavat onnistumiseen. Vaikka kyberturvallisuus nähdään yleisesti tärkeänä ja siitä puhutaan strategisena prioriteettina, käytännön toteutus ei aina vastaa näitä tavoitteita.

Suurin haaste kyberturvallisuuskulttuurin kehittämisessä ammattiliitoissa on **kyberturvallisuusosaamisen puute**. Monissa organisaatioissa puuttuu riittävä tietotaito ja ymmärrys siitä, miten kyberturvallisuuskäytännöt toteutetaan käytännössä. Tämä johtaa siihen, että vaikka uhkat tunnetaan, niitä vastaan ei välttämättä osata suojautua tehokkaasti. Osaamisen puute estää kyberturvallisuuden jalkautumisen kulttuuriksi, joka voisi suojata organisaatiota laajemmin.

Toiseksi suurin haaste ammattiliitoilla on **ajanpuute**. Organisaatiot tunnistavat kyberturvallisuuden merkityksen, mutta kiire ja päivittäiset tehtävät vievät helposti huomion kyberturvaan liittyviltä toimenpiteiltä. Tämä voi tarkoittaa esimerkiksi sitä, että kyberturvaan liittyvät tehtävät jäävät tekemättä, koulutuksiin ei osallistuta tai uusia käytäntöjä ei ehditä omaksua. Kyberturvallisuuden tulisi kuitenkin olla jatkuva osa organisaation arkea, ei satunnainen toimenpide.

Kolmantena merkittävänä haasteena nousi esiin **resurssien puute**, erityisesti taloudellisten ja henkilöstöresurssien osalta. Useat ammattiliitot kamppailevat rajallisten resurssien kanssa, mikä vaikeuttaa kyberturvallisuuden jalkauttamista käytännön tasolle. Vaikka strategisella tasolla kyberturvallisuus on prioriteetti, konkreettisten toimien toteuttaminen jää usein vajaaksi, koska resursseja ei ole riittävästi tai vastuunjako on epäselvä.

Selkeä vastuunjako osoittautui merkittäväksi tekijäksi onnistuneen kyberturvakulttuurin rakentamisessa. Organisaatioissa, joissa kyberturvavastuut oli selkeästi määritelty, riskienhallinta ja käytännön toimenpiteet olivat paremmin hallinnassa. Tämä viittaa siihen, että johdon aktiivinen sitoutuminen ja vastuiden selkeä määrittely ovat keskeisiä edellytyksiä tehokkaalle kyberturvallisuudelle.

Tietoisuuden lisääminen ja säännöllinen koulutus ovat myös avainasemassa. Tulokset osoittavat, että monissa ammattiliitoissa koulutusta järjestetään satunnaisesti tai ei lainkaan, mikä voi lisätä inhimillisten virheiden riskiä. Jatkuva oppiminen ja henkilöstön sitouttaminen ovat välttämättömiä, jotta kyberturvakulttuuri ei jää pelkästään strategiseksi tavoitteeksi, vaan toteutuu myös käytännössä. Innovatiivisuus ja uudet tavat levittää tietoa perinteisten vaatimuksiin pohjautuvien ohjeiden sijaan ovat avain aitoon vahvaan kyberturvallisuuskulttuuriin. Säännöllisen koulutuksen avulla työntekijä nostetaan vahvaksi tekijäksi varauduttaessa kyberuhkiin.

Yhteenvetona voidaan todeta, että vaikka ammattiliitoissa on vahva ymmärrys kyberturvallisuuden merkityksestä, sen kulttuurin rakentaminen ja jalkauttaminen vaatii vielä merkittäviä kehitysaskelia. Ammattiliitoilla on tämän työn nostamien haasteiden korjaamiseen kuitenkin täydet mahdollisuudet kehittyä jopa kyberturvallisuuskulttuurin esimerkkiorganisaatioiksi. Tulevaisuudessa on tärkeää panostaa pelkän ohjenipun laatimisen sijaan osaamisen ja tietoisuuden innovatiiviseen kasvattamiseen, kyberturvakulttuurin kehittämisestä vastaavan resurssin nimeämiseen, ajankäytön priorisointiin sekä selkeisiin käytäntöihin ja johdon aktiiviseen sitoutumiseen. Näin kyberturvallisuus ei jää vain strategiseksi, paperinmakuiseksi tavoitteeksi, vaan toteutuu konkreettisina tekoina ja toimintatapoina koko organisaatiossa.

Tutkimuksen tavoitteena ollut opas (liite 2) ammattiliitoille saatiin luotua empiirisen ja primääriaineiston perusteella, joten voidaan todeta, että asetettu tutkimustavoite saavutettiin. On kuitenkin huomioitava, että koulutuspaketti ei ole kaikenkattava vaan tehty sillä periaatteella, että sitä voidaan muokata kulloisenkin tarpeen mukaisesti pohjautuen tämän tutkimuksen tuloksiin. Koulutuspaketti tarjoaa konkreettisen työkalun kyberturvallisuuskulttuurin vahvistamiseen. Koulutus lisää henkilöstön osaamista ja tietoisuutta, mutta yksin se ei riitä. Koulutuksen ohella tarvitaan myös selkeitä toimintamalleja, vastuiden nimeämistä ja riittävää resursointia, jotta kyberturvallisuuskulttuuri juurtuu pysyvästi osaksi organisaation toimintaa.

7 POHDINTA

Tutkimuksen empiirisenä aineistona toiminut kyselytutkimus toimi tutkimuksen kannalta hyvin. Vastauksista sai tutkimusta hyvin eteenpäin vieviä tietoja ja vastauksia tutkimuskysymyksiin. Tutkimuksen vastausprosentti jäi ennakko-odotuksia pienemmäksi, jota voidaan pitää vähintään hämmentävänä ja pettymyksenä. Hämmentäväksi vastausprosentin pienuuden tekee kyselytutkimuksen kohdentaminen nimenomaan vain heihin, jotka tehtävänkuvansa perusteella tekevät töitä tietosuojan ja/tai tietoturvan kanssa. Kyselyyn vastaaminen olisi siis ollut oletettavan mielenkiintoinen. Toisaalta vastausprosentti kohdistuksesta huolimatta kertoo kenties myös aiheen toisaalta arkaluonteisuudesta, toisaalta osaamisen puutteesta. Jos vastaaja kokee, ettei osaa aihetta tarpeeksi hyvin tai tehtävä on annettu muun työn ohella hoidettavaksi, voi olla pelko osaamattomuudesta.

Koulutuspaketin laadinta yhtenä opinnäytetyöhön kuuluvana tehtävänä laajensi opinnäytettä kenties tarpeettoman suureksi. Tutkimus ilman koulutuspakettiakin, olisi varmasti ollut kriteerit täyttävä. Yhtä kaikille toimivaa kaiken kattavaa koulutuspakettia ei kenties edes pystyisi kokoamaan, koska koulutus on parasta kohdentaa ja suunnitella vastaanottava yleisö ajatellen. Toisaalta opinnäytetyön yhteydessä laadittava koulutuspaketti on helppo pitää yleisluonteisena, jota voi tarvittaessa muokata kohdeyleisön mukaan ja tutkija voi tulosten perusteella räätälöidä milloin vain eri organisaatioille tarvittavan koulutuspaketin.

7.1 Tutkimuksen luotettavuus

Tehty tutkimus on teknisesti helppo toistaa opinnäytetyön liitteenä olevan (liite 1) kyselylomakkeen pohjalta. Sen avulla voisi arvioida minkä tahansa yhteisön kyberturvallisuuskulttuuria ja sitä haastavia tekijöitä. Tutkimustulokset ovat laajennettavissa kaikentyyppisten pienten tai keskisuurten organisaatioiden kyberturvallisuuskulttuuriin. Ammattiliittokonteksti ei sulje pois tai rajaa laajennettavuutta ns. tavalliseen organisaatioon, mutta se tuo laajempaa käsitystä siitä, miten kyberturvallisuus vaikuttaa organisaation tietojen suojaukseen sen käsitellessä arkaluonteisia tietoja. Tutkimuksen tulokset ovat käyttökelpoisia varsinkin ammattiliitoille huolimatta siitä, mihin keskusjärjestöön ne kuuluvat. Vastaavia organisaatiota voi olla esimerkiksi uskonnolliset tai poliittiset yhteisöt, joiden jäsentiedot ovat yhtä lailla arkaluonteisiksi luokiteltavia. Tutkimuksen tulokset ovat hyödynnettävissä myös tutkittaessa yleisesti kyberturvallisuutta, tietoturvaa tai kyberturvallisuuskulttuuria ja näiden kehittämistä.

On kuitenkin huomattava, että vastaava kyselytutkimus kertoo vain sen hetkisen tilanteen ja kyselyyn osallistuneiden ihmisten tiedon. Kysely ei kerro ihmisten käyttäytymistä tai sitä, vastaako eri ihminen täysin samalla tavalla kuin tämän kyselytutkimuksen vastaajat. Tai vastaisiko sama ihminen samalla tavalla eri ajankohtana. Vastaajan tietotasoon vaikuttaa aina myös organisaation omat ohjeet ja arvot.

Reliabiliteetin eli saatujen tutkimustulosten pysyvyyttä on ihmisen käyttäytymistä arvioivassa laadullisessa tutkimuksessa lähes mahdoton arvioida ja saavuttaa. Kyselytutkimus kertoi vain sen hetkisen tilan. Jos vastaava kysely suoritettaisi nyt, tulokset voisivat olla erilaiset johtuen esimerkiksi kyselyjen välillä tehdyistä toimenpiteistä. Tämä oli tiedossa jo tutkimuksen alussa ja tarkoituksena olikin selvittää sen hetkinen tila ammattiliitoissa. Kuten tutkimuksessa todettu, kyberturvallisuus on tila, joka kehittyy ja jota pitää kehittää jatkuvasti.

Validiteetin eli oikeiden asioiden tutkimisen todentamisessa tutkijan valinnat mm. kyselytutkimuksen kysymyksiksi pohjautuvat teoriaan ja tutkijan tietämykseen aiheesta ja ammattiliitoista. Tutkimuksen kohderyhmä on aiemmin tode-

tun mukaisesti tutkimuksen kannalta erittäin validi. Tutkijan esittämät johtopäätökset on perusteltu vain selkeiden tulosten pohjalta eikä tutkimuksen tuloksissa ilmennyt epäselvyyksiä tai asioita, jotka olisivat kyseenalaisia.

Sekundäärinen aineisto tuki tutkimuksen tulosten analysointia. Teoriaa kyberturvallisuudesta on saatavilla paljon, niin kansallisia kuin kansainvälisiä, samoin vuosittaisia tutkimuksia kyberturvallisuuden tilasta. Verrattuna tuloksia teoriaan, ei tullut suuria yllätyksiä. Kuitenkin, parhaat käytännöt, joita teoriassa on paljon liittyen kyberturvallisuuskulttuuriin, ei juurikaan vielä näy ammattiliittokontekstissa. Havainto toisaalta osoitti paikan juuri tämän tutkimuksen tarpeellisuudesta.

Tämä tutkimus toi uutta tietoa ammattiliittojen kyberturvallisuuskulttuurista, joka on aiemmin ollut tutkimuskohteena hyvin vähän esillä. Tutkimuksen tulokset osoittavat, että kyberturvallisuuskulttuurin kehittäminen ammattiliitoissa edellyttää siirtymistä sanoista tekoihin. Tämä työ tarjoaa konkreettisia ratkaisuja aiemmin tunnistamattomiin haasteisiin ja täydentää siten merkittävällä tavalla aiempaa tutkimustietoa organisaatiokulttuurin ja kyberturvallisuuden rajapinnassa.

7.2 Jatkokehitysideat

Tämän tutkimuksen tarkoituksena ei ollut kyberturvallisuuskulttuurin kehittymisen seuranta. Olisi varsin mielenkiintoista jatkotutkimuksena seurata miten erilaiset toimet, kuten tämänkin tutkimuksen tulosten toimeenpano, vaikuttaa kyberturvallisuuskulttuurin kehittymiselle.

Tämän tutkimuksen tarkoituksena ei myöskään ollut kyberturvan hallintamallin tai kyberturvan riskienhallintamallin tarkkaa rakentamista yleispätevästi mihinkään organisaatioon, edes ammattiliitoille. Kuitenkin tutkimus osoitti näiden tärkeyden, joten voisi olla mielenkiintoinen jatkotutkimus validoida ja osoittaa paras kyberturvallisuuden hallintamalli tai kyberturvallisuusriskien hallintamalli ammattiliitoille. Kärjistetysti plug and play -tyyppinen hallintamalli, joka auttaisi pieniä organisaatiota kyberturvan maturiteetin nostoon.

Tutkimuksen teon yhteydessä vastaan tullut tutkimus kulttuurillisten tekijöiden vaikutuksesta tietoturvaohjeiden noudattamisessa jäi mieleen. Löydetty tutkimus osoitti vahvasti mm. häpeän ja sanktioiden toimivan Afrikassa ISP:n noudattamiseen. Olisi varsin mielenkiintoista toteuttaa vastaava tutkimus pohjoismaisessa tai suomalaisessa organisaatiossa – toimisivatko samat vaikuttimet?

LÄHTEET

Alshaikh, M. 2020. Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security 98. Elsevier Ltd. WWW-dokumentti. Saatavissa: https://doi.org/10.1016/j.cose.2020.102003 [viitattu 31.1.2025].

Andreasson, A. & Ylipartanen, A. 2022. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR). 2. päivitetty laitos. Helsinki: Tietosanoma.

Bada, M., Furnell, S., Nurse, J. & Uchendu, B. 2021. Developing a Cyber Security Culture: Current Practices and Future Needs. Computers & Security 109. WWW-dokumentti. Saatavissa: https://doi.org/10.1016/j.cose.2021.102387 [viitattu 12.11.2024].

Boehm, J, Curcio, N., Merrath, P., Shenton, L. & Stähle, T. 2019. The risk-based approach to cybersecurity. McKinsey & Company. PDF-dokumentti. Saatavissa: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20risk%20based%20approach%20to%20cybersecurity/The-risk-based-approach-to-cybersecurity.pdf [viitattu 12.11.2024].

Change Partners Finland Oy s.a. Prosci ADKAR-malli. WWW-dokumentti. Saatavissa: https://changepartners.fi/adkar/ [viitattu 30.1.2025].

CrowdStrike. 2024. 2024 Global treath report. PDF-dokumentti. Saatavissa: https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf [viitattu 11.11.2024].

CrowdStrike. 2025. 2025 Global treath report. PDF-dokumentti. Saatavissa: https://www.crowdstrike.com/explore/2025-global-threat-report [viitattu 28.2.2025].

Da Veiga, A. 2018. An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. Information & Computer Security Vol. 26 No. 5 Emerald Publishing Limited, 584-612. WWW-dokumentti. Saatavissa: http://dx.doi.org/10.1108/ICS-08-2017-0056 [viitattu 30.1.2025].

Da Veiga, A. 2019. Achieving a Security Culture. Cybersecurity Education for Awareness and Compliance, 72-100. E-kirja. Saatavissa: https://uir.unisa.ac.za/bitstream/handle/10500/26783/Chapter%205%20-%20da%20Veiga.pdf [viitattu 17.12.2024].

Da Veiga, A. 2023. A model for information security culture with creativity and innovation as enablers – refined with an expert panel. Information and Computer Security Vol. 31 No. 3. Emerald Publishing Limited, 281-303. WWW-dokumentti. Saatavissa: http://dx.doi.org/10.1108/ICS-11-2022-0178 [viitattu 17.12.2024].

Da Veiga, A., Astakhova, L., Botha, A. & Herselman, M. 2020. Defining organizational information security culture – Perspectives from academia and indus-

try. Computers & Security vol. 92. Elsevier Ltd. WWW-dokumentti. Saatavissa: https://www-sciencedirect-com.ezproxy.xamk.fi/science/article/pii/S0167404820300018/pdfft?md5=ce46b3b8124eab0913f8f81dd1dc48d8&pid=1-s2.0-S0167404820300018-main.pdf [viitattu 18.12.2024].

Da Veiga, A. & Eloff, J. 2010. A framework and assessment instrument for information security culture. Computers & Security vol. 2. Elsevier Ltd., 196–207. WWW-dokumentti. Saatavissa: https://www-sciencedirect-com.ezproxy.xamk.fi/science/article/pii/S0167404809000923 [viitattu 28.1.2025].

Da Veiga, A. & Martins, N. 2017. Defining and identifying dominant information security cultures and subcultures. Computers & Security vol. 70. Elsevier Ltd., 72–94. WWW-dokumentti. Saatavissa: https://www-sciencedirect-com.ezproxy.xamk.fi/science/article/pii/S0167404817300937 [viitattu 28.1.2025].

DNA. 2024. Tietoturvatutkimus 2024 - Miltä kyberturvallisuuden kenttä näyttää suomalaisyritysten silmin? PDF-dokumentti. Saatavissa: https://uutiskirje.dna.fi/res/sibbe/DNA_Tietoturvatutkimus2024_raportti_FINAL.pdf [viitattu 7.11.2024].

Ejigu, K., Siponen, M. & Arage, T. 2021. Investigating the Impact of Organizational Culture on Information Security Policy Compliance: The Case of Ethiopia. *AMCIS 2021 Proceedings* 10. WWW-dokumentti. Saatavissa: https://aisel.aisnet.org/amcis2021/info_security/info_security/10 [viitattu 13.11.2024].

ENISA. 2017. Cyber Security Culture in organizations. E-kirja. Saatavissa: https://doi.org/10.2824/10543 [viitattu 18.12.2024].

ENISA. 2021. Cybersecurity for smes. Challenges and Recommendations. E-kirja. Saatavissa: https://doi.org/10.2824/770352 [viitattu 31.1.2025].

EUR-Lex. 2022. Yleinen tietosuoja-asetus (GDPR). European Union. WWW-dokumentti. Päivitetty 7.1.2022. Saatavissa: https://eur-lex.europa.eu/FI/legal-content/summary/general-data-protection-regulation-gdpr.html [viitattu 29.10.2024].

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679

Fortinet. 2024. Man-in-the-Middle Attack: Types and Examples. WWW-dokumentti. Saatavissa: https://www.fortinet.com/resources/cyberglossary/man-in-the-middle-attack [viitattu 29.10.2024].

F-Secure. 2022a. Mikä on palvelunestohyökkäys (DDoS)? WWW-dokumentti. Julkaistu 21.7.2022. Saatavissa: https://www.f-secure.com/fi/articles/what-is-ddos [viitattu 29.10.2024].

F-Secure. 2022b. Mikä on haittaohjelma? Näin pysyt turvassa vaarallisilta ohjelmilta. WWW-dokumentti. Julkaistu 18.2.2022. Saatavissa: https://www.f-secure.com/fi/articles/what-is-malware [viitattu 24.3.2025].

F-Secure. 2022c. Mitä on tietojenkalastelu eli phishing? Näin verkkourkinta toimii. WWW-dokumentti. Julkaistu 28.10.2022. Saatavissa: https://www.f-secure.com/fi/articles/what-is-phishing [viitattu 29.10.2024].

Heikkinen, H. (toim.) & Kaukko, M. (toim.). 2023. Toimintatutkimus – Käytännön opas. 1. painos. Tampere: Vastapaino. E-kirja. Saatavissa: https://www.ellibslibrary.com/jyu/9789523971035 [viitattu 3.9.2024].

Hoffmann, R., Napiórkowski, J., Protasowicki, T. & Stanik, J. 2020. Risk based approach in scope of cybersecurity threats and requirements. WWW-dokumentti. Teoksessa Lagaros, N., Abdalla, K., Marano, G., Phocas, M. & Rousan, R. (toim.) Procedia Manufacturing. Elsevier B.V., 655–662. Saatavissa: https://doi.org/10.1016/j.promfg.2020.02.243 [viitattu 12.11.2024].

Juutilainen, A. 2022. Johda ajattelua, johda työturvallisuutta. Jyväskylä: Santalahti-kustannus.

Järvinen, P. 2018. Kyberuhkia ja somesotaa. Jyväskylä: Docendo Oy.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä. Jyväskylän ammattikorkeakoulu. Jyväskylän ammattikorkeakoulun julkaisuja -sarja.

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona – opas opinnäytetyön ja pro gradun kirjoittajalle. Jyväskylän ammattikorkeakoulu. Jyväskylän ammattikorkeakoulun julkaisuja -sarja.

Kastepohja, J. 2020. Kyberturvallisuuskulttuuri – ohjelmistoyritys Reaktorin ratkaisuja henkilöstön kautta kohdistuvien kyberuhkien vähentämiseksi. Pro gradu -tutkielma. Jyväskylän yliopisto. Informaatioteknologian tiedekunta. PDF-dokumentti. Saatavissa: https://jyx.jyu.fi/bitstream/handle/123456789/71175/URN%3ANBN%3Afi%3Ajyu-202007155332.pdf?sequence=1&isAllowed=y [viitattu 19.1.2024].

Kyberturvallisuuskeskus. 2023. Tietojenkalastelu- ja huijausviestien kanssa tulee olla yhä tarkempi. WWW-dokumentti. Julkaistu 21.6.2023. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tietojenkalastelu-ja-huijausviestien-kanssa-tulee-olla-yha-tarkempi [viitattu 29.10.2024].

Kyberturvallisuuskeskus. 2024a. Mikä ihmeen kiristyshaittaohjelma? WWW-dokumentti. Julkaistu 15.8.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/mika-ihmeen-kiristyshaittaohjelma [viitattu 28.10.2024].

Kyberturvallisuuskeskus. 2024b. Tietoturvan vuosi 2023 - Kyberturvallisuuskeskuksen vuosikatsaus. Traficomin julkaisuja 10/2024. WWW-dokumentti. Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_Tietoturvan-vuosi-2023_web.pdf [viitattu 20.9.2024].

Kyberturvallisuuskeskus. 2025. Kyberturvallisuuden vuosi 2024. WWW-dokumentti. Saatavissa: https://vuosiraportit.traficom.fi/fi/kyberturvallisuus/kyberturvallisuuden-vuosi-2024 [viitattu 24.3.2025].

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.

Lugo, R. 2023. Editorial: The human factor in cyber security education. Frontiers in Education. WWW-dokumentti. Saatavissa: https://doi.org/10.3389/feduc.2023.1277282 [viitattu 20.2.2025].

Luukka, P. 2019. Yrityskulttuuri on kuningas – Mikä, miksi ja miten? 4. painos. Helsinki: Alma Insights.

McAfee. 2024. Mikä on haittaohjelma? WWW-dokumentti. Saatavissa: https://www.mcafee.com/fi-fi/antivirus/malware.html [viitattu 29.20.2024].

Paananen, R., Soikkeli, M., Starck, M., Aro, M., Kuusisto, T., Rusila, T. & Tuulensuu, T. 2024. Suomen kyberturvallisuusstrategia 2024–2035. Valtioneuvoston kanslian julkaisuja 2024:11. Helsinki: Valtioneuvoston kanslia. E-kirja. Saatavissa: https://urn.fi/URN:ISBN:978-952-383-376-0

Pernaa, J. 2013. Kehittämistutkimus tutkimusmenetelmänä. Teoksessa Pernaa, J. (toim.) Kehittämistutkimus opetusalalla. Jyväskylä: PS-kustannus, 9–26. E-kirja. Saatavissa: http://hdl.handle.net/10138/317958 [viitattu 4.9.2024].

Perustuslaki 11.6.1999/731.

Rikoslaki 19.12.1889/39.

Rousku, K. 2014. Kyberturvaopas – Tietoturvaa kotona ja työpaikoilla. Helsinki: Alma Insights.

Savolainen, M. 2022. ”Kaikki tietää, että se on semmoinen villi länsi tuo netti vielä” – Narratiivinen tutkimus kyberturvallisuuskulttuurista kaupungin hallinto-organisaatiossa. Lapin yliopisto. Yhteiskuntatieteiden tiedekunta. Pro gradu -tutkielma. PDF-dokumentti. Saatavissa: https://lauda.ulapland.fi/bitstream/handle/10024/65231/Savolainen_Markus.pdf [viitattu 20.12.2024].

Saxena, N., Hayes, E., Bertino, E., Ojo, P., & Choo, K-K. 2020. Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics 2020* 9 1460. WWW-dokumentti. Saatavissa: https://doi.org/10.3390/electronics9091460 [viitattu 13.11.2024].

Sevgi, H. 2021. The perspective of labor unions on cybersecurity: The case of Turkey. Teoksessa Skrijelj, R. & Duzgun, E. (toim.) Academic Studies in Humanities and Social Sciences. Lyon: Livre de Lyon, 75–96. E-kirja. Saatavissa: https://books.google.fi/books?id=UOOSEAAAQBAJ&lpg=PA75&ots=PCb_p3Lecz&dq=cyber%20security%20culture%20in%20labour%20unions&lr&hl=fi&pg=PA75#v=twopage&q=cyber%20security%20culture%20in%20labour%20unions&f=true [viitattu 11.11.2024].

Sutton, A., Tompson, L. 2024. Towards a cybersecurity culture-behavior framework: A rapid evidence review. Computers & Security

Volume 148. Elsevier Ltd. WWW-dokumentti. Saatavissa: https://doi.org/10.1016/j.cose.2024.104110 [viitattu 30.1.2025].

Teperi, A-M. 2023. Ihminen turvallisuuden tekijänä. Helsinki: Gaudeamus.

Tietosuojalaki 5.12.2018/1050.

Tietosuojavaltuutetun toimisto. 2024a. Erityisten henkilötietoryhmien käsittely. 2024. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely [viitattu 16.9.2024].

Tietosuojavaltuutetun toimisto. 2024b. Tietosuojalaki. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/tietosuojalaki [viitattu 29.10.2024].

Tietosuojavaltuutetun toimisto. 2024c. Tietoturvaloukkaukset. WWW-dokumentti. Saatavissa: https://tietosuoja.fi/tietoturvaloukkaukset [viitattu 16.9.2024].

Tolah, A., Furnell, S. & Papadaki, M. 2017. A Comprehensive Framework for Cultivating and Assessing Information Security Culture. PDF-dokumentti. Saatavissa: https://www.researchgate.net/profile/Alaa-Tolah/publication/334307233_A_Comprehensive_Framework_for_Cultivating_and_Assessing_Information_Security_Culture/links/5d238055458515c11c1f2b67/A-Comprehensive-Framework-for-Cultivating-and-Assessing-Information-Security-Culture.pdf [viitattu 13.3.2025].

Tolah, A., Furnell, S. & Papadaki, M. 2021. An empirical analysis of the information security culture key factors framework. Computers & Security vol. 108. Elsevier Ltd. WWW-dokumentti. Saatavissa: https://www-sciencedirect-com.ezproxy.xamk.fi/science/article/pii/S0167404821001784 [viitattu 18.12.2024].

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. PDF-dokumentti. Saatavissa: https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf [viitattu 22.1.2024].

Uchendu, B., Nurse, J., Bada, M. & Furnell, S. 2021. Developing a cyber security culture: Current practices and future needs. Computer & Security vol. 109. Elsevier Ltd. WWW-dokumentti. Saatavissa: https://www-sciencedirect-com.ezproxy.xamk.fi/science/article/pii/S016740482100211X [viitattu 28.1.2025].

Verizone. 2022. 2022 Data Breach Investigations Report. PDF-dokumentti. Saatavissa: https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf [viitattu13.11.2024].

Verizone. 2023. 2023 Data Breach Investigations Report. PDF-dokumentti. Saatavissa: https://www.verizon.com/business/en-gb/resources/2023-data-breach-investigations-report-dbir.pdf [viitattu13.11.2024].

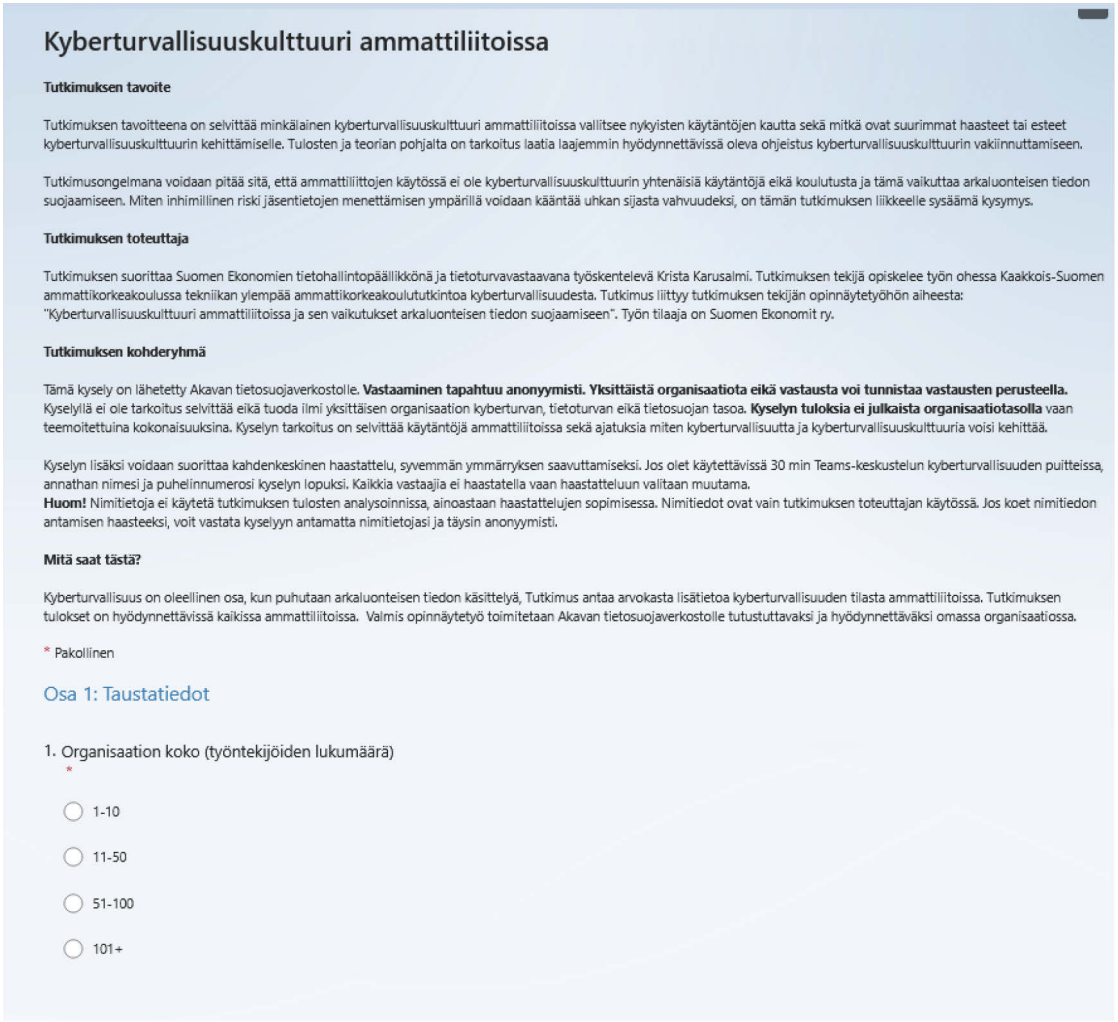
Verizone. 2024. 2024 Data Breach Investigations Report. PDF-dokumentti. Saatavissa: https://www.verizon.com/business/resources/T16e/reports/2024-dbir-data-breach-investigations-report.pdf [viitattu 13.11.2024].

Yhdistyslaki 26.5.1989/503.

Zieniūtė, U. 2022. Mikä on brute force -hyökkäys eli väsytyshyökkäys? NordVPN. Blogi. Julkaistu 7.6.2022. Saatavissa: https://nordvpn.com/fi/blog/vasytyshyokkays/ [viitattu 29.10.2024].

Zieniūtė, U. 2024. Mikä on man-in-the-middle-hyökkäys eli väliintulohyökkäys? Blogi. Julkaistu 21.2.2024. Saatavissa: https://nordvpn.com/fi/blog/vasytyshyokkays/ [viitattu 29.10.2024].

KYSELYTUTKIMUS AMMATTILIITOILLE



Kyberturvallisuuskulttuuri ammattiliitoissa

Tutkimuksen tavoite

Tutkimuksen tavoitteena on selvittää minkälainen kyberturvallisuuskulttuuri ammattiliitoissa valiitsee nykyisten käytäntöjen kautta sekä mitkä ovat suurimmat haasteet tai esteet kyberturvallisuuskulttuurin kehittämiselle. Tulosten ja teorian pohjalta on tarkoitus laatia laajemmin hyödynnettävissä oleva ohjeistus kyberturvallisuuskulttuurin vakiinnuttamiseen.

Tutkimusongelmana voidaan pitää sitä, että ammattiliittojen käytössä ei ole kyberturvallisuuskulttuurin yhtenäisiä käytäntöjä eikä koulutusta ja tämä vaikuttaa arkaluonteisen tiedon suojaamiseen. Miten inhimillinen riski jäsentietojen menettämisen ympärillä voidaan kääntää uhkan sijasta vahvuudeksi, on tämän tutkimuksen liikkeelle sysäämä kysymys.

Tutkimuksen toteuttaja

Tutkimuksen suorittaa Suomen Ekonomien tietohallintopäällikkönä ja tietoturvavastaavana työskentelevä Krista Karusalmi. Tutkimuksen tekijä opiskelee työn ohessa Kaakkois-Suomen ammattikorkeakoulussa tekniikan ylempää ammattikorkeakoulututkintoa kyberturvallisuudesta. Tutkimus liittyy tutkimuksen tekijän opinnäytetyöhön aiheesta: "Kyberturvallisuuskulttuuri ammattiliitoissa ja sen vaikutukset arkaluonteisen tiedon suojaamiseen". Työn tilaaja on Suomen Ekonomit ry.

Tutkimuksen kohderyhmä

Tämä kysely on lähetetty Akavan tietosuojaverkostolle. **Vastaaminen tapahtuu anonyymisti. Yksittäistä organisaatiota eikä vastausta voi tunnistaa vastausten perusteella.** Kyselyllä ei ole tarkoitus selvittää eikä tuoda ilmi yksittäisen organisaation kyberturvan, tietoturvan eikä tietosuojan tasoa. **Kyselyn tuloksia ei julkaista organisaatiotasolla** vaan teemoitettuina kokonaisuuksina. Kyselyn tarkoitus on selvittää käytäntöjä ammattiliitoissa sekä ajatuksia miten kyberturvallisuutta ja kyberturvallisuuskulttuuria voisi kehittää.

Kyselyn lisäksi voidaan suorittaa kahdenkeskinen haastattelu, syvemmän ymmärryksen saavuttamiseksi. Jos olet käytettävissä 30 min Teams-keskustelun kyberturvallisuuden puitteissa, annathan nimesi ja puhelinnumerosi kyselyn lopuksi. Kaikkia vastaajia ei haastatella vaan haastatteluun valitaan muutama.
Huom! Nimitietoja ei käytetä tutkimuksen tulosten analysoinnissa, ainoastaan haastattelujen sopimisessa. Nimitiedot ovat vain tutkimuksen toteuttajan käytössä. Jos koet nimitiedon antamisen haasteeksi, voit vastata kyselyyn antamatta nimitietojasi ja täysin anonyymisti.

Mitä saat tästä?

Kyberturvallisuus on oleellinen osa, kun puhutaan arkaluonteisen tiedon käsittelyä, Tutkimus antaa arvokasta lisätietoa kyberturvallisuuden tilasta ammattiliitoissa. Tutkimuksen tulokset on hyödynnettävissä kaikissa ammattiliitoissa. Valmis opinnäytetyö toimitetaan Akavan tietosuojaverkostolle tutustuttavaksi ja hyödynnettäväksi omassa organisaatiossa.

* Pakollinen

Osa 1: Taustatiedot

1. Organisaation koko (työntekijöiden lukumäärä)
*

- ○ 1-10
- ○ 11-50
- ○ 51-100
- ○ 101+

2. Onko organisaatiolla nimettynä tietoturva ja/tai tietosuojavastaavat. Voit valita useita.
*

- ☐ Tietoturvavastaava
- ☐ Tietosuojavastaava
- ☐ Rooli on yhdistetty eli toimii sekä tietoturvavastaavana että tietosuojavastaavana
- ☐ Meillä ei ole mitään yllä olevista

3. Onko yllä mainitut roolit organisaationne omia täyntekijöitä vai onko roolit ulkoistettu (eli ostetaan palveluna)?
*

- ○ Organisaation omia työntekijöitä
- ○ Ostamme palveluna eli ulkoistettuna
- ○ Sekä omia että ulkoistettuna

Seuraava

Sivu 1/7

Osa 2: Kyberturvallisuuskulttuuri

Tässä osiossa kysytään useita kysymyksiä koskien koko henkilökuntaa. Anna vastauksesi sen mukaan mitä olet henkilökohtaisesti havainnut.

4. **Kuinka tärkeänä organisaationne johto pitää kyberturvallisuutta?** *

1–5 (1 = ei lainkaan tärkeää, 5 = erittäin tärkeää)

1 Ei lainkaan tärkeä	2 Jonkin verran tärkeä	3 Neutraali	4 Tärkeä	5 Erittäin tärkeä
○	○	○	○	○

5. **Miten hyvin mielestäsi henkilöstö noudattaa tietoturvakäytäntöjä, kuten vahvojen salasanojen käyttöä ja monivaiheista tunnistautumista?** Vastaa se mukaa mitä tiedät tai olet havainnut.
*

1–5 (1 = ei lainkaan, 5 = erittäin hyvin)

1 Ei lainkaan	2 Jonkin verran	3 Neutraali	4 Hyvin	5 Erittäin hyvin
○	○	○	○	○

6. **Kuinka hyvin mielestäsi henkilöstö on tietoinen kyberuhista, kuten tietojenkalastelusta ja haittaohjelmista?** Vastaa se mukaa mitä tiedät tai olet havainnut.
*

1–5 (1 = ei lainkaan tietoinen, 5 = erittäin tietoinen)

1 Ei lainkaan tietoinen	2 Jonkin verran tietoinen	3 Neutraali	4 Tietoinen	5 Erittäin tietoinen
○	○	○	○	○

7. **Onko mielestäsi henkilöstöllä tarvittava tieto siitä, miten toimia tietoturva- tai tietosuojaloukkauksen sattuessa?** Vastaa se mukaa mitä tiedät tai olet havainnut.
*

- ○ Kyllä
- ○ Osittain
- ○ Ei

8. **Miten henkilöstö suhtautuu kyberturvallisuuskäytäntöihin ja niiden noudattamiseen?** *

- ○ Positiivisesti ja sitoutuneesti
- ○ Neutraali suhtautuminen
- ○ Negatiivinen suhtautuminen / vastustaminen

9. **Miten arvioisit henkilöstön asenteita ja motivaatiota kyberturvallisuuskäytäntöjen noudattamisessa?** *

Valitse vastauksesi

10. **Onko organisaatiossanne selkeä roolitus ja vastuunjako kyberturvallisuuden osalta?** *

Valitse vastauksesi

11. **Kuinka paljon aikaa käytetään kyberturvallisuuteen liittyvien tehtävien toteuttamiseen organisaatiossanne?**

- ○ Riittävästi
- ○ Liian vähän
- ○ En osaa sanoa

12. **Mitä konkreettisia vaikeuksia olet huomannut kyberturvallisuuskulttuurin jalkauttamisessa?** *
Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

13. **Onko organisaationne kyberturvallisuuden nykykäytännöissä jotain selkeitä puutteita?** *
Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

14. **Miten arvioisit organisaationne kyberturvallisuuskulttuurin tasoa?** Pohdi tässä niin teknisten kuin hallinnollisten käytänteiden kuin johdon ja henkilökunnan tietoisuutta, tapaa toimia ja asennetta kyberturvallisuusasioissa. Toisin sanoen koko kyberturvallisuuskulttuurin tasoa. *
Vastaa alla oleviin kysymyksiin asteikolla 1 = erittäin heikko, 5 = erittäin vahva.

	1 Erittäin heikko	2 Heikko	3 Neutraali	4 Vahva	5 Erittäin vahva
	○	○	○	○	○

Edellinen Seuraava Sivu 2/7

Osa 3: Kyberturvallisuustietoisuuden kasvattaminen

15. **Miten organisaatiossanne kasvatetaan henkilöstön tietoisuutta kyberturvallisuudesta?** *
Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

16. **Mitä menetelmiä käytätte kyberturvallisuustietoisuuden lisäämiseksi?** *
Voit valita useita vaihtoehtoja. Jos vastaat vain Muu, annathan pienen kuvauksen.

- ☐ Säännölliset koulutukset
- ☐ Verkkokoulutuksia
- ☐ Tiedotuskampanjoita (esim sähköposti tai Teams)
- ☐ Tietoturva ja tietosuojatestejä
- ☐ Ei mitään käytössä
- ☐ Muu

17. **Kuinka usein järjestätte koulutuksia (live-osallistuminen tai esim Teams) kyberturvallisuustietoisuuden lisäämiseksi?** *
Vastaa jos organisaatiossanne järjestetään tietoturva- tai tietosuojakoulutuksia

Valitse vastauksesi

18. **Onko teillä käytössä verkkokoulutuksia kyberturvallisuustietoisuuden lisäämiseksi?** *
Vastaa sen perusteella, onko teillä laadittuna tietoturva- tai tietosuojakoulutuksia, joita henkilökunta voi katsoa/kuunnella oman aikataulun mukaisesti.

- ○ On käytössä verkkokoulutuksia
- ○ Ei ole verkkokoulutuksia

19. **Kuinka usein tiedotatte henkilökuntaa kyberturvallisuus-asioista (esim sähköpostitse tai Teamsilla)?** *

Vastaa, jos organisaatiossanne järjestetään tietoturva- tai tietosuojaviestintää

Valitse vastauksesi

20. **Kuinka usein järjestätte tietoturvatestejä kyberturvallisuustietoisuuden lisäämiseksi?** *

Vastaa jos organisaatiossanne tehdään henkilökunnan tietoturva- tai tietosuojatestejä.

Valitse vastauksesi

Edellinen Seuraava Sivu 3/7

Osa 3: Esteet ja haasteet kyberturvallisuuskulttuurin kehittämisessä

21. **Mikä on suurin haaste kyberturvallisuuskulttuurin kehittämisessä organisaatiossanne?** *

(Valitse suurin haaste, seuraavassa kysymyksessä voit valita useampia haasteita)

Valitse vastauksesi

22. **Mitkä ovat muut haasteet kyberturvallisuuskulttuurin kehittämisessä organisaatiossanne?** *

Tässä voit valita havaitsemiasi muita haasteita. Voit valita useita vaihtoehtoja. Jos vastaata vain Muu, annathan pienen kuvauksen.

Ethän valitse tässä samaa, minkä valitsit edellisessä kysymyksessä tärkeimmäksi haasteeksi.

- [ ] Johdon sitoutumisen puute
- [ ] Ei ole kenenkään vastuulla / osoittaa resurssia
- [ ] Ohjeistuksen ja koulutusmateriaalin puute
- [ ] Kyberturvallisuus-osaamisen puute
- [ ] Vähäinen kyberuhkien ymmärrys
- [ ] Henkilökunnan Vastarinta tietoturva- ja tietosuoja-asioissa
- [ ] Taloudelliset tekijät
- [ ] Teknologiset rajoitteet
- [ ] Ajanpuute / kiire
- [ ] Kiinnostuksen puute
- [ ] Laiskuus
- [ ] Muu

23. **Jos valitsit yhdeksi haasteeksi Muu, kuvailisitko hieman tarkemmin mitä haasteella tai haasteilla tarkoitat?**

Kirjoita vastaus

24. **Mitkä ovat suurimmat uhkat kyberturvallisuuden kehittämiselle organisaatiossanne?** *

Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

25. **Miten johdon sitoutuminen kyberturvallisuuteen näkyy organisaatiossanne?** *

Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

26. **Kuinka hyvin organisaatiossanne on varauduttu tietoturva- ja tietosuojaloukkauksiin?** *

1–5 (1 = erittäin huonosti, 5 = erittäin hyvin)

1 Erittäin huonosti	2 Huonosti	3 Neutraali	4 Hyvin	5 Erittäin hyvin
○	○	○	○	○

27. **Onko organisaatiossanne ollut tietoturvaloukkauksia (sisältäen tietosuojaloukkaukset) viimeisen kahden vuoden aikana?** *

- ○ Kyllä
- ○ Ei
- ○ En tiedä

Osa 4: Tietoturvariskien hallinta ja tietosuojakäytännöt

28. **Onko organisaatiossanne käytössä virallinen tietoturvariskien hallintasuunnitelma?** *

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

29. **Kuinka usein organisaatiossanne tehdään tietoturvariskien arviointeja?** *

Valitse vastauksesi

30. **Onko käytössä selkeitä käytäntöjä arkaluonteisten tietojen suojaamiseksi?** *

- ◯ Kyllä
- ◯ Ei
- ◯ En tiedä

31. **Kuinka hyvin henkilöstö tuntee tietosuojalainsäädännön (esim. GDPR) vaatimukset työssään?** *

1–5 (1 = erittäin huonosti, 5 = erittäin hyvin)

	1 Erittäin huonosto	2 Huonosti	Neutraali	4 Hyvin	5 Erittäin hyvin
	◯	◯	◯	◯	◯

32. **Onko tietosuoja otettu huomioon organisaation kaikissa toiminnoissa (esim. tietojen kerääminen, tallentaminen ja käsittely)?** *

Valitse vastauksesi

Osa 5: Lopuksi, parannusehdotukset ja avoin palaute

33. **Mitä parannuksia toivoisit kyberturvallisuuskulttuurin edistämiseksi organisaatiossanne?** Pohdi tässä nimenomaan kulttuuria. Seuraavassa kysymyksessä voit pureutua kyberturvallisuuden kehittämiseen.
*

Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

34. **Miten organisaationne voisi parhaiten kehittää kyberturvallisuutta tulevaisuudessa?** *

Kirjoita omin sanoin ja oman tietämyksesi mukaan. Vastauksella ei ole merkkimäärärajoitetta.

Kirjoita vastaus

35. **Haluatko sanoa vielä jotain muuta liittyen kyberturvallisuuteen ja sen kehittämiseen joko organisaatiossanne tai yleisesti?**

Vapaaehtoinen

Kirjoita vastaus

Edellinen Seuraava Sivu 6/7

Osa 6: Mahdolliseen jatkohaastatteluun osallistuminen

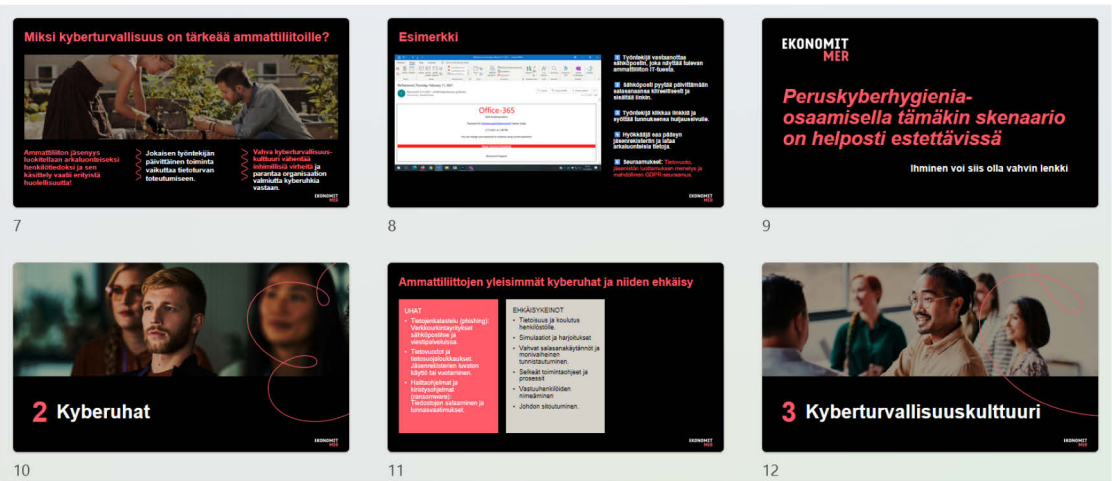
36. Oletko käytettävissä mahdolliseen vapaaehtoiseen jatkohaastatteluun samasta aiheesta? Haatattelun kesto 30 min ja haastattelu suoritetaan teamsin välityksellä.
*

Kaikkia vastaajia ei haastatella vaan tutkimukseen poimitaan tarvittaessa muutama yksittäinen haastateltava. Haastattelun suoritetaan tämän tutkimuksen tulosten valmistuttua, arviolta loka-marraskuussa 2024.

- ○ Kyllä
- ○ En

Edellinen Lähetä Sivu 7/7

KYBERTURVALLISUUSKULTTUURIN OPAS



19 20 21

22 23 24

25 26 27

28 29 30

31 32 33

34 35 36

37

38

39

40

41

42