Tietoturvaprosessien jalkauttaminen ISO/IEC 27001 organisaatioissa – uusi toimintamalli organisaatioiden onnistumiseen

Irina Shevchuk

Haaga-Helia ammattikorkeakoulu

Tradenomi YAMK

Digitaaliset liiketoiminnan mahdollisuudet

Master-opinnäytetyö

2024

Tiivistelmä

Tekijä(t)
Irina Shevchuk

Tutkinto
Tradenomi (YAMK)

Raportin/Opinnäytetyön nimi
Tietoturvaprosessien jalkauttaminen ISO/IEC 27001 organisaatioissa – uusi toimintamalli organisaatioiden onnistumiseen

Sivu- ja liitesivumäärä
66 + 2

Tietoturvan rooli on korostunut nykypäivän tietoyhteiskunnassa, jossa yhä useampi tekee tietotyötä ja käsittelee järjestelmiä. Teknologiaa kehitetään nyt entistä nopeammin. Sen myötä myös kyberuhkat ovat kasvaneet ja kyberhyökkäystekniikat kehittyneet. Vaikka teknologia on kehittynyt, niin ihminen on kuitenkin pysynyt samana. Ihminen voi olla välinpitämätön tai väsynyt ja on yleinen sanonta, että ”ihminen on tietoturvan heikoin lenkki”. Tietoturvan merkitys ei siis rajoitu pelkästään teknologiaan, vaan se sisältää myös prosessien, organisaatiokulttuurin ja ihmisten näkökulmat.

Tässä opinnäytetyössä tutkittiin ilmiötä, joka liittyy tietoturvaprosessien jalkauttamisen haasteisiin organisaatioissa. Organisaatioiden tietoturvatavoitteiden saavuttaminen voi epäonnistua esimerkiksi inhimillisen toiminnan, kuten ohjeiden noudattamattomuuden tai työntekijöiden huolimattomuuden takia. Tutkimuksessa kiinnitettiin erityistä huomiota teknisiin ja hallinnollisiin keinoihin näiden haasteiden ratkaisemiseksi. Opinnäytetyöllä oli kaksi tavoitetta, joista toinen oli kerätä ilmiöstä mahdollisimman paljon tietoa ja toinen kehittää näiden tietojen pohjalta toimintamalli, joka auttaisi organisaatioita tietoturvaprosessien jalkauttamisen suunnittelussa.

Opinnäytetyön teoreettisessa viitekehyksessä tutustuttiin ISO/IEC 27001 tietoturvastandardiin, tietoturvan hallintajärjestelmiin ja näihin kuuluviin elementteihin sekä organisaation tietoturvallisuuteen vaikuttaviin tekijöihin, kuten johtamiseen ja tietoturvakulttuuriin. Lisäksi perehdyttiin tietoturvakoulutuksiin sekä ihmisten tietoturvakäyttäytymiseen. Tutkimuksessa hyödynnettiin konstruktiivista tutkimusmenetelmää, jonka tavoitteena on luoda uutta tietoa ja kehittää uudenlainen ratkaisu käytännön ongelmaan. Empiiristä aineistoa kerättiin haastattelemalla tietoturvan jalkauttamiseen liittyen eri organisaatioiden asiantuntijoita heidän tietoturvaprosessien jalkauttamiseen liittyvistä kokemuksista. Empiirinen osio on otsikoitu vastaamaan teemoja, jotka nousivat esiin haastatteluista.

Opinnäytetyössä tunnistettiin useita jalkauttamiseen vaikuttavia tekijöitä. Teoreettisen ja empiirisen tiedon pohjalta rakennettiin toimintamalli, jonka tarkoituksena on helpottaa tietoturvaprosessien jalkauttamisen suunnitteluvaihetta. Malli perustuu tietoturvan prosessien käyttöönottoon vaikuttavien tekijöiden tunnistamiseen ja pyrkii minimoimaan epäonnistumisen riskit.

Asiasanat
Tietoturva, tietoturvaprosessit, tietoturvan jalkauttaminen, ISO/IEC 27001

Sisällys

1 Johdanto

Tietoturvan rooli on korostunut nykypäivän tietoyhteiskunnassa, jossa yhä useampi tekee tietotyötä ja käsittelee järjestelmiä. Olemme niin yksilöinä kuin organisaatioina yhä riippuvaisempia erilaisista tietojärjestelmistä ja digitaalisista palveluista. Organisaatiot keräävät myös yhä enemmän tietoja asiakkaista. Tietoturvan merkitys korostuu erityisesti niissä organisaatioissa, joiden liiketoiminta perustuu olennaisesti erilaisen tiedon hyödyntämiseen.

1.1 Tietoturvan kasvava merkitys nykypäivän työelämässä

Tietoturvallisuuden toteutumiselle digitaalisen transformaation aikana on useita haasteita. Teknologiaa kehitetään nyt entistä nopeammin. Uudet teknologiat ja erityisesti tekoäly tarjoavat mahdollisuuksia työn tehostamiseen ja esimerkiksi erilaisten kyberhyökkäysten parempaan havaitsemiseen. Teknologian ja tekoälyn nopean kehityksen myötä kuitenkin myös kyberuhkat ovat kasvaneet ja kyberhyökkäystekniikat kehittyneet. Esimerkkejä tekoälyn hyödyntämisestä kyberhyökkäyksistä on jo olemassa ja näitä hyödyntävät niin yksittäiset hyökkääjät, rikollisryhmät kuin myös valtiolliset toimijat. Tekoälypohjaisia tekniikoita käytetään sekä käyttäjän manipuloinnissa että kyberhyökkäysten havaitsemisen vaikeuttamisessa. Tekoälyä hyödynnetään jo esimerkiksi kohdennettuun tietojenkalasteluun, jolloin tekoäly kerää ja analysoi halutun organisaation tietoja ja generoi halutun kohdehenkilön kiinnostuksen kohteiden mukaisia kalasteluviestejä. Tulevaisuudessa myös erilaiset imitaatiohyökkäykset tulevat kasvamaan, jolloin ihmisten ääninäytteitä tai ulkonäköä tullaan matkimaan ja hyödyntämään erilaisissa syväväärennöshuijauksissa. (Aksela, Marchal, Patel, Rosenstedt & WithSecure 2022, 14–15)

Vaikka teknologia on kehittynyt, ihminen on kuitenkin pysynyt samana. Ihminen voi olla välinpitämätön tai väsynyt, jonka takia ihmistä on helpompi huijata. Sen takia tietoturvan kehittämisessä on hyvä keskittyä myös inhimillisiin asioihin ja siihen, että saadaan ihmiset toimimaan asianmukaisesti ja noudattamaan ohjeita. On yleinen sanonta, että ”ihminen on tietoturvan heikoin lenkki”. Jos tutkitaan numeerista dataa ilmiön taustalla, niin esimerkiksi tietoturvayritys Tessianin ja Stanfordin yliopiston tutkija Jeff Hancockin raportin (2022, 3–26) mukaan:

- 88% tietoturvaloukkauksista johtuu inhimillisestä virheestä
- 43% ihmisistä on tehnyt virheitä, jotka ovat vaarantaneet organisaation tietoturvaa
- 25% ihmisistä on joskus klikannut kalastusviestiä
- 58% ihmisistä on lähettänyt sähköpostiviestin väärälle vastaanottajalle

Saman raportin mukaan esteitä hyvien tietoturvapäätösten tekemiseen ovat erilaiset häiriötekijät, stressi, nopea työskentely ja uupumus. 93% työntekijöistä on stressaantunut ja väsynyt töissä.

Hyvin usein tietoturva käsitetään IT-osaston vastuuna ja teknisenä asiana, joka voidaan jättää teknisten ihmisten hoidettavaksi. (Järvinen 2022, 32) Tietoturva ei kuitenkaan voi olla enää pelkän IT-osaston harteilla ja sen kehittämiseen ja kouluttamiseen tarvitaan enemmän resursseja ja keinoja. Erityisesti viime vuosina puhuttaneen Vastaamon tietoturvaloukkauksen jälkeen tietoturvasta on alettu puhumaan yhä enemmän niin palveluntarjoajien kuin asiakkaiden keskuudessa. Tapaus oli ennennäkemätön laajuudeltaan ja julmuudeltaan.

Vastaamo oli vuonna 2008 perustettu yksityinen psykoterapiapalveluiden tarjoaja, jonka järjestelmiin murtauduttiin ensimmäistä kertaa vuonna 2018, jolloin yhtiön potilastietokanta varastettiin. Tietokanta sisälsi 31 980 potilaan sensitiivisiä henkilötietoja henkilötunnuksista terapeutin muistiinpanoihin. Yrityksen itse kehittämä tietojärjestelmä tallensi potilastietoja palvelimelle, joka oli ollut julkisesti saatavilla internetissä ainakin kaksi vuotta. Potilastietokanta oli niin heikosti suojattu, että se murrettiin ainakin kahdesti. Toisessa, vuoden 2019 tietoturvamurrossa ei varastettu merkittäviä määriä tietoja. Yritys jopa huomasi toisen tietomurron ja siirsi potilastietokannat turvallisempaan paikkaan, mutta ei kuitenkaan vielä tuolloin tehnyt ilmoituksia potilastietojen vaarantumisesta. Syyskuussa 2020 tietomurron tekijä alkoi kiristämään Vastaamon johtoa tietojen julkaisemisella. Kun yritys ei lopulta suostunut maksamaan lunnaita, tietomurron tekijä alkoi kiristämään potilaita ja vuotamaan potilastietoja pimeään verkkoon. (Hyppönen, 2022, alaluku CASE Vastaamo)

Tapauksen käsittely jatkuu edelleen oikeudessa tämän opinnäytetyön kirjoittamisen aikaan, mutta erityisesti johdon vastuu on korostunut ja puhuttanut tämän tapauksen yhteydessä. Organisaatiot ovat alkaneet kantaa enemmän huolta omasta tietoturvan tasostaan ymmärrettyään millaisia sanktioita tietoturvan laiminlyönnistä voi seurata, puhumattakaan mainehaitasta, joka yhdessä luottamuspulan kanssa voi johtaa täyteen asiakaskatoon ja liiketoiminnan loppumiseen. Viime vuosina tietoturvan johtamisjärjestelmät ja standardit, kuten tässäkin opinnäytetyössä käsiteltävä ISO/IEC 27001 -standardi, ovat kasvattaneet suosiotaan todennäköisesti myös tämän tapauksen saaman julkisuuden myötä.

1.2 Tutkimusongelma

Tietoturvan merkitys ei rajoitu pelkästään teknologiaan, vaan se sisältää myös prosessien, organisaatiokulttuurin ja ihmisten näkökulmat. Tämän takia tietoturvan jalkauttaminen organisaatioon on monimutkainen prosessi, jolle ei ole helppo löytää yhtä ja oikeaa tapaa. Jalkauttamisella tarkoitetaan tässä yhteydessä eri tietoturvastrategioiden ja -suunnitelmien toimeenpanemista ja käytäntöön viemistä organisaatiossa. Jalkauttamiseen kuuluu viestintä sekä ne konkreettiset toimet, joilla saadaan haluttu muutos tapahtumaan organisaatiossa ja käytännöt osaksi organisaation jokapäiväistä toimintaa.

Tietoturvaprosessien jalkauttamiseen organisaatiossa voi käyttää useita eri keinoja. Jalkauttamisen keinot pitää valita kunkin tavoitteen osalta erikseen. Jalkauttamista voidaan tehdä hallinnollisin keinoin, kuten ohjeistamalla ja kouluttamalla tai teknisin keinoin, kuten esimerkiksi käyttäjien tekemistä rajoittamalla, uusien järjestelmien tai automaatioiden käyttöönotolla. Kaikkien prosessien ja käytäntöjen jalkauttaminen hallinnollisin keinoin ei välttämättä johda riittävään lopputulokseen. Ihmiset saavat loppukädessä itse päättää haluavatko he noudattaa ohjeistuksia tai keskittyä koulutuksissa. Yhtä lailla kaiken jalkauttaminen teknisin keinoin ei ole mahdollista tai kannattavaa esimerkiksi taloudellisten syiden tai työntekijöiden työtehtävien merkittävän hidastumisen tai estymisen takia. Kaikkia prosesseja ei siis pysty jalkauttamaan samalla kaavalla. Käytännön ongelma on se, että joskus valitsemme jalkauttamisen keinot intuitiivisesti oman tai organisaation kollektiivisen kokemuksen pohjalta, eivätkä valitsemamme keinot aina tuota haluttua lopputulosta, jolloin tietoturvaan liittyvät riskit eivät aina pienene. Organisaatioissa saattaa myös syntyä muutosvastarintaa, mikä vaikuttaa negatiivisesti organisaation tietoturvakulttuuriin.

Esimerkiksi jos organisaatiossa halutaan ottaa käyttöön tiedon luokittelumalli, jonka tavoitteena on se, että salaiseksi luokiteltuja dokumentteja ei lähetettäisi sähköpostitse organisaation ulkopuolelle ilman sitä, että sähköpostiviesti on salattu, voidaan jalkauttamistavaksi valita aluksi hallinnolliset keinot, kuten ohjeistus ja koulutus. Tällöin uusi käytäntö kirjattaisiin yrityksen tietoturvaohjeistukseen ja -politiikkaan ja viestittäisiin organisaatiolle tietoturvakoulutuksen yhteydessä. Myöhemmin kuitenkin organisaation IT-osastossa huomataan, että henkilöstö ei noudateta kyseistä ohjetta ja salassa pidettäviä dokumentteja sisältävät sähköpostiviestit lähetetään edelleen salaamattomina, jolloin siis todetaan, että alun perin valittu jalkauttamiskeino ei ole toiminut. Myöhemmin IT-osasto ryhtyisi tutkimaan, millä tavoin uusi käytäntö olisi voitu jalkauttaa ilman riskiä siitä, että ihmiset eivät noudata ohjeita ja löytäisi markkinoilta sähköpostiin integroitavan teknisen työkalun, joka tunnistaisi salassa pidettävät dokumentit ja salaisi automaattisesti näitä sisältävät sähköpostiviestit.

1.3 Tutkimuksen rajaus

Organisaation tietoturvan tasoa on hankala mitata yhdellä mittarilla, sillä se koostuu niin monesta eri osa-alueesta. Tietoturvan tason mittaamiseen on kuitenkin kehitetty useita kansallisia ja kansainvälisiä eri viitekehyksiä ja standardeja. Yksi tietoturvallisuuden kansainvälinen standardisarja on ISO/IEC 27000, joka sisältää suosituksia tietoturvallisuuden johtamisjärjestelmän rakentamiseen ja ylläpitämiseen sekä riskien arviointiin ja hallintaan. (SFS ry s.a.) Suomessa yhä useampi organisaatio on alkanut hankkimaan ISO/IEC 27001 -tietoturvasertifikaatteja. Sertifioidun organisaation on helpompi vakuuttaa asiakkailleen ja muille sidosryhmilleen tietoturvakäytäntöjensä olevan hyvällä tasolla. Koska sertifikaatti on voimassa kolme vuotta, organisaatio myös osoittaa sertifioitumalla olevansa sitoutunut tietoturvan jatkuvaan kehittämiseen. (Kolehmainen, 2023)

Tietoturvan merkityksen kasvaessa yhä useammat organisaatiot rakentavat tietoturvan hallintajärjestelmiä ja hankkivat sertifikaatteja vastatakseen asiakkaidensa kasvaviin vaatimuksiin, eli joskus jopa ulkoisen paineen vuoksi.

Tämä tutkimus rajattiin koskemaan tietoturvakäytäntöjen jalkauttamista ISO/IEC 27001 -standardia noudattavissa organisaatioissa. Haastateltavien henkilöiden organisaatiot olivat joko valmiiksi ISO/IEC 27001 -sertifioituja tai sellaisia organisaatioita, jotka olivat rakentaneet tietoturvan hallintajärjestelmänsä tämän standardin pohjalta. Tämä varmisti sen, että haastatteluista saadut tulokset olisivat vertailukelpoisia, kun tiedettiin, että organisaatiot ovat jalkauttaneet samanlaisia käytäntöjä ja prosesseja. Kaikkien haastateltavien organisaatiot olivat asiantuntijaorganisaatioita, joiden toimintaan liittyy korkeita tietoturvariskejä niiden käsittelemän arkaluontoisten tai luottamuksellisten tietojen takia. Tutkimuksessa ei kuitenkaan paneuduttu yksityiskohtaisesti ISO/IEC 27001 -standardin vaatimuksiin ja hallintakeinoihin, vaan ennemmin tarkasteltiin muutamien standardin vaatimusten ja hallintakeinojen soveltamisen kautta jalkauttamistapaan vaikuttavia tekijöitä. Liitteen 1 esimerkkitapaukset tai -tavoitteet ovat ISO/IEC 27001 -standardista sovellettuja. Koska ISO/IEC 27001 on kuitenkin niin yleisessä käytössä oleva tietoturvastandardi, olivat sen vaatimukset ja hallintakeinot hyviä yleiskäytäntöjä, joiden soveltamistapoja pystyi käyttämään esimerkkinä haastatteluissa.

1.4 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tässä opinnäytetyössä keskitytään tietoturvakäytäntöjen ja -prosessien jalkauttamiseen organisaatioissa ja siihen, millaisia tekijöitä tulee ottaa huomioon jalkauttamisprosessin onnistumiseksi. Tutkimuksella on kaksi tavoitetta. Ensimmäisenä tavoitteena on kerätä tietoa siitä, miten asiantuntijaorganisaatiot, jotka ovat kehittäneet tietoturvaansa ISO27001 standardin mukaisesti, valitsevat ja soveltavat erilaisia keinoja tietoturvaprosessien ja -käytäntöjen jalkauttamiseen. Toisena tavoitteena on kehittää tämän tiedon ja teoreettisen viitekehyksen pohjalta uusi, toimiva ja tietoon perustuva toimintamalli, jota voidaan hyödyntää jatkossa tietoturvaprosesseja jalkauttaessa. Toimintamalli tulee perustumaan niiden tekijöiden tunnistamiseen, jotka vaikuttavat tietoturvan jalkauttamiseen ja mallin avulla minimoidaan riskit siitä, että jalkauttaminen epäonnistuu.

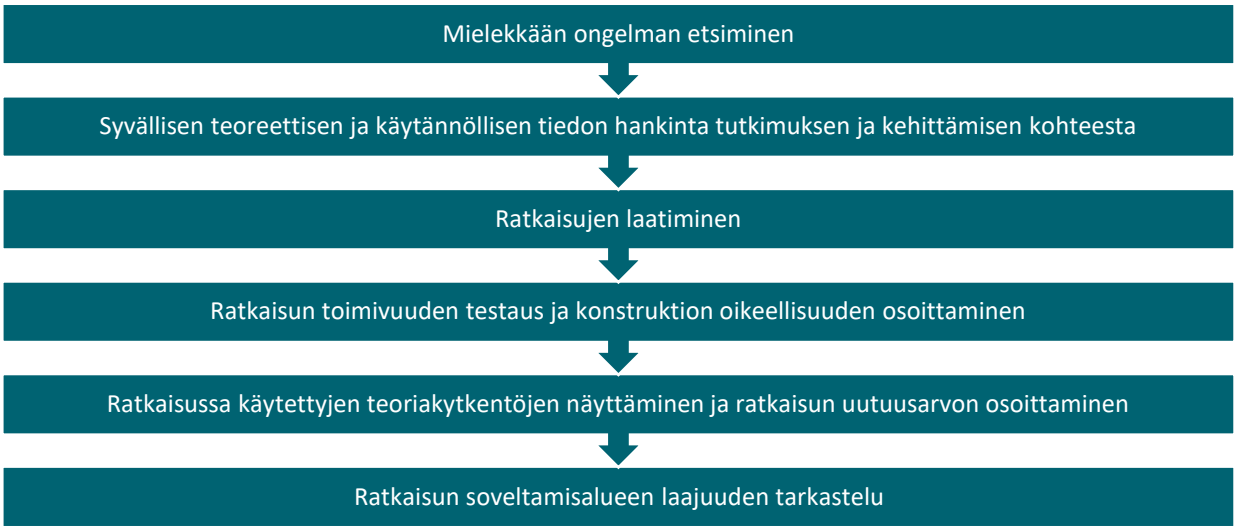
Tutkimuskysymykset keskittyvät organisaatioiden tietoturvaprosessien jalkauttamiseen ja siihen, miten tämä toteutetaan erilaisin keinoin. Ensimmäinen kysymys tutkii, mitä erilaisia menetelmiä ja toimintatapoja organisaatiot käyttävät tietoturvaprosessiensa levittämiseen ja juurruttamiseen. Toinen kysymys syventyy tutkimaan sitä, mitkä tekijät vaikuttavat jalkauttamiskeinojen tehokkuuteen ja soveltuvuuteen. Kysymykset, joihin opinnäytetyössäni on vastattava saavuttaakseni opinnäytetyön tavoitteet ovat:

- K1 – Millaisilla eri keinoilla organisaatiot jalkauttavat tietoturvaprosesseja?
- K2 – Mitkä tekijät vaikuttavat jalkauttamiseen?

Toivon mukaan tästä opinnäytetyöstä ja siitä syntyvästä mallista on hyötyä tietoturvan kehittämisestä vastaaville asiantuntijoille, jotka miettivät keinoja jalkauttamaan tietoturvaprosessejaan paremmin.

1.5 Konstruktiivinen tutkimus

Tutkimuksen lähestymistapa on konstruktiivinen tutkimus, jonka vaiheet on kuvattu Kuva 1. Konstruktiivisen tutkimuksen tavoitteena on luoda käytännön ongelmaan teoreettisen ja empiirisen tiedon pohjalta uutta tietoa ja uudenlainen ratkaisu, joka tuo hyötyä. Konstruktiivinen tutkimus soveltuu lähestymistavaksi, kun halutaan luoda jokin konkreettinen tuotos kuten malli, prosessi tai suunnitelma. (Ojasalo, Moilanen & Ritalahti, 2014, 65–66) Tässä tutkimuksessa halutaan luoda ymmärrystä ja malli sille, mitä jalkauttamistapaa kannattaa käyttää missäkin tilanteessa. Koska kyseessä on konkreettinen malli, konstruktiivinen tutkimus soveltuu hyvin lähestymistavaksi. Myös konstruktiiviseen tutkimukseen soveltuva kysymys ”Voidaanko organisaatiossamme tehdä jokin paremmin?” sopi tähän tutkimusaiheeseen ja tuotokseen.



Kuva 1. Konstruktiivisen tutkimuksen prosessin vaiheet (mukaillen Ojasalo ym. 2014, 67)

Koska konstruktiivinen tutkimus perustuu uusien ideoiden ja innovaatioiden kehittämiseen, on suositeltavaa suorittaa alustavia kokeiluja tai testejä ennen ideaan perustuvan ratkaisun lopullista testausta. Kehittämishaaste, työn tavoitteet ja kuvassa 1 näkyvät prosessin eri vaiheet on tärkeä dokumentoida selkeästi. Prosessin loppuvaiheessa ratkaisu on esiteltävä ja arvioitava ymmärrettävästi. Kehitetyn ratkaisun toimivuus tulisi arvioida markkinoilla tai organisaation sisällä. Ratkaisun

toimivuuden arvioinnin voi toteuttaa joskus myös jälkikäteen, minkä takia opinnäytetöistä voikin puuttua lähestymistavalle tyypillinen ratkaisun testausvaihe. (Ojasalo ym. 2014, 67–68)

1.6 Haastattelu tiedonhakumenetelmänä

Konstruktiivisen tutkimuksen menetelminä voi käyttää useita vaihtoehtoja sillä lähestymistapa ei rajaa pois mitään menetelmää. Tyypillisiä menetelmiä tässä lähestymistavassa on kuitenkin havainnointi, ryhmäkeskustelut, kysely ja haastattelu. Haastattelu on vuorovaikutteista toimintaa, joka vaatii luottamuksen osallistujien, eli tiedon kerääjän (haastattelija) ja tiedon antajan (haastateltava) välillä. Haastattelun ja kehittämistyön tarkoitus ja luottamuksellisuus on selitettävä haastateltavalle. Haastattelu eroaa tavallisesta keskustelusta, koska siinä haastattelija ohjaa keskustelua. Puolistrukturoidussa haastattelussa kysymykset ovat ennakkoon laadittuja, mutta niiden järjestystä tai muotoilua voidaan muokata tilanteen mukaan. Tiettyjä kysymyksiä voidaan jättää tapauskohtaisesti pois ja vastaavasti nostaa uusia mieleen tulleita kysymyksiä haastattelun edetessä. Puolistrukturoitu haastattelu mahdollistaa tietyn joustavuuden ja lisää mahdollisuutta syvälliseen tietojenkeruuseen. Avoimessa haastattelussa taas haastattelija ja haastateltava keskustelevat aiheesta tai -ongelmasta yleisesti ja molemmat osallistuvat keskusteluun aktiivisesti ja tasavertaisesti, jolloin keskustelu voi olla myös epämuodollista. Sekä puolistrukturoitu että avoin haastattelu ovat molemmat hyödyllisiä, kun tarkoituksena on esimerkiksi tutkia jonkin ilmiön merkitystä osallistujille. (Ojasalo ym. 2014, 68; 108–109; Hirsjärvi & Hurme, 2009)

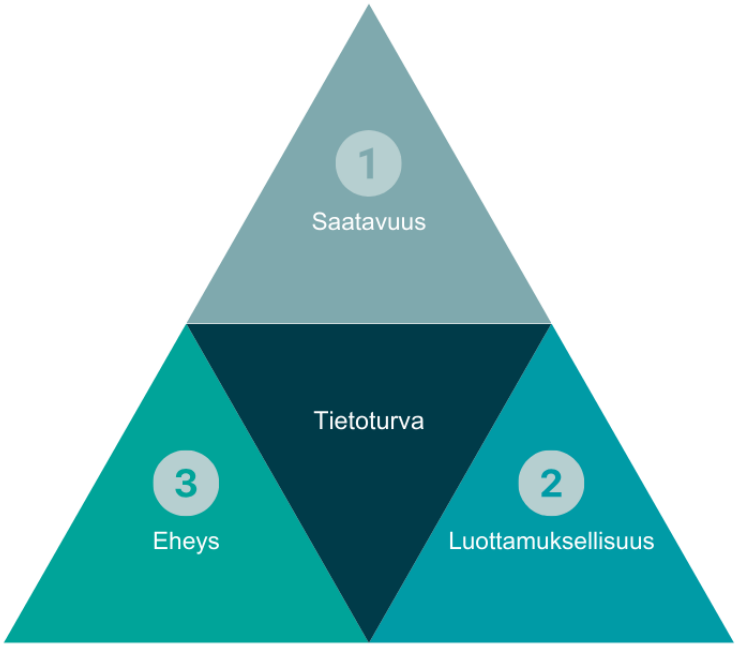
Dokumenttianalyysi on menetelmä, jossa tavoitteena on tehdä päätelmiä kirjallisesta aineistosta, kuten litteroiduista haastatteluista. Aineisto analysoidaan järjestelmällisesti ja tutkittavasta aiheesta luodaan ymmärrettävä sanallinen kuvaus. Analyysin avulla aineisto tiivistetään, järjestellään ja selkeytetään, jotta siitä voidaan tehdä luotettavia johtopäätöksiä. (Ojasalo ym. 2014, 136) Empiirisessä osiossa käytettyä aineistoa hankittiin puolistrukturoitujen asiantuntijoiden syvähaastattelujen avulla, jotka ajoittain muuttuivat myös avoimeksi haastatteluksi. Haastattelut nauhoitettiin ja litteroitiin. Tämän jälkeen litteroiduille haastatteluille tehtiin dokumenttianalyysi, jonka aikana aineisto luokiteltiin teemoittain. Opinnäytetyön empiirinen osio, eli kappale 3 on otsikoitu näiden teemojen mukaisesti.

Haastattelun pohjaksi haastateltaville esiteltiin opinnäytetyön tavoitteet, taustaa, liitteessä 1 luetellut sovellettavat esimerkkitapaukset sekä vastausten luottamuksellisuus. Haastateltaville on kerrottu, että tavoitteena on kerätä tietoa siitä, miten organisaatiot, joilla on ISO/IEC 27001 -sertifikaatti tai jotka ovat hankkimassa sellaista, valitsevat ja soveltavat erilaisia keinoja tietoturvaprosessien ja -käytäntöjen jalkauttamiseen sekä siitä, mitkä asiat näihin päätöksiin vaikuttavat. Ennen haastattelua haastateltaville on suositeltu haastattelun saate- ja suostumuslomakkeen yhteydessä, että he miettisivät tai palauttaisivat mieleen omia kokemuksia, onnistumisia tai haasteita

tietoturvakäytäntöjen jalkauttamisprosesseista ja erityisesti teknisten tai hallinnollisten (ohjeistus, koulutus) keinojen käytöstä. Haastateltaville on myös kerrottu, että tutkimuksen tavoitteena on kehittää uusi, toimiva ja tietoon perustuva toimintamalli, jota voidaan hyödyntää jatkossa tietoturvaprosesseja jalkauttaessa. Haastattelut ovat sisältäneet avoimia kysymyksiä, mikä mahdollisti haastateltavien näkökulmasta tärkeiden asioiden esiin nostamisen. Suurin osa haastatteluista järjestettiin Teamsin välityksellä ja ne ovat kestäneet johdantoineen noin tunnin. Haastateltavia asiantuntijoita oli yhteensä viisi ja he työskentelivät kaikki eri organisaatioissa. Haastateltavat asiantuntijat ovat työskennelleet sekä pk-yrityksissä että suurissa yrityksissä, joiden toimintaan liittyy korkeita tietoturvariskejä niiden käsittelemän arkaluontoisten tai luottamuksellisten tietojen takia. Haastatteluissa käytettiin esimerkkinä liitteeseen 1 listattuja esimerkkitapauksia, joiden toteutuksiin organisaatiot voisivat harkita sekä teknisiä että hallinnollisia toteutustapoja. Nämä esimerkit tarjosivat konkretiaa, joilla haastateltavat pääsivät kiinni siihen, miten standardin eri osa-alueita voidaan toteuttaa käytännössä sekä teknisin että hallinnollisin keinoin.

2 Teoreettinen viitekehys: tietoturvastandardit, käytännöt ja vaikutukset

Tietoturva koostuu hallinnollisista ja teknisistä toimenpiteistä. Hallinnollisilla toimenpiteillä tarkoitetaan esimerkiksi tietoturvakäytäntöjen laatimista tai tietoturvakoulutuksen järjestämistä henkilöstölle ja teknisillä toimenpiteillä taas esimerkiksi virustorjuntajärjestelmien tai palomuurien käyttöönottoa. Lähes kaikessa alan kirjallisuudessa tietoturvallisuuden tavoitteena pidetään Kuva 2 esitettyä kolmea periaatetta: *saatavuutta*, *luottamuksellisuutta* ja *eheyttä*. Saatavuuden tilalla käytetään joskus myös termiä *käytettävyys*.



Kuva 2. Tietoturvan kolme periaatetta (mukaillen Chopra & Chaudhary, 2020, luku 1)

Luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat vain niiden saatavilla, kenellä on siihen oikeus. Tällä pyritään siis varmistamaan, että tietoja ei paljasteta luvattomille vastaanottajille. *Eheydellä* tarkoitetaan sitä, ettei tietoja voi muuttaa muut kuin siihen oikeutetut. Tavoitteena on varmistaa, että tiedot eivät vääristy tai korruptoidu tahattomasti tai tarkoituksellisesti henkilön, viruksen tai järjestelmän toimesta. *Saatavuudella* taas tarkoitetaan sitä, että tiedot sekä tietojärjestelmät ovat siihen oikeutettujen saavutettavissa ja käytettävissä silloin kun he niitä tarvitsevat. (Raggad 2010, 20; Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020)

Kuten tutkimusongelman kuvauksessa todettiin, tietoturvan toteutumisessa olisi otettava teknologisen näkökulman lisäksi huomioon prosessit, organisaatiokulttuuri ja ihmiset. Teoreettinen viitekehys keskittyy avaamaan näitä näkökulmia tarkemmin. Aluksi käsitellään tietoturvastandardit ja erityisesti ISO/IEC 27001, jonka prosessien jalkauttamiseen tämä opinnäytetyö keskittyy.

2.1 Tietoturvastandardit ja -viitekehykset

Tietoturvan suunnittelun jäsentämiseksi ja organisoimiseksi on luotu kansainvälisiä ja kansallisia standardeja ja viitekehyksiä. Vaikka niitä yleisesti kutsutaan tietoturvastandardeiksi, ne eivät aseta suoraa vaatimusta itse tietoturvan tasolle tai sisällölle, vaan ohjaavat tietoturvasuunnittelun menettelytapoja. Erityisesti tietoturvan suunnittelun dokumentaatiolle standardit tarjoavat selkeän ja vertailukelpoisen rakenteen. Pelkkä standardin noudattaminen ei siis takaa riittävää turvallisuustasoa. Standardit määrittelevät ainoastaan sen, mitä suunnittelutyöhön kuuluu ja miten sen tulokset tulee esittää. (Hakala, Vainio & Vuorinen 2006, 46)

Organisaatiot käyttävät useita erilaisia tietoturvan standardeja, kuten esimerkiksi National Institute of Standard and Technology (NIST), Control Objectives for Information and Related Technologies (COBIT), International Organization for Standardization (ISO) ja International Electrotechinal Commission (IEC). Nämä standardit tarjoavat ohjeita ja suosituksia parhaista tietoturvakäytännöistä tietoturvariskien vähentämiseksi. NIST on kehitetty Yhdysvalloissa liittovaltion ja yksityisyritysten yhteistyönä ja onkin eniten käytetty amerikkalaisyritysten keskuudessa, kun taas ISO/IEC ja COBIT ovat kansainvälisiä ja globaalisti tunnistettuja standardeja, joita voidaan käyttää missä tahansa maassa tai toimialalla. Erityisesti ISO/IEC 27001 ja ISO/IEC 27002 ovat standardeja, jotka sisältävät paljon ohjeita ja parhaita käytäntöjä tietoturvan parantamiseksi. Näiden soveltamiseen ja käyttöönottoon kuitenkin liittyy ihmisen käyttäytymiseen liittyviä haasteita. Erään tutkimuksen mukaan organisaatiot eivät huomioi sisäisiä ongelmiaan suunnitellessaan tietoturvakäytäntöjään. Organisaatioiden tietoturva koostuu monimutkaisista prosesseista, joihin liittyy useita tekijöitä, kuten koulutus, inhimilliset tekijät ja teknologia. Näitä kaikkia on hallittava yhden yhteisen viitekehyksen avulla. (Ali, Dominic, Ali, Rehman, & Sohail, 2021, 2; Omnistruct 2020; Yeniman Yildirim, Akalp, Aytac, & Bayram, 2011, 360)

2.2 ISO/IEC 27001 -standardi

ISO/IEC 27001 -standardi kuuluu ISO/IEC 27000 -tietoturvallisuuden standardisarjaan ja on maailman tunnetuin tietoturvan hallintajärjestelmien standardi. Se soveltuu kaiken kokoisille ja kaikilla toimialoilla toimiville organisaatioille ja sisältää vaatimukset hallintajärjestelmän rakentamiseen, ylläpitämiseen ja jatkuvaan parantamiseen. ISO/IEC 27001 -standardin pyrkimyksenä on määritellä malli tietoturvallisuuden hallinnalle sisältäen tietoturvan hallintajärjestelmän luomisen, käyttöönoton, ylläpidon, valvonnan, katselmuksen sekä kehittämisen. Standardin keskeisenä ideana on kehittää tietoturvallisuuden hallintajärjestelmää prosessiluontoisesti PDCA-mallin (Plan, Do, Check, Act) pohjalta, jonka vaiheet on kuvattu tarkemmin seuraavan luvun Kuva 3. (International Organization for Standardization s.a.; Hakala ym. 2006, 49)

ISO/IEC 27001 -standardi koostuu kahdesta osiosta. Ensimmäisessä osassa, joka koostuu luvuista 0–10, on päävaatimukset tietoturvan hallintajärjestelmän perustamiselle ja ylläpitämiselle. Luvut 0–3 kuvaavat itse standardia. Luvut 4–10 kattavat organisaation toimintaympäristön, johtajuuden, suunnittelun, tukitoiminnot, toiminnan, suorituskyvyn arvioinnin ja parantamisen. Kaikki vaatimukset näissä kohdissa on täytettävä sertifikaatin saadakseen, eikä yhdenkään kohdan poissulkeminen ole mahdollista. Toisessa osassa, liitteessä A, on listattu tietoturvan hallintajärjestelmän hallintakeinoja. Uusimmassa ISO/IEC 27001:2022 versiossa näitä liitteen A hallintakeinoja on 93 jaettuna 4 kategoriaan, kun aiemmassa ISO/IEC 27001:2013 versiossa niitä on ollut 114, jaettuna 14 kategoriaan. Vaikka standardi on päivitetty vastaamaan nykyisen teknologian ja tietoturvan muuttuvia vaatimuksia, suurin osa muutoksista on luonteeltaan kosmeettisia ja muutokset liittyivät lähinnä olemassa olevien hallintakeinojen uudelleenjärjestelyyn, yhdistämiseen ja tarkentamiseen. Kaikkien hallintakeinojen käyttäminen ei ole pakollista, mutta niitä odotetaan käytettävän apuna organisaation riskien tunnistamisessa, -arvioinnissa ja -käsittelyssä. (Kenyon 2019, luku 1.3; Adarsh & Greeshma, 2023, luku 2; ISMS.online, 2023)

Hallintakeinot jaetaan uusimman, vuonna 2022 julkaistun standardin version mukaan organisaatioon liittyviin hallintakeinoihin, ihmisiin tai henkilöstöön liittyviin hallintakeinoihin, fyysiseen turvallisuuteen liittyviin hallintakeinoihin sekä teknologisiin hallintakeinoihin. Organisaation hallintakeinot liittyvät johtamiseen sekä hallintaan ja edistävät tietoturvaa strategian ja johtajuuden kautta. Organisaation hallintakeinot painottavat selkeiden roolien, vastuiden ja politiikkojen tarvetta, jotka tukevat yrityksen tietoturvatavoitteita. Ihmisiin tai henkilöstöön liittyvät hallintakeinot keskittyvät ihmisten toimintaan ja käyttäytymiseen organisaatiossa ja ne on suunniteltu vähentämään tietoturvariskejä, jotka voivat johtua inhimillisistä virheistä tai toiminnasta. Näihin kuuluu esimerkiksi jatkuvan tietoturvakoulutuksen tarjoaminen henkilöstölle. Fyysiseen turvallisuuteen liittyvät hallintakeinot ovat konkreettisia toimenpiteitä organisaation omaisuuden ja tietovarantojen suojaamiseksi. Niiden tavoitteena on estää luvaton pääsy ja vahingot sekä suojata tietojärjestelmät. Esimerkiksi yrityksen puhtaan pöydän periaate kuuluu näihin hallintakeinoihin. Teknologiset hallintakeinot pyrkivät suojaamaan organisaation digitaalisia järjestelmiä, estämään luvattoman pääsyn tietoihin ja ylläpitämään järjestelmien eheyttä. Näihin kuuluu esimerkiksi haittaohjelmilta suojautuminen, tietojen varmuuskopiointi tai järjestelmien lokitus. (Adarsh & Greeshma, 2023, luku 3)

ISO/IEC 27001 -standardin julkaisun voi ostaa pdf-muotoisena suoraan kansainväliseltä standardoimisjärjestöltä (International Organization for Standardization ISO) tai Suomen Standardisoimisliitolta SFS ry:ltä heidän verkkosivuiltaan, jolloin sen saa myös suomen kielellä englannin lisäksi. Voisi kuvitella, että pelkkä standardin hankkiminen antaisi tarvittavat ohjeet sille, mitä pitäisi sertifikaatin saadakseen tehdä, mutta näin ei kuitenkaan ole. ISO/IEC 27001 -standardi ei ole ohjaileva siinä mielessä, että se ottaisi kantaa varmuuskopiointien tiheyteen tai siihen, millaista teknologiaa

tulisi käyttää verkkojen suojaamiseksi. Nämä päätökset jätetään organisaatioiden itsensä päätettäväksi. Virallisen standardin mukaan organisaation on laadittava soveltuvuuslausunto (englanniksi *Statement of Applicability* tai lyhennettynä *SoA*), jossa luetellaan kaikki hallintakeinot sekä perustelut niiden käyttämiselle tai käyttämättä jättämiselle. (Chopra & Chaudhary 2020, luku 1)

Alla olevasta taulukosta 1 ilmenee, että niin Suomessa kuin koko maailmassa ISO/IEC 27001 -sertifioitumisen trendi on viime vuosina ollut nouseva. Kaikkialla maailmassa sertifioitujen organisaatioiden määrä on kasvanut vuosittain noin 20–30 % ja Suomessa kasvu on ollut jopa noin 55–75 %. Viimeaikaisista Suomen ISO/IEC 27001 -sertifioiduista yrityksistä lähes 70 % toimii tietotekniikka-alalla. (International Organization for Standardization 2022–2023)

Taulukko 1. ISO/IEC 27001 sertifikaattien määrä vuosina 2019–2021 (International Organization for Standardization 2022–2023)

	2019	**% muutos**	**2020**	**% muutos**	**2021**
ISO/IEC 27001 -sertifioitua organisaatiota koko maailma	36 337	+22 %	44 499	+31 %	58 687
ISO/IEC 27001 -sertifioitua organisaatiota Suomi	66	+55 %	102	+76 %	180

Suomessa on tämän opinnäytetyön kirjoittamisen aikaan noin 200 sertifioitua organisaatiota ja määrä kasvaa koko ajan. ISO/IEC 27001 -sertifikaatti on voimassa kolme vuotta, kuitenkin niin, että voimassaolon aikana tehdään seuranta-auditointeja vuosittain. Sertifikaatin voi siis menettää, jos tietoturvan hallintajärjestelmää ei ylläpidetä ja kehitetä asianmukaisesti tai auditoinnissa ilmi tulleita puutteita ei korjata. Vaikka sertifiointi noudattaa standardoitua prosessia, käytännössä auditoinnit voivat vaihdella. On esimerkiksi havaittu tilanteita, joissa yritykset, joille on aiemmin myönnetty sertifikaatti, on uudelleensertifiointiprosessissa toisen auditoijan toimesta havaittu merkittävä määrä toimenpiteitä vaativia huomioita. ISO/IEC 27001 -sertifikaatti ei ole myönnettävissä yrityksen tuotteelle, vaan se kuvastaa organisaation yleisten tietoturvakäytäntöjen tasoa. ISO/IEC 27001 -sertifikaatit maksavat noin 15 000–50 000 euroa riippuen laajuudesta. Hintaan vaikuttavat esimerkiksi sertifioitavan organisaation koko ja sertifioitavat toimipisteet. On siis mahdollista jättää tietyt fyysiset sijainnit tai prosessit sertifioimatta. (Kolehmainen, 8.2.2023) Suomessa ISO/IEC 27001 -sertifiointeja ovat akkreditoituja myöntämään muun muassa KPMG, Bureau Veritas, Kiwa Inspecta ja Nixu.

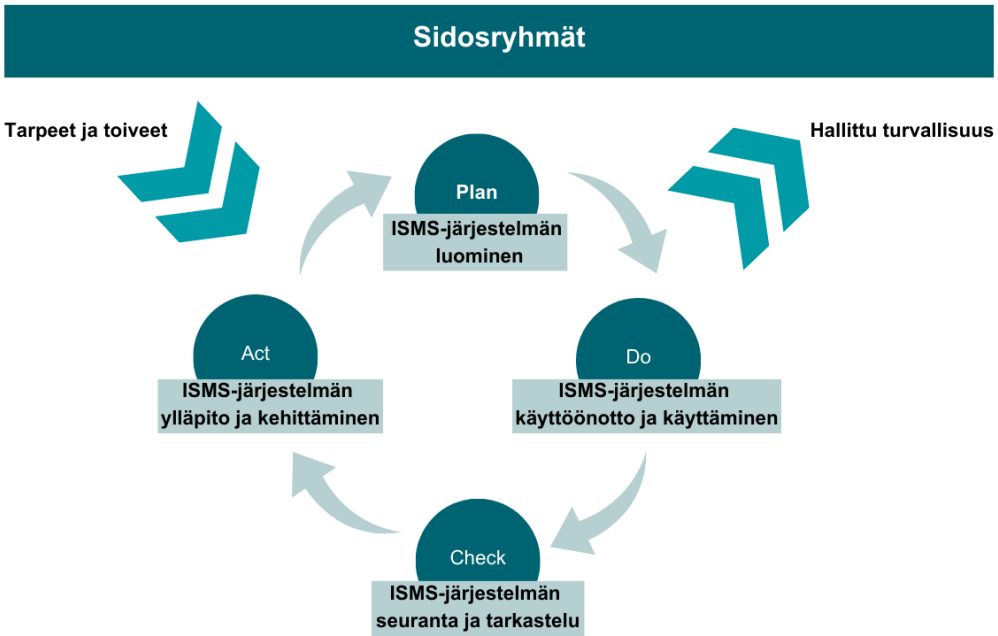
2.3 Tietoturvan hallintajärjestelmät

Tietoturvan hallintajärjestelmä (englanniksi *Information Security Management System* tai lyhennettynä *ISMS*) voi tuntua terminä hyvinkin abstraktilta. Puhuttaessa nykypäivänä hallintajärjestelmästä tai mistä tahansa järjestelmästä ajattelemme helposti tietojärjestelmää. Se ei kuitenkaan ole

mikään konkreettinen teknologia tai ohjelmisto, vaan viitekehys ja systemaattinen toimintatapa, jolla hallitaan organisaation tietoturvaa. Tietoturvan hallintajärjestelmä on iso kokonaisuus, joka sisältää paljon dokumentaatiota ja kuvailee organisaation tapaa toteuttaa ja kehittää tietoturvaa. Valtiovarainministeriön (2007, 40) ohje määrittelee tietoturvallisuuden hallintajärjestelmän viitekehykseksi, joka koostuu useista eri toimintamalleista ja dokumenteista. Järjestelmä kattaa ”tietoturvallisuuden yksityiskohtaisen organisoinnin, politiikat, suunnittelun, vastuut, menetelmätavat, prosessit ja tarvittavat resurssit”.

Tietoturvan hallintajärjestelmän tavoitteena on turvata organisaation tieto-omaisuus, joka voi olla esimerkiksi asiakas- ja henkilötietoa tai aineetonta omaisuutta, kuten liikesalaisuuksia tai tuotekehityssuunnitelmia. Tietoturvan hallintajärjestelmä tarjoaa järjestelmällisen lähestymistavan tietojen turvaamiseksi ja sisältää erilaisia käytäntöjä ja prosesseja riskien kohentamiseksi. Tietoturvan hallintajärjestelmän käyttöönotto on tärkeä strateginen päätös, sillä se koskee niin organisaation ihmisiä, prosesseja kuin IT-järjestelmiä. (Chopra & Chaudhary 2020, luku 1; SFS ry s.a.)

Tietoturvan hallintajärjestelmän kehittämisen PDCA-malli juontaa juurensa laadunvarmistuksesta. Sen mukaan liiketoimintaprosesseja tulisi tarkastella jatkuvan palautteen näkökulmasta, jotta johto voi tunnistaa ne kohdat, jotka vaativat parannusta. Suunnittelu tulisi tehdä ensin, minkä jälkeen seuraa toteutus ja suorituskyvyn mittaus. Mittausten tuloksia tulisi verrata alkuperäiseen suunnitelmaan, jotta tunnistetaan poikkeamat tai mahdolliset parannukset. Nämä tulokset tulisi raportoida johdolle, jotta voidaan päättää seuraavista toimenpiteistä. (Adarsh & Greeshma, 2023, luku 2)



Kuva 3. PDCA-mallin mukainen prosessi (mukaillen Hakala ym. 2006, 49)

Kun ISO/IEC 27001 mukaista tietoturvan hallintajärjestelmää lähdetään rakentamaan, olisi sen laajuus määriteltävä, eli mitä fyysisiä sijainteja, organisaation osastoja, prosesseja, tieto- tai muuta omaisuutta hallintajärjestelmä kattaa ja myös, mitä mahdollisesti jää sen ulkopuolelle. Tämän lisäksi olisi suoritettava riskiarviointi, eli tunnistaa mahdolliset tapahtumat ja arvioimaan niihin liittyvät riskit. Organisaation on myös valmisteltava tietoturvapolitiikka, jonka päätehtävänä on määritellä mitä turvatoimilla halutaan saavuttaa ja valittava ne hallintakeinot, jotka halutaan toteuttaa. Hallintakeinojen valinnan perusteella laaditaan myös soveltuvuuslausunto, johon kirjataan perusteluineen ja kuvauksineen mitkä hallintakeinot on toteutettu ja mitkä hallintakeinot on jätetty toteuttamatta. (Chopra & Chaudhary, 2020, luku 1)

Kun organisaatio saa ISO/IEC 27001 -sertifikaatin, se osoittaa, että sen tietoturvan hallintajärjestelmä on auditoitu akkreditoidun sertifiointiorganisaation toimesta, ja hyväksytty standardin mukaiseksi. Tämä viestii sidosryhmille ja asiakkaille, että yritys ottaa tietoturvan vakavasti ja on luotettava. Sertifiointiauditointi koostuu yleensä kahdesta vaiheesta. Ensimmäinen vaihe on asiakirjojen tarkastus, jossa auditoija tarkistaa prosessit ja käytännöt varmistaakseen, että ne ovat standardin mukaisia. Toinen vaihe on varsinainen sertifiointiauditointi, jossa auditoija arvioi kuinka organisaatiossa noudatetaan ISO/IEC 27001-standardia. Tässä vaiheessa auditoija arvioi pohjimmiltaan organisaatiossa implementoitujen hallintakeinojen tehokkuutta laaditun soveltuvuuslausunnon perusteella. (Adarsh & Greeshma, 2023, luku 2)

SWOT-analyysi tietoturvan hallintajärjestelmän implementoinnista voi auttaa varmistamaan tietoturvan hallintajärjestelmän toteutuksen onnistumisen. Analyysi tarjoaa paremman ymmärryksen turvallisuusympäristöstä ja antaa näkemyksiä haasteista, joita IT-osasto ja koko yritys kohtaavat. Kuva 4 Esimerkki tietoturvan hallintajärjestelmän toteutuksen SWOT-analyysistä (Adarsh & Greeshma, 2023, luku 2)Kuva 4 on lueteltuna joitain vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia, joita tietoturvan hallintajärjestelmän toteutuksesta voi seurata. (Adarsh & Greeshma, 2023, luku 2)

Vahvuudet	Heikkoudet
• Parantaa organisaation kokonaisturvallisuustasoa ja lisää yrityksen luotettavuutta. • Kilpailijoista erottautuminen asiakkaiden silmissä. • Tuo hyviä tietoturvakäytäntöjä ja vähentää turvallisuuspoikkeamista aiheutuvia kuluja.	• Merkittävä ajan, taloudellisten ja inhimillisten resurssien investointi prosessiin. • Prosessien omaksumisen ja jalkauttamisen haasteet. • Kustannukset voivat nousta ja järjestelmästä voi tulla liian monimutkainen käytettäväksi ja ylläpidettäväksi, jos sitä ei ole suunniteltu ja toteutettu oikein.

Mahdollisuudet	Uhat
• Kilpailuetu markkinoinnissa. • Auditoimisprosessissa voidaan tunnistaa parannusmahdollisuuksia. • Parempi markkina-asema, joka houkuttelee parempia mahdollisuuksia.	• Organisaatiotiedon paljastamisen riski kolmansille osapuolille. • Voi vaatia runsaasti resursseja • Liiallinen luottamus siihen, että tietoturvan hallintajärjestelmä suojaa kaiken tiedon.

Kuva 4 Esimerkki tietoturvan hallintajärjestelmän toteutuksen SWOT-analyysistä (Adarsh & Greeshma, 2023, luku 2)

2.4 Riskienhallinta

Tietoturvariskien hallinta tarkoittaa eri uhkien tunnistamista, arviointia ja käsittelyä organisaation tietovarantojen suojelemiseksi. Riskienhallinta on yksi kriittisimmistä vaiheista ISO/IEC 27001 -standardin vaatimusten toteuttamisessa, sillä se määrittää kaikki seuraavat toimenpiteet ja hallintakeinot, jotka organisaatio aikoo toteuttaa. ISO/IEC 27001 -standardissa keskitytään tunnistamaan todennäköisimmät tietoturvatapahtumat, jotka saattaisivat aiheuttaa organisaatiolle uhkia ja sen jälkeen suunnittelemaan keinot niiden välttämiseksi. Riskienhallintaprosessin (kuvattuna Kuva 5Kuva 1) jokaisessa vaiheessa on tärkeää kommunikoida ja konsultoida kaikkia asiaankuuluvia ulkoisia ja sisäisiä sidosryhmiä parhaimman näkemyksen saamiseksi. Organisaation on alkuun määriteltävä ja dokumentoitava tietoturvariskien arviointikriteerit ja riskien hyväksymisperusteet varmistaakseen yhdenmukaiset arviointitulokset organisaationlaajuisesti. Riskienhallinnassa ei pyritä siihen, että riski on nolla, vaan siihen, että riskit ovat hallittavissa. Koska riskejä ei voi täysin eliminoida, yrityksen on määriteltävä, mikä riskitaso on hyväksyttävä. Riskienhallintaprosessin laajuuden määrittely sisältää tavoitteiden ja odotettujen tulosten asettamisen sekä käytettävien riskityökalujen ja -menetelmien päättämisen. Myös vaadittavia resursseja, rooleja ja vastuita sekä riippuvuuksia muihin projekteihin on mietittävä. (Adarsh & Greeshma, 2023, luku 4)

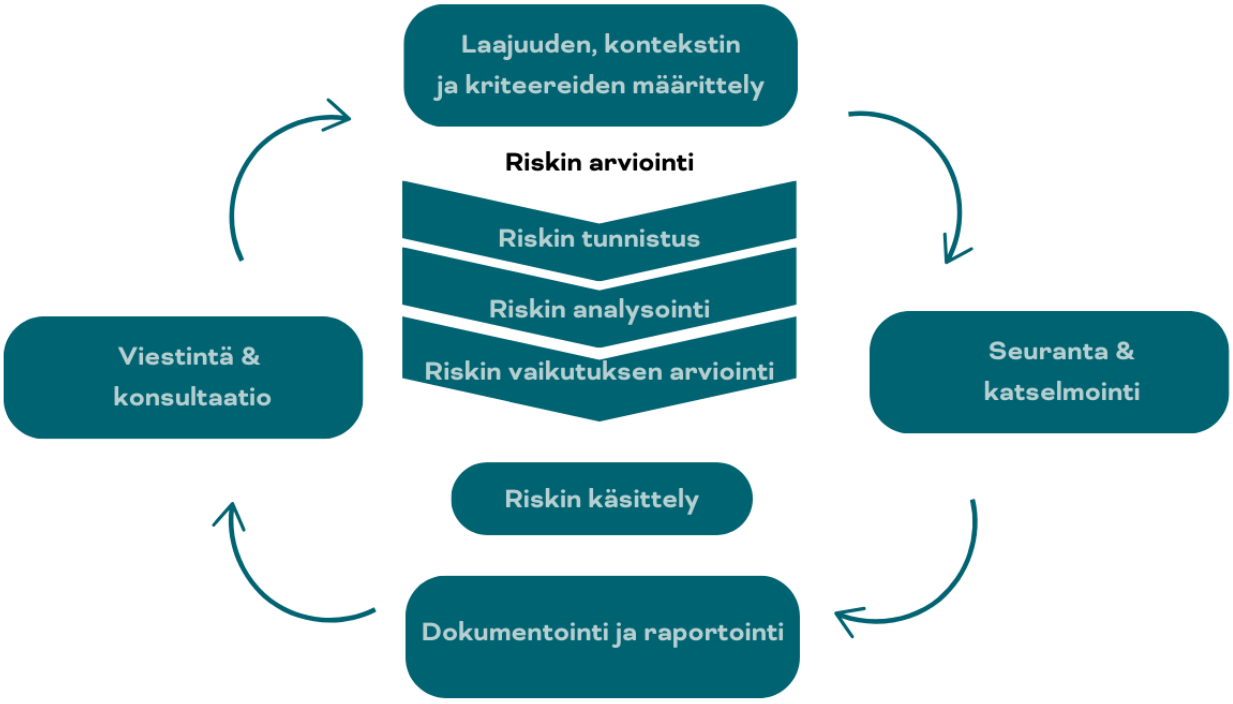
Riskienhallinta on prosessi, joka sisältää relevanttien riskien tunnistuksen, analysoinnin, vaikutusten arvioinnin ja käsittelyn. Tunnistukseen sisältyy potentiaalisten haavoittuvuuksien ja ongelmien pohdinta. Tällöin tarkastellaan skenaarioita tai tekijöitä, joita hyökkääjät voisivat käyttää hyväkseen tai virheitä, joita työntekijät saattaisivat tehdä. Tämän jälkeen analysoidaan ja arvioidaan riskien vaikutukset toteutuessaan, jotta saadaan riskitaso määriteltyä. Kun riskitaso on määritelty, on päätettävä paras toimintatapa välttääkseen se. Riskin käsittelyvaiheessa mietitään mikä olisi paras strategia hallita riskejä. Riskien käsittelyyn voidaan käyttää esimerkiksi seuraavaa neljää strategiaa:

1. Riskin pienentäminen tai vähentäminen on yleisin strategia. Tällöin on mietittävä tarvittavat kontrollit riskin pienentämiseksi.

2. Riskin jakamisella voidaan jakaa riski toisen osapuolen kanssa, esimerkiksi sopimuksilla tai hankkimalla vakuutus.

3. Riskin välttämisellä tarkoitetaan sellaisten toimien välttämistä, jotka aiheuttavat riskin. Esimerkiksi jos luvattoman pääsyn riski työntekijöiden kannettaviin tietokoneisiin on korkea, on parempi kieltää niiden vienti toimiston ulkopuolelle.

4. Riskin hyväksyminen tarkoittaa sitä, että organisaatio päättää olla tekemättä toimia ja hyväksyä, että riski voi toteutua. Tämä voi johtua esimerkiksi siitä, että riskin vaikutukset toteutuessaan eivät olisi niin merkittävät tai jos riskin hallinta olisi kustannuksiltaan liian suuri. (Adarsh & Greeshma, 2023, luku 4)



Kuva 5 Riskienhallintaprosessi (mukaillen Adarsh & Greeshma, 2023, luku 4)

2.5 Tietoturvapolitiikat ja ohjeet

ISO/IEC 27001 standardi vaatii, että ylin johto on laatinut tietoturvapolitiikan, joka on saatavana dokumentoituna, on koko organisaation tiedossa ja tarvittaessa myös sidosryhmien saatavilla.

Tietoturvapolitiikassa on oltava tietoturvatavoitteet tai perustat niiden asettamiselle. Tietoturvapolitiikan tulisi myös osoittaa sitoutuminen tietoturvavaatimusten täyttämiseen sekä hallintajärjestelmän jatkuvaan parantamiseen. (Suomen Standardoimisliitto SFS, 2022, 7)

Tietoturvapolitiikka on joukko sääntöjä, jotka auttavat määrittelemään hyväksyttävän turvatason organisaatiossa. On äärettömän tärkeää, että organisaation kaikki työntekijät, järjestelmien käyttäjät ja muut yhteistyökumppanit noudattavat näitä. Tietoturvapolitiikka koostuu ohjeista ja toimenpiteistä, joilla varmistetaan organisaation tietoturva. Jokaisella organisaatiolla on erilaiset tietoturvapolitiikkansa, jotka yleensä kattavat työntekijöiden vastuun, turvallisuuden valvonnan, tavoitteet ja päämäärät sekä hallinnoinnin. Nämä politiikat selittävät, miten yrityksen tietovarantoja suojellaan ja jaetaan tai miten tärkeitä toimintoja suojataan. On myös välttämätöntä, että tietoturvan vaatimukset määritellään. Tällaisen arvioinnin tulokset auttavat organisaatiota päättämään, millaisia hallinnollisia toimia ja oikeuksia on sovellettava. Tulokset myös ohjaavat organisaatioita sopivien hallintakeinojen käyttöönotossa tietoturvauhkia vastaan suojautuessaan. Tarkemmat ohjeet esimerkiksi siitä, miten käyttäjätilit luodaan, miten niitä hallinnoidaan, mitä tehdä, jos salasana unohtuu tai se täytyy vaihtaa ja miten uudet salasanat määritellään, on selitettävä erillisissä tietoturvaohjeistuksissa. (Yeniman Yildirim ym., 2011, 360–361)

Tehokkaan tietoturvapolitiikan kehittämiseen ja toteuttamiseen liittyvät prosessit ovat parhaimmillaankin haastavia. Kirjallisuudessa kuvataan se, millaisen tietoturvapolitiikan rakenteen ja sisällön tulisi olla, mutta siinä ei anneta yksityiskohtaista kuvausta tietoturvapolitiikan kehittämisprosessista. Tämän vuoksi politiikan laatijoilla on vain vähän ohjeita siitä, miten heidän tulisi toimia. Monet organisaatiot saattavat käyttää toisten organisaatioiden politiikkoja tai kaupallisesti saatavilla olevia tai internetistä löytyviä malleja, jotka eivät välttämättä sovi oman organisaation erityistarpeisiin eivätkä ne näin ollen torju erityisiä turvallisuusuhkia, joita kyseinen organisaatio kohtaa. Tietoturvapolitiikan kehittämisen ja toteuttamisen prosessi ei ole yksinkertainen, vaan siihen vaikuttavat monet tekijät, kuten sääntely, uusien teknologioiden monimutkaisuus ja erilaiset sisäiset tai ulkoiset uhkat. (Flowerday & Tuyikeze, 2016, 170)

2.6 Sisäinen auditointi

ISO27001-standardi vaatii, että organisaatiot toteuttavat suunnitelluin aikavälein sisäisiä auditointeja tietoturvan hallintajärjestelmälleen varmistuakseen siitä, että se on sekä omien vaatimusten että ISO27001-standardin vaatimusten mukaan toteutettu ja ylläpidetty. Organisaatioiden on määriteltävä itse auditointiohjelma ja suunniteltava auditointien taajuus, menetelmät, auditointikriteerit ja soveltamisala sekä vastuut ja raportointityyli. Sisäisen auditoijan on oltava sellainen, joka voi varmistaa auditoinnin objektiivisuuden ja puolueettomuuden. Auditointien löydökset on myös

raportoitava johdolle ja raporteista on säilytettävä dokumentoitua tietoa. (Suomen Standardisoimisliitto SFS ry, 2022, 13)

Sisäiset auditoinnit auttavat tunnistamaan ongelmia, jotka voivat vahingoittaa organisaatiota. Auditointiohjelman on katettava kaikki standardin pakolliset vaatimukset sekä kaikki hallintakeinot, jotka organisaatio on sisällyttänyt valmistelemaansa soveltuvuuslausuntoon (SoA). Sisäisen auditoinnin tavoitteena on myös auttaa tunnistamaan tietoturvan hallintajärjestelmän parantamisen mahdollisuuksia. (Adarsh & Greeshma, 2023, luku 5)

2.7 Johtaminen ja johdon sitoutuminen tietoturvaan

Vaikka on tärkeää tarjota tietoturvakoulutusohjelmia ja toteuttaa tietoturvapolitiikkaa, ne eivät yksin riitä, kuten mediassa toistuvasti raportoidut tietoturvamurrot ovat osoittaneet. Ylimmän johdon aktiivinen osallistuminen ja oikeanlainen organisaatiokulttuuri ovat avainasemassa työntekijöiden asenteiden ja käyttäytymisen hallinnassa. Sen sijaan, että keskityttäisiin vain teknologiaan tai politiikkoihin, tietoturvaohjelmien tulisi keskittyä muuttamaan työntekijöiden asenteita ja käyttäytymistä. (Hu, Dinev, Hart & Cook. 2012, 648) Johdon omat toimintatavat heijastavat usein sen, miten yrityksessä suhtaudutaan tietoturvaan. Onnistunut tietoturvariskien hallinta edellyttää sen, että yrityksen johto on sitoutunut riskien hallintaan ja on itse perehtynyt tietoturvakäytäntöihin. (Laaksonen, Nevasalo & Tomula, 2006, 258)

Tietoturvapolitiikat ovat ylimmän johdon ilmaus siitä, miten suojata tietojärjestelmiä ja varmistaa arkaluonteisten tietojen turvallisuus. Ylhäältä alas -lähestymistavalla tarkoitetaan turvatoimien määrittämistä ja toteuttamista ylimmän johdon ohjeiden mukaisesti. Organisaatiot, jotka toteuttavat tietoturvaohjelmansa ylhäältä alas hyötyvät ohjelmasta enemmän, koska se on linjassa tietoturvatavoitteiden kanssa ja on suunniteltu niiden mukaisesti, mahdollistaen resurssien tehokkaamman suojaamisen. Vaikka on tärkeää tunnistaa turvallisuusongelmat henkilöstön tasolla, tietoturvaohjelman tulee olla ylimmän johdon ohjauksessa, jotta se voi tukea organisaation liiketoimintatavoitteita. Kun riski havaitaan, monia tekijöitä on otettava huomioon määritettäessä, miten siihen reagoidaan organisaation tasolla, koska se toteutuessaan saattaa vaikuttaa muihin osastoihin, raportointiin, sääntelyyn, sopimuksiin tai asiakkaisiin. Alhaalta ylös -lähestymistapa voi tuntua suoraviivaisemmalta, mutta se voi johtaa resurssien tehottomaan käyttöön ja suurempiin turvallisuusriskeihin. Oireperusteinen korjaaminen keskittyy tietoturva-aukkojen oireiden tekniseen korjaamiseen eikä niiden syihin. Esimerkiksi, jos penetraatiotestauksen yhteydessä havaitaan, että palvelimella on vanhentunut ohjelmisto, yleinen ratkaisu on vain päivittää se ja jatkaa seuraavaan tehtävään. Tämä "penetrate-patch-and-proceed" -lähestymistapa ei kuitenkaan estä samanlaisia ongelmia tulevaisuudessa, koska se ei käsittele ongelman perimmäistä syytä. Parempi lähestymistapa olisi

ymmärtää ja korjata ongelman juurisyy, joka voi olla henkilöstön koulutuksen puute tai puutteelliset käytännöt. (Landoll, 2016, luku 1.2)

Puhakaisen ja Siposen (2010, 770–775) tutkimustuloksissa korostui, että tietoturvakäytäntöjen noudattamisen edistämiseksi olisi tärkeää varmistaa ylimmän johdon näkyvä tuki. Johdon olisi säännöllisesti korostettava tietoturva-asioita viestinnässään, kuten johdon katselmuksissa, intranetissä tai henkilöstölehdissä. Ylimmän johdon tuki tulee näkyväksi myös, kun johtajat itse noudattavat tietoturvakäytäntöjä esimerkillisesti. Tutkijat havaitsivat, että yksi pääsyy siihen, miksi työntekijät eivät noudattaneet sähköpostien salausta koskevia tietoturvaohjeita, oli toimitusjohtajan koettu passiivisuus tietoturva-asioissa. Kun toimitusjohtaja muutti asennettaan tietoturvaa kohtaan ja alkoi aktiivisesti osallistua tietoturva-asioihin, työntekijöiden asenteissa tietoturvakäytäntöjen noudattamista kohtaan tapahtui havaittavia muutoksia. Myös työntekijöiden osallistuminen tietoturva-aiheisiin keskusteluihin ja aloitteisiin lisääntyi.

Myös tutkijat Hu, Dinev, Hart & Cook (2012, 647–648) tutkivat ylimmän johdon ja organisaatiokulttuurin vaikutuksia ihmisten tietoturvakäyttäytymiseen. Heidän tutkimuksensa osoitti, että näistä ylimmän johdon osallistuminen oli merkittävin ulkoinen tekijä, joka muokkasi työntekijöiden käyttäytymistä. Joissakin organisaatioissa, erityisesti niissä, joissa IT ei ole ydinliiketoimintaa, ylimmällä johdolla on tapana siirtää tietoturvaan liittyvät päätökset ja vastuut alemman tason IT-päälliköille, koska he uskovat, että heillä on parhaat asiantuntijat varmistamassa korkeimman tason tietoturvaa. Tutkimuksen tulokset kuitenkin korostavat ylimmän johdon aktiivisen ja näkyvän osallistumisen merkitystä. Ylimmän johdon rooli organisaatiokulttuurin muokkaamisessa on erittäin tärkeä. Johdon osallistuminen ei ainoastaan muuta organisaation kulttuuria, vaan vaikuttaa myös suoraan työntekijöiden käsityksiin, mikä puolestaan vaikuttaa positiivisesti heidän aikomukseensa noudattaa tietoturvakäytäntöjä.

ISO/IEC 27001-standardi asettaa myös useita vaatimuksia johtajuudelle. Ylimmän johdon on pystyttävä osoittamaan sitoutumisensa tietoturvallisuuden hallintajärjestelmään ja sen jatkuvaan parantamiseen. Tietoturvapolitiikan laatimisen lisäksi ylimmän johdon on asetettava tietoturvatyölle tavoitteet ja varmistettava, että ne ovat linjassa organisaation strategian kanssa. Heidän on varmistettava, että hallintajärjestelmän vaatimukset integroidaan organisaation muihin prosesseihin, taattava hallintajärjestelmälle tarvittavat resurssit ja varmistettava, että tietoturvan kannalta keskeisten henkilöiden vastuut ja valtuudet määritellään ja tiedotetaan organisaatiossa. Johdon on korostettava tietoturvallisuuden hallinnan merkitystä viestinnässään varmistaakseen, että vaatimuksia noudatetaan ja että hallintajärjestelmä saavuttaa halutut tulokset. Lisäksi heidän tulee ohjata ja tukea henkilöstöä tietoturvallisuuden tehostamisessa ja kannustaa muita johtajia omilla vastuualueillaan. Ylimmän johdon on arvioitava tietoturvan hallintajärjestelmän toimivuutta säännöllisesti, tyypillisesti

ennalta määrätyin väliajoin järjestettävässä johdon katselmointikokouksessa. Johdon katselmoinnissa tulee käsitellä aiemmista johdon katselmoinneista seuranneet toimenpiteet, tietoturvan hallintajärjestelmään liittyvät sisäiset ja ulkoiset muutokset, sidosryhmien palaute, mittaus- ja seurantatulokset, auditointien havainnot sekä riskienhallintasuunnitelma. Katselmoinnin perusteella tehdään päätöksiä jatkuvista parannuksista ja mahdollisista muutoksista hallintajärjestelmään. Ennen johdon katselmointia tulisi myös suorittaa tietoturvan hallintajärjestelmän sisäinen auditointi, sillä sen löydökset ovat myös olennainen osa johdon katselmointia. Katselmoinnin tulokset on dokumentoitava kokousmuistioon ja säilytettävä näyttönä auditoijia varten. (Suomen Standardoimisliitto SFS, 2022, 7–8; Adarsh & Greeshma, 2023, luku 5)

2.8 Tietoturvakoulutukset ja tietoisuuden lisääminen

Niin kirjallisuudessa kuin ISO/IEC 27001 -standardissa ollaan samaa mieltä siitä, että tietoturvaviestinnän, -koulutuksen ja -tietoisuuden lisäämisellä voidaan parantaa organisaatioiden tietoturvaa ja tietoturvakulttuuria. Tässä kappaleessa esitellään tietoturvakoulutukseen liittyviä teorioita sekä käytännön vinkkejä tietoturvallisuuden kouluttajille organisaatiossa.

Yleisellä tietoisuudella tietoturvasta on vaikutusta niin henkilöstön asenteeseen kuin myös siihen, mitä uskotaan tietoturvakäytäntöjen noudattamattomuudesta seuraavan. Työntekijöiden käsitystä siitä, että käytäntöjen noudattaminen haittaa työtehtävien suorittamista, voidaan vähentää lisäämällä tietoturvatietoisuutta. Tämä parantaa myös työntekijöiden itsetehokkuutta. Organisaatioiden tulisi myös huolehtia siitä, että hyvä tietoturvakäyttäytyminen ei kilpaile työtehtävien suorittamisen kanssa. Tämä tapahtuu allokoimalla työntekijöiden aikaa myös tietoturvavaatimusten täyttämiselle. (Bulgurcu, Cavusoglu & Benbasat, 2010, 523–540)

Tietoturvakoulutuksen tavoitteena on varmistaa, että ihmiset toimivat tavalla, joka suojaa organisaation tiedot tarkoituksenmukaisesti ja kustannustehokkaasti. Koulutuksen tulisi pohjautua tietoturvapolitiikkaan, toimintaohjeisiin ja prosessikuvauksiin. Myös johdon katselmoinneissa tai auditoinneissa mahdollisesti tunnistetut tietoturvakäyttäytymisen ongelmat tulisi huomioida koulutuksen suunnittelussa. Henkilöstön sisäiset ja ulkoiset motivaattorit vaikuttavat suuresti koulutuksen tehokkuuteen ja tietoturvakoulutuksissa onkin tärkeää ottaa huomioon eri motiivien vaikutus oppimisprosessiin. (Laaksonen ym., 2006, 254) Sisäisistä ja ulkoisista motiiveista kerrotaan lisää luvussa 2.13.

Organisaatioiden tulisi kouluttaa työntekijöitään säännöllisesti ja useissa yrityksissä tämä tarkoittaa vähintään tietoturvapolitiikan ja ohjeistuksen vuosittaisen läpikäynnin. Koulutusta on tärkeää järjestää erityisesti silloin, kun tietoturvassa tapahtuu suuria muutoksia tai kun jokin teema on erityisen ajankohtainen. On myös erityisen tärkeää, ettei koulutusta koeta pakollisena taakkana, jonka

työntekijät haluaisivat välttää. (Laaksonen ym. 2006, 256; 259) Beyerin ja Brummelin (2015, 6; 18) mukaan tehokkaan tietoturvakoulutuksen järjestäminen on vaikeaa sillä koulutukset ovat usein liian yleisluontoisia ja satunnaisia. Organisaatioiden on tunnistettava loppukäyttäjien tiedon puutteet ja tarjottava kohdennettua tai roolikohtaista koulutusta, jotta koulutus olisi tehokasta. Puhakaisen & Siposen (2010, 774–775) tutkimustuloksissa korostui se, että koulutuksen tulisi olla systemaattista, sillä kertaluontoiset koulutukset eivät yksinään riitä. Koulutusohjelmat ovat hyödyllisiä taitojen kouluttamiseksi ja tietoturvallisuusasenteiden parantamiseksi ja organisaatioissa olisi oltava prosessit, jotka tekevät tietoturvaviestinnästä jatkuvaa toimintaa.

Oppimisen tapa on yksilöllinen ja tämän takia on tärkeää tunnistaa paras tapa kullekin henkilölle. Tietoturvakoulutuksen suunnittelussa tulisi ottaa huomioon koulutettavien osaamistaso ja räätälöidä sisältö ja menetelmät sen mukaisesti. Koulutuksen harjoitustehtävät voidaan perustaa työntekijän todellisiin työtehtäviin, jolloin käytännön soveltamisen kautta oppiminen on tehokkaampaa. Perinteisesti tietoturvapolitiikan ja ohjeiden laatimisen jälkeen edellytetään henkilöstöä lukemaan nämä. Vaihtoehtona tälle voidaan käyttää monivalintatenttejä tai järjestää kilpailuja tietoturvatietouden testaamiseksi. (Laaksonen ym., 2006, 257–258) Puhakaisen & Siposen (2010, 774–775) mukaan kyselyt ja haastattelut ovat hyödyllisiä koulutuksia suunniteltaessa. Kyselyt ovat hyödyllisiä anonyymin tiedon keräämiseen, kun taas haastattelut auttavat saamaan syvällisen ymmärryksen henkilöiden näkemyksistä. Varsinaisissa koulutuksissa työntekijät tulisi jakaa eri koulutusryhmiin heidän tietotasonsa mukaan, jotta voidaan ottaa huomioon oppijoiden aiempi tietotaito.

Tietoturvan suunnittelu, toteutus ja tietoturvakoulutusten järjestämisen koordinointi ovat yleensä organisaatioissa IT-osaston vastuulla. Vaikka he eivät itse järjestäisi kaikkea koulutusta, heidän tulisi olla mukana suunnittelussa. Tämä takaa sen, että yrityksen koulutukset ovat yhtenäisiä ja varmistaa, että ne noudattavat organisaation tavoitteita ja käytäntöjä. IT-osaston työntekijät ovat usein teknisesti kouluttautuneita ja suuntautuneita ihmisiä, jotka eivät ole parhaimpia henkilöitä viestimään tietoturvasta henkilöstölle. (Laaksonen ym. 2006, 259; Järvinen, 2022, 32) Tyypillisesti IT-asiantuntijoilla ei ole erityistä osaamista kouluttamisessa ja usein organisaation koulutusvelvollisuuksien täyttymisestä huolehtiminen jää HR-osaston vastuulle. HR-asiantuntijat ymmärtävät koulutettujen työntekijöiden merkityksen tietoturvariskien hallinnassa ja heillä on kyky löytää ratkaisuja organisaation haasteisiin. Näiden haasteiden ratkaiseminen vaatii monitieteellistä lähestymistapaa, jolloin olisi hyvä, että IT-asiantuntijat ja HR-asiantuntijat tekisivät yhteistyötä, sillä IT-asiantuntijat osaavat tunnistaa organisaatioiden haavoittuvuuksia, kun taas HR-asiantuntijoilla on vastuu puuttua henkilöstön koulutuksen puutteisiin. HR-asiantuntijoilla on laajan vastuualueensa vuoksi myös mahdollisuus hankkia organisaatiotukea ja koota yhteen asiantuntijoita. (Beyer & Brummel, 2015, 14; 18)

Oppimisen voi jakaa ymmärtämiseen ja harjaantumiseen. Ymmärryksen saavuttaminen on yksilöllistä ja siihen voi vaikuttaa monin eri tavoin, kuten selityksillä, käytännön esimerkeillä tai kuvilla. Tehokkainta on tarjota eri tapoja ymmärtämisen tueksi. Harjaantuminen taas perustuu kokeilun kautta kokemukseen, joka paranee ajan myötä. Ennen kokeilua tarvitaan kuitenkin ymmärrystä tehtävästä. Tietoturvallisuudessa on tärkeää, että työntekijät ymmärtävät toimiensa vaikutukset yritykseen, sillä kokeilut voivat johtaa ei-toivottuihin seurauksiin, vaikka niistä oppisikin. Käytännön esimerkit auttavat henkilöstöä ymmärtämään tietoturvapolitiikkoja ja -ohjeita paremmin. Jos ohjeet eivät ole konkreettisia, tietoturvallisuus ei saavuta haluttua tasoa. Esimerkit kannustavat keskustelemaan siitä, miten ja miksi tietoturvaohjeita tulisi noudattaa eri tilanteissa. Työntekijöiden toimintatapojen tulisi olla yhtenäisiä. Keskustelulla ja kokemuksien jakamisella pyritään määrittelemään yhteiset pelisäännöt ja kehittämään parhaimmat toimintatavat. (Laaksonen ym., 2006, 255–257) Koulutuksen oppimistehtävien olisi hyvä olla henkilökohtaisesti merkityksellisiä koulutettaville, jotta he ymmärtävät todelliset seuraukset itselleen ja muille. Koulutuksessa voidaan käyttää esimerkiksi oikeita tietoja sisältäviä sähköpostiviestejä ja keskustella niiden salaamattomana lähettämisen seurauksista. Kognitiivista pitkäaikaista oppimista voidaan edistää syy-seuraus-ajattelumallien avulla. Tämä saavutetaan antamalla työntekijöiden pohtia mahdollisia ei-toivottuja seurauksia omista toimistaan. Esimerkiksi salaamattoman sähköpostin lähettäminen voi johtaa luottamuksellisen tiedon vuotamiseen kilpailijalle, mikä puolestaan voi johtaa kilpailuedun menettämiseen. (Puhakainen & Siponen, 2010, 774–775)

Integroimalla tietoturvakoulutus muihin organisaation sisäisiin viestintäkanaviin varmistetaan se, etteivät työntekijät näe tietoturvaa heidän työtehtävistään tai organisaation liiketoiminnasta erillisenä asiana. Henkilöstöä tulisi rohkaista koulutusistuntojen tai muun jatkuvan tietoturvaviestinnän yhteydessä raportoimaan tietoturvaongelmista ja osallistumaan tietoturvakäytäntöjen kehittämiseen. (Puhakainen & Siponen, 2010, 774–775) Henkilöstön ei tarvitse tietää kaikkea tietoturvasta, kunhan he ymmärtävät omaan työtehtäväänsä liittyvät riskit ja keinot riskien minimoimiseksi. Suurimmat virheet koulutuksessa tehdään usein siinä, että työntekijöille ei korosteta tarpeeksi syitä toimintatapojen taustalla, mikä saa työntekijät pitämään ohjeita byrokraattisena päätöksenä, joka haittaa työntekoa. (Laaksonen ym., 2006, 254–255)

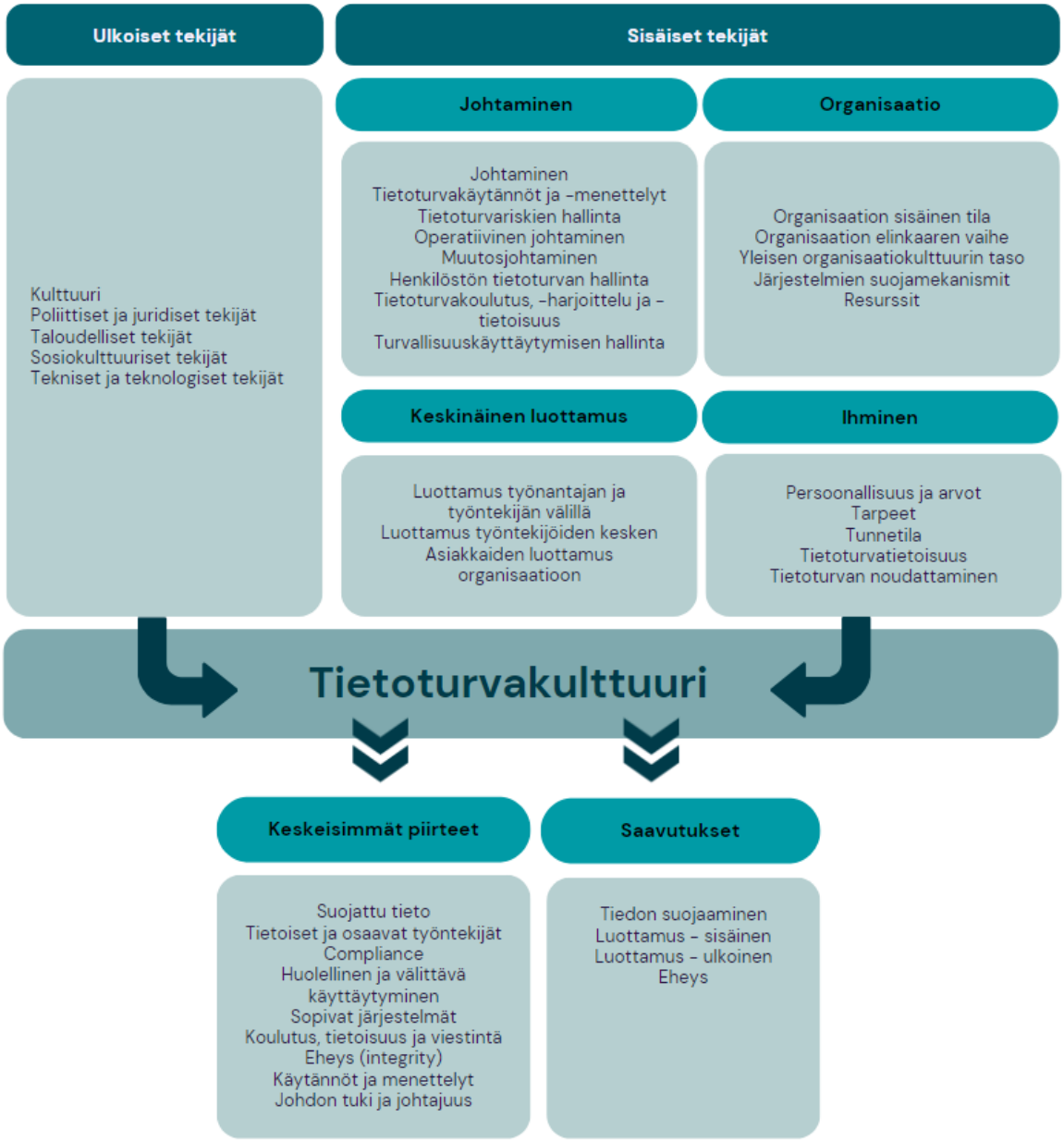
2.9 Tietoturvakulttuuri

Da Veiga, Astakhova, Botha & Herselman (2020, 20) määrittelivät kattavassa kirjallisuuskatsauksessaan tietoturvakulttuurin kuvaukseksi sitä, kuinka organisaation ihmiset suojelevat tietoa, noudattavat tietoturvasääntöjä ja -ohjeistuksia, ymmärtävät tietoturvan merkityksen ja kuinka he saavat koulutuksen ja viestinnän kautta tietoa keskeisistä tietoturva-asioista. Ajan myötä nämä käytännöt muuttuvat organisaation normeiksi ja arkipäiväiseksi toiminnaksi. Tämä pohjautuu työntekijöiden

arvoihin, uskomuksiin, tietoon sekä heidän suhtautumiseensa tietojen suojaamiseen. Tietoturvakulttuurin muovautumiseen vaikuttavat **Virhe. Viitteen lähdettä ei löytynyt.** luetellut sisäiset sekä ulkoiset tekijät ja kulttuuria tukee asianmukainen ICT-infrastruktuuri. Kulttuurin tavoitteena on rakentaa luottamusta kaikkien sidosryhmien välillä.

Darcyn & Greenen (2014, 477; 484-486) empiirinen tutkimus tarkasteli turvallisuuskulttuurin, työtyytyväisyyden ja organisaation tuen vaikutusta tietoturvakäytäntöjen noudattamiseen. Sekä turvallisuutteen liittyvät että yleiset työympäristötekijät vaikuttivat työntekijöiden aikomukseen noudattaa käytäntöjä. Tuloksissa oli viitteitä myös siitä, että työntekijän asema, toimiala ja työsuhteen kesto saattavat vaikuttaa. Tietoturvakulttuuriin vaikuttavat ylimmän johdon sitoutuminen, tehokas tietoturvaan liittyvä viestintä ja tietoturvan valvontatoimet. Valvontatoimet, kuten työntekijöiden internetin käytön tai verkkotoiminnan seuranta ja tietoturva-auditoinnit ovat tapa valvoa tietoturvapolitiikan toteutumista ja nämä viestivät työntekijöille, että organisaatio suhtautuu vakavasti tietoturvaan, eikä hyväksy poikkeamia määritellyistä tietoturvakäytännöistä ja menettelyistä. Tutkijat havaitsivat, että työntekijöiden työtyytyväisyys vaikuttaa heidän aikomukseensa noudattaa tietoturvakäytäntöjä. Työntekijät ovat halukkaampia käyttäytymään positiivisesti ja hyödyllisesti organisaatiossa, jos he ovat tyytyväisiä. Tämän takia monialainen lähestymistapa, joka ulottuu IT-osaston ulkopuolelle, voi olla hyödyllinen. HR:n työtyytyväisyyden edistämisaloitteet voivat siis parantaa tietoturvaa. Odotusten vastaisesti tutkimus myös osoitti, että työntekijät, jotka kokivat saavansa vahvaa tukea organisaatiolta, saattoivat laiminlyödä tietoturvakäytäntöjä, koska he ajattelivat IT-osaston hoitavan tietoturvaongelmat, jolloin heidän oma roolinsa ei ole kriittinen. Tämä voi johtua siitä, että ihmiset ottavat enemmän riskejä, kun he kokevat olevansa turvassa tietyllä alueella. Organisaatioiden tulisi korostaa, että tietoturva on jokaisen työntekijän vastuu ja riippuvainen työntekijöiden toimista. Havaittu yhteys turvallisuuskulttuurin ja tietoturvakäytäntöjen noudattamisen aikomuksen välillä vahvistaa ajatusta siitä, että turvallisuuskulttuuri on tärkeä tekijä tietoturvan hallintajärjestelmien jalkauttamisen tukemisessa.

Aiemmin mainitun Hun ym. (2012, 647) tutkimuksen mukaan sääntöihin ja tavoitteisiin keskittyvällä kulttuurilla on merkittävä vaikutus työntekijöiden käsityksiin tietoturvasta. Tutkimuksen tulokset viittasivat siihen, että organisaatiokulttuuri, jossa tavoitteet, säännöt ja käytännöt määritellään selkeästi ja niitä kunnioitetaan, voi vaikuttaa positiivisesti työntekijöiden aikomukseen noudattaa tietoturvakäytäntöjä. Tällaisessa kulttuurissa työntekijöitä arvostetaan ja palkitaan kun he saavuttavat asetetut tavoitteet ja noudattavat sääntöjä, kun taas tietoturvakäytäntöjen rikkomuksista rangaistaan.



Kuva 6 Organisaation tietoturvakulttuurin malli (mukaillen da Veiga ym., 2020, 20)

2.10 Tietoturvan toteutumisen valvonta, seuranta ja mittaus

Mittarit ovat arvokkaita työkaluja, jotka auttavat edistämään muutosta ja muuttamaan yrityskulttuuria, kunhan niitä käytetään oikein. Mittareiden tulisi olla yksinkertaisia ja datan tulisi olla helppo kerätä. Tarkoituksettoman datan käyttäminen ja jakaminen ei ole järkevää. Eri asiat ovat tärkeitä eri kohderyhmille. Liiketoimintajohtajat haluavat yksinkertaisia vastauksia, kuten tiedon siitä, miten hyvin organisaatio pärjää verrattuna kilpailijoihin. IT-johtajat ja tietoturvajohtajat taas kaipaavat teknisiä yksityiskohtia ja voivat haluta tietoja, jotka eivät mitenkään kiinnosta muita ryhmiä. Mittarit kannattaa siis räätälöidä kohderyhmien mukaan. Mittareiden ei tulisi rajoittua ainoastaan

liikennevalotyyppisiin laadullisiin luokituksiin. Määrällisiä mittareita on suositeltavaa hyödyntää aina kun se on mahdollista. Yhdistämällä sekä laadulliset että määrälliset mittarit saavutetaan tehokkain lähestymistapa. Parhaimmat mittarit kertovat tarinan, näyttävät trendin, ohjaavat toimintaa, kouluttavat tai tiedottavat. (Brown, 2022, 233)

Tietoturvallisuuden mittaamisen tavoitteena on toiminnan jatkuva parantaminen ja tehokas johtaminen. Mittaaminen auttaa tunnistamaan ja korjaamaan tietoturvaan liittyviä heikkouksia ja aukkoja sekä varmistamaan, että organisaation suojaustoimenpiteet ovat ajantasaisia ja oikein priorisoituja. Tietoturvallisuuden säännöllisellä mittaamisella voidaan saada arvokasta ja vertailukelpoista tietoa tietoturvallisuuden tilanteesta. Mittaus auttaa arvioimaan, mihin toimiin kannattaa jatkossa investoida ja se auttaa esimerkiksi tehostamaan henkilöstön koulutusta. Tietoturvallisuuden mittaaminen on haastavaa, koska se voi perustua tekijöihin, jotka ovat epävarmoja tai ennalta arvaamattomia, kuten ihmisten käyttäytyminen, tuntemattomat hyökkäysmenetelmät ja järjestelmien tietoturva-aukot. Tämän epävarmuuden vuoksi mittaustulokset voivat olla epäluotettavia, jos mittarit ovat herkkiä näille tekijöille. Hyvä mittari näyttää kehityksen suunnan. Kuvassa 7 on lueteltuna esimerkkimittareita eri tavoitteisiin liittyen. Työntekijöiden käyttäytymisen mittaaminen on keskeinen tapa arvioida hallinnollisten toimien tehokkuutta. Mittaamisen kanssa on tärkeää, että ei aiheuteta negatiivisia tuntemuksia tai syyllistetä henkilöstöä. Tulosten pitäisi heijastaa suurempaa joukkoa, pienemmissä yrityksissä kaikkia työntekijöitä ja suuremmissa vakio-otosta vertailtavuuden varmistamiseksi. Esimerkkejä henkilöstön toiminnan mittaukseksi ovat esimerkiksi tiedon luokittelun ja käsittelyn tarkistaminen, työasemien lukitsemisen tarkastaminen tai tietoturvatietämyksen taso esimerkiksi kyselyitä apuna käyttäen. (Laaksonen ym., 2006, 268–272; 278–279)

Liiketoimintanäkökulma		Sidosryhmänäkökulma	
Tavoitteet	Esimerkkimittarit	Tavoitteet	Esimerkkimittarit
Liiketoiminnan tarpeiden ja tietoturvaratkaisujen yhdistäminen Tuottavuuden maksimointi tietoturvariskien optimaalisella hallinnalla Käytön helppouden maksimointi	Tietoturvaprojektien yhteys liiketoiminnan vaatimuksiin Kuvatut liiketoimintatarpeet tietoturvallisuuden osalta Liiketoiminnan tavoitteet, joita tietoturvallisuus tukee	Sidosryhmien huomioiminen ja tarpeiden tyydyttäminen Asiakas- ja muiden sidosryhmien tyytyväisyys Vaatimustenmukaisuus Sujuva tiedonkulku	Sidosryhmäkyselyiden tulokset Tietoturvaan liittyvien valitusten määrä Ylimmän johdon osallistuminen tietoturvaan liittyviin päätöksiin ja projekteihin Vaatimustenmukaisuus

Toiminnallisen tehokkuuden näkökulma		Tulevaisuuden näkökulma	
Tavoitteet	Esimerkkimittarit	Tavoitteet	Esimerkkimittarit
Prosessien kehittyneisyys Selkeät roolit ja vastuut Johdonmukaisen heikkouksien tunnistaminen ja toimintatapojen kehittäminen	Prosessien kypsyystaso Tietoturvaorganisaation rakenne ja vastuut Yrityksen ylimmän johdon osallistuminen tietoturvaa koskeviin päätöksiin Eri standardien ja viitekehyksien kattamien prosessien määrä	Henkilöstön osaamisen hyvä hallinta Työntekijöiden työtyytyväisyys Riittävä tietoturvaosaamisen määrä Tekniikan ja ympäristön tilan seuraaminen	Tietoturvakoulutusten määrä ja sen seurauksena lisääntynyt tietoturvatietoisuus Yrityksen johdolle pidettyjen tietoturvaesitysten ja koulutusten määrä Henkilöstön tietoturvasertifikaatit Tietoturvafoorumeihin ja yhteistyöelimiin osallistuminen

Kuva 7 Tietoturvallisuuden mittareita eri näkökulmista (Laaksonen ym. 2006, 278)

2.11 Pelotteet, sanktiot ja neutralisointitekniikat

On vaikea kuvitella organisaatiota, jossa tietoturvaohjeiden vastaisesta toiminnasta ei olisi minkäänlaisia seuraamuksia. ISO/IEC 27001-standardi jopa vaatii, että organisaatiolla olisi oltava muodollinen ja henkilöstön tiedossa oleva kurinpitoprosessi niitä tilanteita varten, kun joku on syyllistynyt tietoturvapolitiikan rikkomukseen. (Suomen Standardisoimisliitto SFS ry, 2022, 19)

Peloteteoria on yksi hallitsevista teoreettisista näkökulmista tietoturvakäytäntöjen noudattamisen tutkimuksissa ja sitä onkin tutkittu vaihtelevin tutkimustuloksin. Peloteteoria juontaa juurensa kriminologiasta. Se perustuu ajatukseen siitä, että ihmiset ovat itsekkäitä ja pyrkivät maksimoimaan omia hyötyjään ja minimoimaan haittojaan, kuten esimerkiksi rangaistuksista aiheutuvia haittoja. Teorian mukaan ihminen arvioi rangaistuksen haitallisuutta miettimällä, kuinka todennäköinen ja vakava se on. Suurin osa tutkimuksista on tarkastellut virallisten sanktioiden roolia. Virallisia sanktioita ovat esimerkiksi varoitukset, sakot, työpaikan menettäminen tai rikossyytteet. Viime aikoina on kuitenkin alettu myös tarkastelemaan epävirallisten sanktioiden vaikutuksia. Näitä ovat esimerkiksi maineen ja luottamuksen menetys, häpeä tai menetetty mahdollisuus edetä organisaatiossa. Tutkijat ovat todenneet, että nämä ovat tehokkaita keinoja estämään ei-toivottua käyttäytymistä. (Vance, Siponen & Straub, 2020, 1–3; Hengstler, Kuehnel, Masuch, Nastjuk & Trang, 2023, 6)

Hengstler ym. (2023, 19) toteuttivat tutkimuksen, joka tarkasteli rangaistusten ja sanktioiden vaikutusta työntekijöiden haluun noudattaa tietoturvasääntöjä. Tutkijat kehittivät mallin, joka perustuu peloteteoriaan ja analysoivat aineistoa, joka saatiin 263 henkilöstä. Tutkijat jakoivat työntekijät

kolmeen ryhmään: (1) niihin, jotka ovat taipuvaisia tietoturvasääntöjen rikkomiseen, (2) niihin, jotka yleensä noudattavat sääntöjä, ja (3) niihin, jotka ovat erityisen tunnollisia sääntöjen noudattamisessa. Tutkimuksen tulokset osoittivat, että erilaiset rangaistukset toimivat eri tavoin eri ryhmissä. Esimerkiksi virallisten sanktioiden ankaruus ja epävirallisten sanktioiden varmuus toimivat tehokkaammin niille työntekijöille, joilla oli tietoturvasääntöjen vastainen asenne, kuin niille, jotka keskimääräisesti noudattavat sääntöjä. Virallisten sanktioiden varmuus taas toimi ainoastaan keskimääräisesti tietoturvasääntöjä noudattaville.

Siponen ja Vance (2010, 487–491) esittivät, että rangaistusten pelotevaikutus vähenee, koska ihmiset käyttävät muun muassa seuraavassa kuvassa lueteltuja neutralisointitekniikoita, joilla he rationalisoivat tietoturvaan liittyviä rikkomuksiaan. Tutkijat myös ehdottivat jokaiselle neutralisointitekniikalle strategiaa, joka löytyy oikeanpuolimmaisesta sarakkeesta. (2010, 497–498)

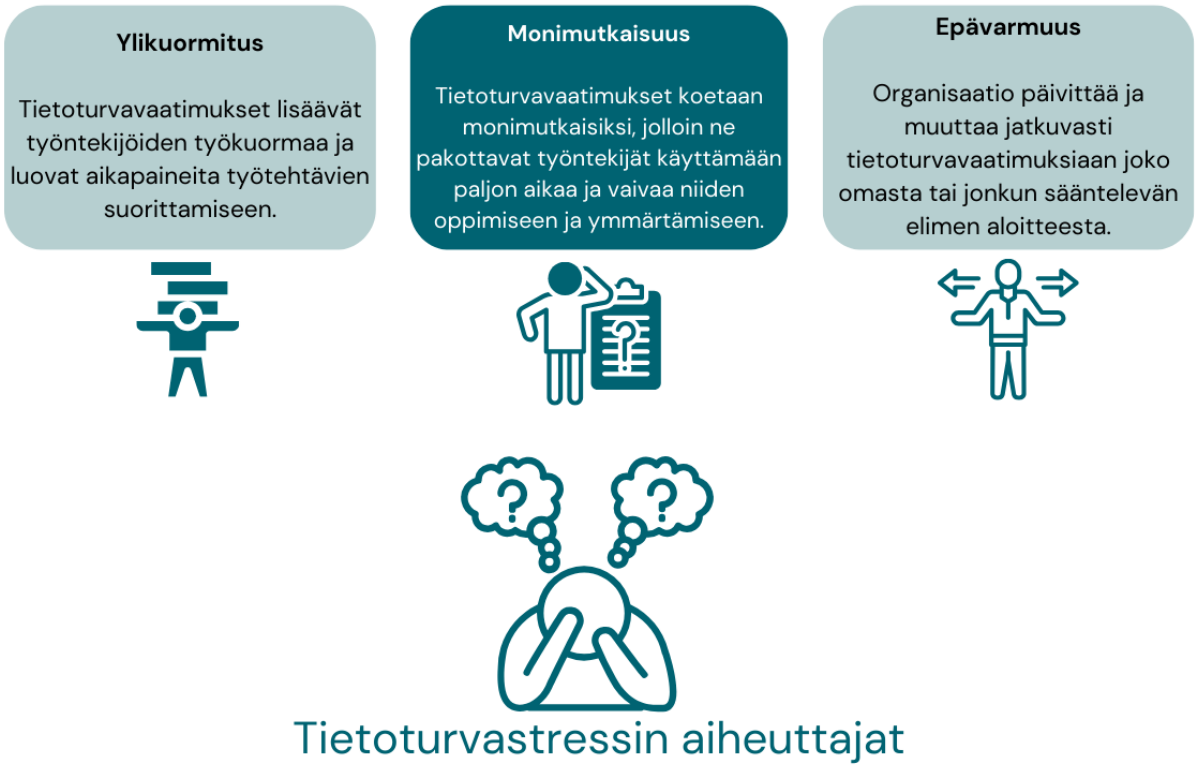
Neutralisointitekniikka, selitys ja esimerkki tietoturvakontekstissa	Strategia
Vahingon kieltäminen Henkilö oikeuttaa toimintansa vähättelemällä sen aiheuttamaa haittaa. Esimerkki: Työntekijä väittää, että on hyväksyttävää rikkoa tietoturvasääntöjä, jos se ei aiheuta haittaa yritykselle.	Koulutusten järjestäminen, joissa työntekijöille kerrotaan tietoturvakäytäntöjen rikkomisen seurauksista esimerkiksi skenaariopohjaisten harjoitusten avulla. Lisäksi esihenkilöitä tulisi rohkaista keskustelemaan työntekijöiden kanssa mahdollisista vahingoista, jos tietoturvakäytäntöjä ei noudateta.
Vastuun kieltäminen Henkilö rationalisoi, että kyseinen toiminta on hänen kontrollinsa ulkopuolella ja määrittelee itsensä vastuuttomaksi teoistaan. Esimerkki: Työntekijä lähettää luottamuksellisen sähköpostin salaamattomana ja oikeuttaa toiminnan sillä, että tietoturvakäytäntö on epäselvä.	On tärkeää painottaa, että tietoturvakäytäntöjen laiminlyönnille ei ole hyväksyttäviä tekosyitä, vaikka työntekijät eivät olisi varmoja tai ymmärtäisi niitä. Kouluttamisen, selkeän esitystavan ja saavutettavuuden lisäksi on tärkeää korostaa, että kaikki työntekijät ovat vastuussa omista toimistaan.
Välttämättömyyden pakko Henkilö oikeuttaa sääntöjen rikkomisen sillä perusteella, että se on välttämätöntä.	Johdon on tärkeää korostaa työntekijöille, että tiukkojenkin määräaikojen paineessa ei ole hyväksyttävää käyttää oikoteitä, jotka rikkovat

Esimerkki: Työntekijä väittää, että hänellä ei ole aikaa noudattaa tietoturvakäytäntöjä tiukkojen määräaikojen vuoksi.	tietoturvakäytäntöjä, ja että rikkominen on työntekijän oma valinta.
Korkeampiin velvollisuuksiin vetoaminen Henkilö tuntee olevansa dilemman edessä, joka on ratkaistava jopa lain tai käytännön rikkomisen kustannuksella. Esimerkki: Työntekijä rikkoo tietoturvasääntöjä, koska hän kokee, että hänen on saatava työnsä valmiiksi.	Organisaatioiden on varmistettava, että esihenkilöt tai tiiminvetäjät eivät tue alaisiaan rikkomaan tietoturvakäytäntöjä työtehtävien suorittamiseksi, edes määräaikojen paineessa. Työntekijöille on koulutettava se, että tietoturvakäytäntöjen noudattaminen on olennainen osa heidän työtään ja noudattamisen laiminlyönti on työvelvollisuuksien laiminlyöntiä.
Tuomitsijoiden tuomitseminen Henkilö oikeuttaa toimintansa syyttämällä niitä, jotka ovat toiminnan kohteena. Esimerkki: Työntekijä sanoo, että tietoturvasääntöjen rikkominen ei ole väärin, jos säännöt ovat kohtuuttomia.	Organisaatiossa tulisi oikeuttaa se, että vaikka tietoturvakäytäntöjen noudattaminen vaatisi ylimääräistä vaivaa, on tämä ylimääräinen ponnistus silti välttämätön.
Vetoaminen tilien pysymiseen tasapainossa Henkilö uskoo voivansa kompensoida huonoja tekoja hyvillä teoilla. Esimerkki: Työntekijä saattaa väittää, että koska hän yleensä noudattaa tietoturvakäytäntöjä, voi hän satunnaisesti olla noudattamatta niitä.	Työntekijöille tulisi selittää, että tietoturvakäytäntöjen noudattaminen yleensä ei oikeuta rikkomaan sääntöjä välillä ja että kova työ yrityksen hyväksi ei anna heille oikeutta rikkoa tietoturvakäytäntöjä silloin tällöin.

Kuva 8 Neutralisointitekniikat ja strategiat niiden taltuttamiseksi (Siponen ja Vance, 2010, 287–498)

2.12 Tietoturvastressi

D'Arcy, Herath & Shoss (2014, 288–289) tutkivat tietoturvastressin vaikutusta turvallisuuskäytäntöjen noudattamatta jättämiseen. Tietoturvastressillä tarkoitetaan psykologista stressiä, joka johtuu erityisesti tietoturvavaatimuksista, jotka kuormittavat henkilön kognitiivisia resursseja tai kykyjä ja usein häiritsevät työntekijöiden muita työtehtäviä. Sen kolme tärkeää ulottuvuutta ovat kuvassa 5 näkyvät *ylikuormitus*, *monimutkaisuus* ja *epävarmuus*. Tutkijat löysivät todisteita siitä, että työntekijät saattavat rationalisoida tietoturvasääntöjen rikkomisen, jos he kokevat tietoturvavaatimukset liian kuormittavina, monimutkaisina tai epävarmoina. Tämän vuoksi organisaatioiden on oltava tietoisia tietoturvavaatimusten stressiä aiheuttavista tekijöistä suojellessaan tieto-omaisuuttaan sisäisiltä uhkilta.



Kuva 9 Tietoturvastressin kolme ulottuvuutta (D'Arcy ym., 2014, 288–289)

Ylikuormittavalla tietoturvastressillä tarkoitetaan tilanteita, joissa tietoturvavaatimukset lisäävät työntekijöiden työkuormaa ja luovat siten lisää aikapaineita työtehtävien suorittamiseen. Esimerkiksi tilanteet, jossa työntekijät saattavat joutua käyttämään arvokasta aikaa IT-ammattilaisen odottamiseen ohjelmiston asentamiseksi tai ajoitetut tietoturvapäivitykset, jotka häiritsevät työntekijän suunnittelemia työtehtäviä voivat aiheuttaa turhautumista ja stressiä. Ylikuormituksen torjumiseksi

voi auttaa esimerkiksi nopea tekninen tuki ja käyttäjäystävälliset ohjelmistoratkaisut. (Darcy ym. 2014, 288–289)

Monimutkaisuudella taas tarkoitetaan tilanteita, joissa tietoturvavaatimukset koetaan monimutkaisiksi, jolloin ne pakottavat työntekijät käyttämään paljon aikaa ja vaivaa niiden oppimiseen ja ymmärtämiseen. Esimeriksi jos tietoturvapolitiikat sisältävät useita poikkeuksia tai sisältävät teknistä jargonia voivat työntekijät kokea, että heiltä puuttuu tarvittavat tiedot ja taidot, mikä voi johtaa stressiin. *Monimutkaisuuteen* liittyvää tietoturvastressiä saa vähennettyä tekemällä ymmärrettäviä tietoturvaohjeita, jotka välttelevät jargonia, jotta myös ei-tekniset ihmiset ymmärtävät ne. Tämän lisäksi aiemminkin useasti korostettu tietoturvatietoisuuden lisääminen esimerkiksi säännöllisellä koulutuksella on tärkeää. (Darcy ym. 2014, 288–289)

Epävarmuus viittaa tilanteisiin, joissa organisaatio päivittää ja muuttaa jatkuvasti tietoturvavaatimuksiaan joko omasta tai jonkun sääntelevän elimen aloitteesta. Organisaatiot joutuvat myös jatkuvasti hallitsemaan uusien teknologioiden luomia riskejä, mikä edellyttää tietoturvavaatimusten muuttamista. Seurauksena tästä työntekijät joutuvat sopeutumaan uusiin vaatimuksiin, mikä voi olla huolestuttavaa ja stressaavaa. Työntekijöiden osallistamisella tietoturvavaatimusten suunnitteluun ja toteutukseen, jolloin he voivat esimerkiksi testata niitä, tarjota palautetta ja auttaa muutosten viestimisessä kollegoille, on hyötyä. Työntekijöiden osallistamisella epävarmuuteen liittyvä stressi voi vähentyä, koska työntekijöillä on mahdollisuus tutustua tietoturva-vaatimuksiin ennen niiden täydellistä toteuttamista. Lisäksi, kun työntekijöillä on vaikutusvaltaa tietoturva-vaatimusten suunnitteluun ja toteutukseen, he saattavat kokea, että vaatimukset eivät ole niin haitallisia tuottavuudelle, mikä voi vähentää ylikuormituksen tunnetta. (Darcy ym. 2014, 288–289)

Tietoturvastressin käsittelyn lisäksi organisaatioiden tulisi myös pyrkiä torjumaan kognitiivisia rationalisointimekanismeja, jotka aiheuttavat tietoturvarikkomuksia. Tutkijat huomasivat, että viralliset sanktiot ovat tehokas menetelmä tässä suhteessa, koska ne lähettävät tärkeän viestin siitä, että rikkomukset ovat vastoin organisaation moraalisia periaatteita. Organisaatioiden on myös selkeästi ilmaistava sanktioiden varmuus, ankaruus ja nopeus tietoturvapolitiikassaan. Myös seuraavia asioita tulisi korostaa:

- Kaikkien työntekijöiden on otettava vastuu tietoturvasta.
- Tietoturvakäytäntöjen rikkomukset eivät ole koskaan hyväksyttävissä, riippumatta olosuhteista, kuten vaativista tietoturvavaatimuksista tai tiukoista aikatauluista
- Tietoturvakäytäntöjen rikkomukset voivat aiheuttaa suurta taloudellista tai maineellista vahinkoa organisaatiolle. (Darcy ym. 2014, 288–289)

2.13 Ihmisten tietoturvakäyttäytyminen ja motivaatiot

Jotta tietoturvaprosessien jalkauttaminen organisaatiossa onnistuisi, on tärkeää ymmärtää syitä ihmisten käyttäytymisen takana. Tietoturvakäyttäytymistä sekä tietoturvakäytäntöjen noudattamisen ja noudattamatta jättämisen syitä on onneksi tutkittu aiemmin ja tutkimuksiin on sovellettu erilaisia psykologisia teorioita. Tässä osiossa esitellään niistä muutamia.

Työntekijät voivat olla uhka, koska he voivat olla mukana tahallisessa väärinkäytöksessä, kuten esimerkiksi tietojen varastamisessa tai tuhoamisessa mutta myös tahattomassa tai vahingossa tapahtuvissa tapahtumissa, kuten esimerkiksi salasanan vaihtamisen tai uloskirjautumisen unohtamisessa. Koska työntekijöillä kuitenkin on suora pääsy organisaation verkkoon ja tietoihin, heistä tulee usein varkaiden tai hakkereiden kohteita. Siitä huolimatta monet organisaatiot aliarvioivat ihmisten johtamisen merkityksen ja luottavat puhtaasti teknologisiin ratkaisuihin tietoturvaa kehittäessään. Useimmat organisaatiot kehittävät tietoturvaohjelmansa ottamatta huomioon ihmisen roolia tietoturvaloukkauksissa. (Son, 2011, 296) Laaksosen ym. (2006, 254–255) mukaan teknisten ratkaisujen tulisi näkyä henkilöstölle niin vähän kuin mahdollista, koska tilannetta pahentaa, jos otetaan käyttöön teknisiä ratkaisuja, jotka haittaavat heidän työntekoaan tai muuttavat heidän rutiinejaan. Tietoturvallisuutta kehittäessä on muistettava, että rutiinit luovat ihmisille turvallisuudentunnetta ja muutokset taas epävarmuutta.

Bulgurcun, Cavusoglun ja Benbasatin empiirisen tutkimuksen (2010, 523–540) mukaan työntekijän aikomukseen noudattaa tietoturvakäytäntöjä vaikuttavat merkittävästi normatiiviset uskomukset, asenne ja itsetehokkuus. Asenteeseen vaikuttavat esimerkiksi tietoturvakäytäntöjen noudattamisen hyödyt ja kustannukset sekä noudattamatta jättämisen kustannukset, jotka perustuvat uskomukseen noudattamatta jättämisen seurauksista. Noudattamisen kustannuksilla tarkoitetaan esimerkiksi työn estymistä ja noudattamatta jättämisen kustannuksilla taas esimerkiksi resurssihukkaa tai sanktioita.

D’Arcy ja Lowry (2019, 60–61) tuottivat yhden ensimmäisistä tutkimuksista, joka sisällytti myös mielialat tietoturvakäytäntöjen noudattamista käsittelevään kirjallisuuteen. Heidän ilmeisin löydöksensä oli se, että työntekijöiden tietoturvakäytäntöjen noudattamisen asenne ja käyttäytyminen vaihtelevat päivittäin ja positiiviset ja negatiiviset mielialat vaikuttavat heidän aikomuksiinsa noudattaa käytäntöjä. Tämä tarkoittaa sitä, että vaikka työntekijä normaalisti noudattaisikin tietoturvaohjeita, saattaa hän yksittäisen tapahtuman tuloksena rikkoa sääntöjä. Organisaatioiden olisi hyvä keskittyä positiivisen työympäristön edistämiseen ja pyrkiä ennustamaan mahdolliset affektiiviset vaikutukset negatiivisista tapahtumista, kuten irtisanomista tai yritysjärjestelyistä. Koska työn estyminen myös aiheuttaa negatiivisia asenteita, tutkijat ehdottivat, että tietoturvakäytäntöjen noudattamisen edistämiseen voisi osallistaa IT-osaston lisäksi myös HR-osaston. Yhteistyöllä

varmistettaisiin, etteivät tietoturvavaatimukset tukahduttaisi työntekijöiden suorituskykyä. Myös tietoturvapolitiikan räätälöintiä työtehtävän tai osaston mukaan ehdotettiin. Organisaatioiden olisi tuotava tietoturvakäytäntöjen noudattamisen hyödyt työntekijöiden tietoisuuteen joko palkitsemalla tai sen korostamisella, että tietoturvakäytäntöjen noudattaminen on moraalisesti oikein. Tämän voi tehdä esimerkiksi moraalisten vastuiden sisällyttämisellä tietoturvallisuuskoulutuksiin ja -materiaaleihin. On tärkeää, että työntekijöille tarjotaan riittävästi koulutusta ja tukea, jotta he tuntevat olonsa itsevarmemmaksi tietoturva-asioissa. Työntekijät ottavat usein vihjeitä työtovereidensa käyttäytymisestä. Siksi ehdotettiin myös, että työpaikalla annettaisiin julkisesti tunnustusta hyvästä tietoturvakäyttäytymisestä.

Tietoturvan kiristykset vaikuttavat lähes aina käyttäjäkokemukseen. Käyttäjäystävällisyys ja tietoturvallisuus ovat usein ristiriidassa keskenään. Organisaatiot eivät yleensä halua huonontaa tietoturvallisuuttaan käyttömukavuuden takia. Työntekijät saattava kuitenkin lipsua sääntöjen noudattamisesta, jos se tekee heidän työstään mukavampaa tai nopeampaa. Tämän takia organisaatioiden olisi tärkeä löytää kompromissi, jolla ylläpidetään tietoturvallisuutta, mutta ei vaikeuteta työntekijöiden työntekoa älyttömästi. (Järvinen, 2022, 32)

Tietoturvakäyttäytymisen tutkimuksissa toistuu usein erilaisten motivaatioiden merkitys. Motivaatioista puhutaan esimerkiksi sisäisestä ja ulkoisesta motivaatiosta, jossa sisäinen motivaatio on ihmisen sisäsyntyistä ja ulkoinen taas sellaista, joissa tekemiseen vaikuttavat ulkoiset tekijät, kuten palkitseminen tai rangaistuksen välttäminen. Sisäisen motivaation merkitys on kirjallisuuden ja tutkimusten mukaan merkittävämpi.

Niina Kinnusen väitöskirjatutkimuksen mukaan usko ohjeiden noudattamisen tärkeydestä motivoi työntekijöitä noudattamaan tietoturvaohjeita. Hän tutki suomalaisten viranomaisten tietoturvaohjeiden sisältöä, työntekijöiden tietoturvaohjeiden noudattamisen pyrkimystä ja sen motivaatiotekijöitä. Tietoisuus tietoturvariskeistä ja erityisesti yrityksen jakamat tiedot tietoturvauhkista vahvistavat työntekijöiden motivaatiota noudattaa tietoturvaohjeita, kunhan tietojen määrä pysyy kohtuullisena. Viranomaisten tulisi Kinnusen mukaan pyrkiä vähentämään tietoturvaohjeistuksia ja niitä antavien tahojen määrää. Erityisesti pienet ja keskisuuret yritykset kokevat haastavaksi ohjeiden huomioimisen ja toteuttamisen, kun ohjeistavia tahoja ja ohjeistuksia on niin runsaasti. Kinnusen tutkimuksessa korostui, että työntekijät eivät tietoisesti halua toimia tietoturvaohjeiden vastaisesti. Työntekijät kuitenkin mainitsivat, että työtehtävien hoitamisen sitä edellyttäessä tai esihenkilön määräyksestä he pystyisivät toimimaan ohjeiden vastaisesti. Toisen henkilön tai tilanteen vaatimus oli toinen tärkeä motivoiva tekijä tutkimuksen mukaan. (Vaasan yliopisto 2015)

Sonin (2011, 296–297) mukaan ihmisten merkittävä rooli tietoturvan hallinnassa on herättänyt kiinnostusta myös siihen, kuinka työntekijöitä voitaisiin motivoida parantamaan organisaatioiden

tietoturvaa. Aiemmat tutkimukset ovat hänen mukaansa kuitenkin perustuneet paljolti ulkoiseen motivaatioon ja peloteteoriaan, kun on haluttu selvittää syitä tietoturvaohjeiden noudattamisen tai noudattamattomuuden taustalla. Hänen oletuksensa kuitenkin oli, että työntekijöiden ohjeiden noudattamista voisi paremmin selittää lähestymistavalla, joka perustuu sisäiseen motivaatioon. Tämän takia hän kehitti tietoturvaohjeiden noudattamista selittävän mallin, joka yhdisti sekä ulkoisen että sisäisen motivaation. Hän halusi selvittää noudattavatko työntekijät tietoturvaohjeita pääasiassa pelosta (ulkoinen motivaatio), halusta (sisäinen motivaatio) vai molemmista. Mallia testattiin 602 yhdysvaltalaistyöntekijällä ja havaittiin, että sisäisillä motivaatiotekijöillä oli tosiasiassa paljon merkittävämpi vaikutus työntekijöiden ohjeiden noudattamiseen kuin ulkoisesti motivoivilla tekijöillä.

Kranz & Haeussinger (2014, 1–4; 10–11) toteuttivat tutkimuksen 444 työntekijällä eri organisaatioista ja havaitsivat myös, että työntekijät, jotka olivat sisäisesti motivoituneita, eli heillä oli henkilökohtainen halu noudattaa sääntöjä, noudattivat tietoturvasääntöjä tunnollisemmin kuin ne, jotka noudattivat niitä vain välttääkseen rangaistuksia. Mitä enemmän henkilö on sisäistänyt ulkopuolelta tulleen säännön tai määräyksen (kuten tietoturvaohjeen), sitä autonomisemmin hän kokee noudattavansa tätä sääntöä tai määräystä. Henkilön kokemus autonomiasta, pätevyydestä ja yhteenkuuluvuudesta lisää hänen motivaatiotaan suorittaa tiettyä käyttäytymistä ja tämä parantaa hänen suorituskykyään, sinnikkyyttään ja luovuuttaan. Tutkijoiden tulokset tarjoavat vahvaa empiiristä näyttöä siitä, että työntekijät, jotka kokevat käyttäytymisensä omaehtoiseksi ja kokevat ulkoiset tietoturvasäännöt yhdenmukaisiksi omien arvojensa kanssa, noudattavat todennäköisemmin tietoturvakäytäntöjä. Sillä ei taas ollut vaikutusta noudattamisen aikomukseen, jos työntekijä kokee, että hänen toimintaansa ohjataan ulkopuolelta. Tämä viittaa heidän mukaansa siihen, että perinteisten lähestymistapojen, kuten pelotteiden ja palkitsemisen, tehokkuus on rajallinen ja vaikka pelotekeinot ovat varmasti edelleen tärkeitä, ne eivät yksin riitä motivoimaan työntekijöitä sitoutumaan tietoturvaan. Käytännön näkökulmasta tietoturvan ammattilaisten tärkein haaste työntekijöiden tietoturvakäyttäytymisen ja organisaatioiden tietoturvavaatimusten yhteensovittamisessa on siirtää toimintaa ohjaavan kokemuksen tunne ulkoisesta sisäiseksi. Tietoturvasääntöjen sisäistämistä voi edistää sillä, että välttää niiden esittämistä työntekijöille ilman sitä, että riittävästi selittää, miksi ne ovat organisaatiolle kriittisiä ja kuinka jopa pienin väärinkäytös voi johtaa vakaviin seurauksiin. Koulutukset tulisi suunnitella niin, että niissä perustellaan ja selitetään tietoturvakäytäntöjen ja -sääntöjen merkitys, jotta työntekijät ymmärtävät, että heidän yksilöllinen käyttäytymisensä voi vaarantaa heidät, heidän organisaationsa ja asiakkaansa. Pakotuksen tunteiden välttämiseksi olisi tehtävä selväksi, että käytännöt eivät ole olemassa työntekijöiden holhoamiseksi ja että jokaisella säännöllä on tarkoituksensa.

3 Empiirinen osio: Tietoturvaprosessien jalkauttaminen

Opinnäytetyön empiiristä osiota varten on tutkittu ja vertailtu, millaisia keinoja eri organisaatiot ovat käyttäneet jalkauttaakseen tietoturvakäytäntöjään ja -prosessejaan ja mitkä asiat näihin valintoihin ovat vaikuttaneet. Kuten johdannossa todettiin, tietoturvaprosessien jalkauttamiseen organisaatiossa voi käyttää useita eri keinoja ja jalkauttamisen keinot pitää valita kunkin tavoitteen osalta erikseen. Jalkauttamisen keinoja voivat olla tekniset toimenpiteet, kuten tekninen rajoittaminen tai uuden teknologisen ratkaisun tai järjestelmän käyttöönotto tai hallinnolliset toimenpiteet, kuten ohjeistaminen ja kouluttaminen. Kaikki haastateltavat olivat jalkauttaneet tietoturvaansa käyttäen sekä hallinnollisia että teknisiä keinoja ja pitivät molempia tärkeinä organisaation tietoturvan varmistamiseksi. Myös päätöksenteko nähtiin tärkeänä osana jalkauttamisprosessia. Jalkauttamistavat riippuivat aina käytännöstä ja sen vaatimuksista. Esimerkiksi jotkin käytännöt saattavat vaatia vain politiikkaa ja ohjeistusta, kun taas toiset vaativat järeämpiä teknologisia ratkaisuja.

3.1 Organisaation ominaisuudet

Organisaation koon merkitystä jalkauttamistavan valinnassa korostettiin. Haastatteluissa ilmeni, että pienissä ja varsinkin uusissa organisaatioissa on mahdollisuus määritellä toimintatavat alusta alkaen tiukasti, mikä on merkittävä etu. Tämä helpottaa monien asioiden selittämistä henkilöstölle. Pienissä organisaatioissa tietoturvan hallinta voi olla yksinkertaisempaa, kun prosesseja voidaan luoda ketterästi ja tietoa jakaa helpommin. Tällöin luottamuspohjaiset hallinnolliset keinot voivat toimia tehokkaasti. Ihmiset saattavat tuntea toisensa paremmin ja kun sovitaan yhteisistä säännöistä, ryhmän sisäinen koheesio voi vahvistua. Pienessä organisaatiossa voi olla helpompi ylläpitää luottamusta ja saavuttaa yhteinen tavoite hallinnollisin keinoin.

Haastateltavien kanssa myös keskusteltiin organisaation tietoturvakulttuurista ja muutoksensietokyvystä viitaten siihen, kuinka organisaatio vastaanottaa tietoturvaohjeita ja sopeutuu tietoturvan kiristyksiin. Eräs haastateltava toi esiin, että organisaation kyky ottaa vastaan uusia tietoturvaohjeita ja muutoksia riippuu paljon sen koosta ja iästä. Pienet ja nuoret organisaatiot, erityisesti teknologiaorientoituneet yritykset, ovat luontaisesti ketterämpiä ja sopeutuvat helpommin uusiin toimintatapoihin. Tämä johtuu siitä, että niiden päätoiminta liittyy usein kehitykseen ja muutokseen. Toisaalta suuret ja vanhemmat organisaatiot, joilla on enemmän vakiintuneita toimintatapoja, kohtaavat suurempia haasteita muutosten läpiviemisessä. Muutosvastarinta saattaa skaalautua näin ollen organisaation iän ja koon mukaan.

Suurissa ja mahdollisesti monikansallisissa organisaatioissa, joissa on tuhansia tai jopa kymmeniätuhansia usein vaihtuvia työntekijöitä, pehmeiden keinojen toteuttaminen on jo paljon haastavampaa, sillä kaikki työntekijät eivät mitenkään voi tuntea toisiaan. Tässä tilanteessa

luottamuspohjaiset keinot eivät välttämättä toimi samalla tavalla, jolloin formaalimpi lähestymistapa ja teknisempien ratkaisujen käyttöönotto voi olla perustellumpaa. Organisaation koko voi ylittää sen pisteen, jossa ihmiset voivat ylläpitää henkilökohtaisia suhteita ja tuntea toisensa riittävän hyvin. Haastateltava viittasi 150 ihmisen rajaan, joka on tuttu brittiläisen antropologin Robert Dunbarin teoriasta, jonka mukaan ihminen pystyy luonnollisesti ylläpitämään sosiaalisia suhteita noin 150 ihmisen kanssa. Ylittäessään tämän rajan organisaation on luotava tehokkaampia hallinnollisia rakenteita tai valvontamekanismeja, jotta tavoitteet saavutetaan, koska pelkästään käytäntöjen noudattamisen valvonta saattaa olla mahdotonta suuren henkilömäärän tai maantieteellisen sijainnin takia. Jalkauttamisen haasteet kasvavat, kun puhutaan suurista, monikansallisista yrityksistä. Prosessien jalkauttaminen edellyttää vastuullisten henkilöiden nimeämistä, ohjeistusten laatimista ja prosessin jatkuvuuden varmistamista, erityisesti kun työtä tehdään monissa toimipisteissä globaalisti ja kun henkilöstöä ei tunneta henkilökohtaisesti. Isoimmissa organisaatioissa ratkaisujen miettiminen voi olla myös paljon byrokraattisempaa, sillä prosessiin liittyy useita eri vaiheita ja osastoja ja päätöksentekoon tarvitaan usein monia hyväksyntäkierroksia.

3.2 Riskienhallinta

Jalkauttamistavan valinnassa on tärkeää huomioida erilaiset tietoturvariskit ja niiden hallinta. Koska tietoturvan kehittäminen on jatkuva prosessi, on säännöllinen riskien arviointi keskeistä. Riskienhallinta on myös yksi tärkeimmistä ISO27001 standardin vaatimuksista ja kriittisyys- ja riskianalyysi oli usein se, mistä haastateltavien organisaatiot lähtivät liikkeelle jalkauttamisprosessia miettiessään ennen kuin tekivät päätöksiä tai miettivät viestintää ja koulutuksia. Oman sisäisen riskianalyysin lisäksi tietoa ulkopuolisista riskeistä haastateltavat keräsivät eri lähteistä, kuten Kyberturvallisuuskeskukselta ja Cyberwatch Finlandilta, jotka päivittävät uhka- ja tilannekuvaa. Näiden riskien skaala on laaja, alkaen selaimen haavoittuvuuksista aina kriittisiin infrastruktuurijärjestelmiin kohdistuviin hyökkäyksiin. Riskianalyysissä haastateltavat saattoivat ottaa huomioon paitsi uhkien vaikutukset omaan liiketoimintaan, myös asiakkaidensa liiketoimintaan. Vaikka organisaatiot pyrkivät kattavaan suojaukseen ulkopuolisilta uhilta, uusia uhkaskenaarioita ilmenee jatkuvasti, mikä edellyttää jatkuvaa valppautta ja suojauksen päivittämistä. Riskejä arvioitiin haastateltavien organisaatioissa erilaisin syklein. Osa suoritti säännöllisen tai systemaattisen ISO27001 -standardiin liittyvän riskiarviointikierroksensa kerran vuodessa, osa jopa kerran kvartaalissa. Haastateltavien puheessa kuitenkin korostui, että tietoturvariskien arviointia tehdään organisaatioissa jatkuvasti, vaikka sitä ei suoritettaisi joka kerta niin strukturoidusti. Riskien tunnistamisen ja arvioinnin työkaluina organisaatiot käyttivät sekä perinteisiä Excel-taulukoita että kehittyneempiä, riskienhallintaan erikoistuneita tietojärjestelmiä tai alustoja.

3.3 Resursointi ja budjetti

Vaikka tietoturvan ylläpitoon liittyvät kulut saattavat tuntua suurilta, ne ovat kuitenkin mitättömiä verrattuna mahdollisiin vahinkoihin, jos tietoturva pettää. On siis edullisempaa ennaltaehkäistä ja varautua kuin korjata sitten kun vahinko on jo sattunut. (Järvinen, 2022, 34) Tietoturvan toteuttamiseen liittyy useita kustannuksia. Kustannuksia syntyy niin teknologian (virustorjuntaohjelmistot, palomuurit, seurantajärjestelmät) hankinnoista tai päivityksistä, kuin erinäisistä asennus- ja -konfigurointitöistä. Erilaiset tietoturvaprojektit saattavat tulla siis yllättävänkin kalliiksi, erityisesti jos organisaatiolla ei ole omaa sisäistä IT-resurssia.

Eräs haastateltava nosti, että ihanteellisessa tilanteessa organisaatiot miettisivät alusta asti, miten he voivat täyttää erilaiset tietoturvavaatimukset tehokkaasti. Tämä prosessi sisältäisi pohdintaa siitä, mikä olisi järkevin tapa toteuttaa vaadittavat toimenpiteet. Valitettavasti usein todellisuudessa ei ole riittävästi aikaa, kykyä tai resursseja tällaisten asioiden huolelliseen suunnitteluun. Työntekijöillä on usein monenlaisia muitakin velvoitteita, mikä tekee tietoturvastrategioiden kehittämisen haastavaksi. Monissa organisaatioissa voi olla rajoituksia resurssien, kuten aikaresurssien, henkilöstö- tai asiantuntemusresurssien tai taloudellisten resurssien suhteen. Erityisesti teknisten ratkaisuvaihtoehtojen harkinnassa ja valinnassa on kuitenkin aina otettava huomioon budjetointi, kustannukset ja sijoituksen tuotto. Resursointi ja budjetti siis vaikuttavat luonnollisesti siihen, kuinka perusteellisesti organisaatiot voivat suunnitella ja toteuttaa tietoturvakäytäntöjä. Joillekin organisaatioille hinta saattaa olla kynnyskysymys, esimerkiksi juuri teknisten ratkaisujen kohdalla. Tällöin sillä on suuri vaikutus myös jalkautumiskeinon valitsemiseen.

3.4 Työkulttuuri

Haastatteluissa ilmeni, että henkilöstön käyttökokemuksen vaikutus tietoturvan jalkauttamisprosesseihin ja päätöksiin riippuu suuresti organisaation työkulttuurista ja toimialasta. Esimerkiksi turvallisuussektorilla työskentelevät organisaatiot voivat asettaa korkeita odotuksia henkilöstön tietoturvakäytänteisiin, jopa siinä määrin, että työntekijät hyväksyvät aikaa vievät tietoturvaprosessit osana normaalia toimintatapaa. Toisaalta asiantuntijaorganisaatioissa, joissa työpaine on kova ja tuloksia on saavutettava nopeasti, tietoturvan monivaiheiset prosessit voivat olla ristiriidassa työn tehokkuusvaatimusten kanssa. Jalkauttamisprosessin onnistuminen riippuu siitä, kuinka hyvin se sopii yhteen organisaation kulttuurin ja toimintamallien kanssa. Tietoturvan jalkauttamisen haasteet kasvavat, kun tietoturvaprosessit ovat kauempana organisaation henkilöstön ydintehtävistä, jolloin ne voivat joutua ristiriitaan vallitsevan työkulttuurin kanssa.

3.5 Muutoksensietokyky

Eräs haastateltava toi esiin, että henkilöstön on aina hyväksyttävä uudet tietoturvatoimenpiteet, mutta kun tietoturvan tiukentamisesta tulee yleinen puheenaihe kahvipöytäkeskusteluissa, se voi olla merkki siitä, että tietoturvan tason muutokset ovat tapahtuneet liian nopeasti ja kiristyksiä on ollut liikaa. Jos tietoturvamuutoksista keskustellaan jatkuvasti ja ne koetaan häiritseviksi, voi olla hyödyllistä harkita ajoittaa tiukennukset tai muutosten harvemmin tapahtuviksi, jotta työntekijöiden päivittäinen toiminta ei häiriintyisi liikaa. Toisaalta kun tietoturvasta tulee keskustelunaihe henkilöstön keskuudessa, se osoittaa myös sen, että henkilöstön tietoturvatietoisuus on lisääntynyt ja tietoturvakulttuuri kehittynyt. Täydellinen tasapaino tietoturvan tiukkuuden ja käytännön toimivuuden välillä on hankala saavuttaa.

3.6 Johtaminen

Haastatteluissa tuli myös ilmi, että johdolla on iso rooli tietoturvan jalkauttamisessa, sillä se vaikuttaa paljon myös organisaation muutoksensietokykyyn. Havainnot siis tukevat vahvasti teoriaosiossa esitettyjä oletuksia. Muun muassa organisaation muutoksensietokyky tietoturvaprosessien jalkauttamisessa, kuten ISO27001-standardin mukaisissa toimissa, riippuu merkittävästi johdon sitoutumisesta ja ymmärryksestä. ISO27001 on kuitenkin johtamisjärjestelmä, joka vaatii paljon myös johdon toimintatapojen muuttamista.

Eräs haastateltava korosti, että yksi yleinen virhe on aloittaa tietoturvaprosessien, kuten ISO27001-standardin mukaisten toimien, käyttöönotto organisaation alimmilta tasoilta ilman ylemmän johdon tukea ja ymmärrystä. Tämä lähestymistapa johtaa usein siihen, että vaikka alatasoilla saattaa kehittyä tehokkaita mittauksia ja prosesseja, ne eivät tuota toivottua tulosta kokonaisuuden kannalta. Ilman ylemmän johdon aktiivista osallistumista ja selkeää kanavaa, jonne tulokset ja havainnot raportoidaan, nämä aloitteet eivät saavuta haluttuja vaikutuksia. On tärkeää, että johto ei ainoastaan tue ISO27001-prosesseja sanallisesti, vaan on myös aktiivisesti mukana esimerkiksi riskianalyysissä tai henkilöstön tietoturvakoulutuksissa painottamassa asian tärkeyttä, jotta henkilöstö aidosti ymmärtää, että johto vaatii heiltä sitoutumista yhteisiin tietoturvasääntöihin ja että tietoturva on organisaatiolle ensisijainen prioriteetti, johon kaikkien on sitouduttava – vaikka koulutukseen käytettävät työtunnit olisivatkin pois esimerkiksi laskutettavasta työstä.

Johdon muutosvastarinta syntyy usein ymmärtämättömyydestä siitä, mitä johdolta odotetaan. Tällöin on kriittistä tehdä johdon rooli ja odotukset erittäin selviksi ja "myydä" ISO27001-prosessien implementointi niin, että johto ymmärtää sen merkityksen ja vaatimukset. Tämä tarkoittaa konkreettisten esimerkkien ja selitysten antamista siitä, mitä johdon sitoutuminen käytännössä tarkoittaa, kuten esimerkiksi säännöllisten kokousten järjestämistä, joissa keskustellaan tietoturvatilanteesta

ja ehdotetaan toimenpiteitä. Tällöin johdon tuki ei ole pelkästään teoreettista, vaan he näkevät konkreettisesti, miten heidän panoksensa edistää organisaation tietoturvaa. Tämä edellyttää selkeää viestintää ja suunnittelua, jotta johto näkee tietoturvan kehittämisen arvon ja on motivoitunut tukemaan sitä, mikä puolestaan lisää organisaation kykyä sietää muutosta.

3.7 Vastuutus

Useampi haastateltava korosti, että tietoturvakäytäntöjen tehokas toteutus vaatii selkeän vastuutuksen. Jokaiselle tietoturvakäytännölle on nimettävä vastuuhenkilö ja käytäntö tulee kuvata selkeästi, riippumatta siitä onko kyseessä teknologinen ratkaisu tai hallinnollinen päätös. Ilman nimettyä vastuuhenkilöä käytännön toteutuminen saattaa jäädä epäselväksi. Koko henkilöstölle voidaan vastuuttaa vain niitä asioita, jotka ovat selkeästi relevantteja koko henkilöstölle, kuten esimerkiksi mobiililaitteiden vastuullisen käytön tai tietoturvaohjeiden mukaisen toiminnan.

Eräs haastateltava kertoi, että heidän tietoturvan hallintajärjestelmän rakentamisprosessi toteutettiin 5 hengen projektiryhmässä, jonka vetäjänä hän itse toimi. Johto antoi alustavan tuen projektin suunnalle ja ryhmässä käytiin keskusteluja ja sparrailtiin siitä, mikä olisi organisaation tietoturvalle sopiva taso ja linja. Koska heidän organisaationsa ei ole erityisen tiukan toimialasäätelyn tai asiakasvaatimusten alainen, heillä oli suurempi vapaus määritellä itse oma tietoturvan tasonsa. Lopullinen hyväksyntä päätöksille tuli kuitenkin johtoryhmältä, mutta kun tietoturvan perusperiaatteet oli kerran vahvistettu, toimivat ne toimintaohjeina jatkossa. Mikäli joku työntekijä ei tämän jälkeen noudattanut ohjeita, kirjattiin se poikkeamana ja asiaan puututtiin. Haastateltavan kuvauksen perusteella prosessi oli osallistava ja joustava, mutta samalla selkeästi ohjeistettu ja johtoryhmän tukema.

3.8 Hallinnolliset keinot

Hallinnollisten keinojen osalta mainittiin konkreettisia esimerkkejä, kuten tietoturvapolitiikan kirjoittamisen, ohjeistusten ja toimintaohjeiden laatimisen henkilöstölle. Nämä dokumentit ohjaavat organisaation toimintaa tietoturvan osalta. Hallinnolliset keinot ovat tavallaan aina läsnä, sillä teknisenkin kontrollin taustalla on aina jokin tietoturvapolitiikka tai -periaate, joka ohjaa teknisten keinojen käyttöä.

Eräs haastateltava nosti, hallinnolliset keinot, kuten ohjeistukset ja säännöt, voivat toimia hyvin vain, jos niitä valvotaan ja niiden noudattamista seurataan. Usein organisaatioissa ei kuitenkaan ole riittävästi resursseja tähän tehtävään ja seuranta jää tämän osalta puutteelliseksi. Vaikka organisaatiolla olisikin tietoturvan vastuuhenkilö tai velvoitteiden noudattamisesta vastaava henkilö tai "Compliance Officer”, heiltä voi puuttua silti tarvittava tuki tai tiimi, joka pystyisi aidosti valvomaan, että tietoturvatoimenpiteitä noudatetaan. On hyvin yleistä, että organisaatiot tekevät

tietoturvapolitiikkansa ja prosessinsa tunnollisesti ISO/IEC 27001 -standardin mukaisesti, mutta näiden prosessien ja käytäntöjen valvominen voi olla erittäin haastavaa. ISO/IEC 27001 on kuitenkin erittäin laaja ja kattava standardi, joka sisältää monia erilaisia prosesseja ja vaatimuksia. Pehmeiden tietoturvakeinojen pitäisi perustua ymmärrykseen siitä, että ne toimivat samalla tavalla kuin yhteiskunnan lait. Lait voivat olla olemassa, mutta niiden noudattamisen valvonta on keskeistä niiden toimivuuden kannalta. Valvontaa voi kuitenkin olla hallinnollisten toimenpiteiden kohdalla käytännössä vaikea toteuttaa, jolloin asioiden toistamisella voi olla suuri merkitys. Tämä voi tarkoittaa säännöllisiä koulutuksia ja toistuvaa viestintää, jotta tietoturvakäytännöt juurtuvat organisaation kulttuuriin. Tärkeintä on, että resursseja on tarpeeksi, jotta tietoa voidaan levittää ja varmistua siitä, että tieto menee perille.

3.9 Viestintä

Eräs haastateltava kertoi tietoturvan hallintajärjestelmän kehittämisprosessinsa viestinnästä, mikä auttoi välttämään suuren muutoskuorman syntymistä. Viestintä aloitettiin hyvissä ajoin, mutta he eivät tiedottaneet yksityiskohtaisesti jokaisesta prosessista kaikille, sillä tietyt prosessit, kuten esimerkiksi riskienhallinta vastuutettiin pääsääntöisesti johtoryhmälle tai muille tällä tasolla toimiville. Tämä mahdollisti vain tarvittavan henkilöstön osallistumisen prosesseihin tarpeen mukaan, tehden osallistumisesta helpompaa ja vähentäen muutosvastarintaa. Organisaation viestintästrategia keskittyi olennaiseen tiedonjakoon oikea-aikaisesti. Esimerkiksi tietoturvaohjeistus tiivistettiin 20-sivuisesta 10-sivuiseksi ja sen esittely henkilöstölle suunniteltiin niin, että se tapahtui vasta prosessin loppuvaiheessa, kun suuria muutoksia ei enää odotettu tapahtuvan. Tämä auttoi välttämään tarpeetonta sekaannusta ja tarpeen tehdä lisämuutoksia ohjeistukseen. Keskittyminen olennaiseen viestintään auttoivat rakentamaan ja ylläpitämään toimivaa tietoturvakulttuuria.

Äärimmäisen selkeyden merkitystä henkilöstön ohjeistamisessa korostettiin, jolloin henkilöstölle annetaan yksiselitteiset toimintatavat ja ohjeet, jotta he ymmärtävät tietoturvaroolinsa organisaatiossa. Ohjeiden on oltava selkeitä ja ymmärrettäviä, eikä niissä saa olla ristiriitaisuuksia, jotta henkilöstö pystyy noudattamaan niitä ongelmitta. Tämä vähentää virheiden tekemisen mahdollisuutta ja on erityisen tärkeää tietoturvan ja henkilöstölähtöisten toimien kannalta. Selkeä viestintä edistää ymmärrystä ja myönteistä suhtautumista muutoksiin. Kun henkilöstö on tottunut selkeisiin prosesseihin ja heille viestitään muutosten syistä ja tavoista selkeästi, on todennäköisempää, että he omaksuvat uudet toimintatavat ja suhtautuvat muutoksiin positiivisesti.

3.10 Tietoturvakoulutus

Vaikka moni haastateltavista järjesti tietoturvakoulutuksensa henkilöstölle itse, oli haastateltavilla myös hyviä kokemuksia koulutusten ulkoistamisesta palveluntarjoajille. Palveluntarjoajilta ostettiin

niin kyberturvallisuuskoulutusta kuin esimerkiksi simulointipalveluita, jotka valmentavat työntekijöitä tunnistamaan kalasteluhyökkäyksiä. Koulutukset ovat tällöin interaktiivisempia ja saattavat olla käyttökokemuksena työntekijöille mukavampia kuin perinteiset luentomaiset koulutukset. Etuna näissä palveluissa on myös se, että henkilöstö voi suorittaa koulutusmoduuleita omalla ajallaan ja että koulutusten suorituksista ja simulaatioharjoituksista jää myös dataa esimerkiksi tietoturvakulttuurin mittarointia varten.

Kohdennettu tietoturvakoulutus todettiin tehokkaaksi jalkauttamiskeinoksi teoriaosiossa mainitussa Beyerin ja Brummelin (2015, 6; 18) tutkimuksessa. Kohdennetun tietoturvakoulutuksen osalta haastateltavien vastauksista ilmeni, että useammissa organisaatiossa toteutettiin kohdennettua tietoturvakoulutusta eri työntekijäryhmille tai käyttöoikeusryhmille, vähintään sen jälkeen kun organisaatiossa on saavutettu hyvä perustaso yleisessä tietoturvatietoisuudessa. Kohdennettu koulutus myös johtui usein siitä, että eri tiimit käyttävät erilaisia järjestelmiä työssään. Esimerkiksi myyntitiimin jäseniä ei kouluteta samalla tavalla kuin teknisemmän työtehtävän omaavia työntekijöitä. Tämä lähestymistapa mahdollistaa koulutuksen räätälöinnin kunkin ryhmän erityistarpeiden ja käyttämien järjestelmien mukaan, mikä tekee koulutuksesta tehokkaamman ja relevantimman eri käyttäjäryhmille.

Eräässä tietoturva-alalla toimivassa organisaatiossa järjestettiin kahden viikon välein tunnin mittaisia tietoturvatyöpajoja koko henkilöstölle. Työpajojen sisältö vaihteli laajasti ja agendalla saattoi olla esimerkiksi lainsäädäntöön ja direktiiveihin liittyviä aiheita sekä ajankohtaisia tietoturvauutisia, joita henkilöstön jäsenet saivat itse nostaa ja joista kaikkien oli hyvä tietää ja keskustella, jotta he voisivat neuvoa asiakkaitaan paremmin. Haastateltava kuitenkin korosti, että vaikka heidän henkilöstönsä onkin vahva tietoturvaosaamiseltaan ja aktiivinen tietoturvauhkien havaitsemisessa ja niistä ilmoittamisessa, ei organisaatio voi pelkästään luottaa henkilöstönsä osaamiseen suojautumisessa tietoturvauhkia vastaan. Uuden henkilön perehdyttäminen tietoturvakulttuuriin voi kestää jopa vuoden, mikä asettaa omat haasteensa.

3.11 Tekniset keinot

Vaikka organisatoriset toimenpiteet, kuten tietoturvakoulutukset ja -käytännöt ovat olennaisia tehokkaan tietoturvaympäristön toteuttamiseksi, tietoturvallisuuden toteuttaminen pelkillä hallinnollisilla toimenpiteillä ei kuitenkaan yksinään riitä ja organisaatioiden on otettava myös teknologia avuksi. Teknologiaa tarvitaan useita tietoturvallisuuden osa-alueita, kuten muun muassa pääsynhallintaa tai virustorjuntaa varten. Teknologiset ratkaisut, kuten virustorjuntaohjelmistot ja palomuurit tarjoavat välttämättömän suojan jatkuvasti kehittyviä uhkia vastaan. Teknologisilla ratkaisuilla voidaan havaita, analysoida ja reagoida uhkiin nopeasti jo ennen sitä, kuin ihmisiin liittyvät riskit tulevat kuvioihin. Teknologisilla ratkaisuilla voidaan nykyisin myös helposti kerätä dataa

tietoturvahäiriöistä. Haastattelujen yhteydessä tekniselle keinolle löydettiin useita tarkoituksia ja määritelmiä. Keino voi olla muun muassa uusi järjestelmä, konfiguraatiomuutos tai vaikkapa jonkin manuaalisen vaiheen automatisointi. Tietoturvan alueella innovaatiot ja uudet teknologiat kehittyvät jatkuvasti, joten mahdollisuudet kasvavat teknologian kehittyessä nopeasti.

Jalkauttamisprosessi teknistenkin ratkaisujen osalta kuitenkin alkaa usein hallinnollisesta näkökulmasta, jossa arvioidaan organisaation kapasiteettia ja mahdollisuuksia toteuttaa uusia teknisiä ratkaisuja. Teknisistä keinoista puhuttaessa lähes kaikki haastateltavat toivat esiin, että teknisiä hallintakeinoja kannattaisi käyttää aina kun se on mahdollista, sillä ne tukevat hallinnollisia käytäntöjä. Esimerkkinä nousi toimistolle pääsyn kontrollointi: vaikka olisi olemassa politiikka tai ohje, joka rajoittaisi pääsyn vain tietyille henkilöille, on silti järkevää asentaa oveen lukko. Teknisiä kontrolleja käyttäessä käyttäjät eivät pysty ohittamaan omilla toimillaan rajoituksia ja jos käyttäjä ei ole syystä tai toisesta sisäistänyt ohjeistettua tai koulutettua asiaa, voidaan silti teknisillä kontrolleilla estää tai rajoittaa käyttäjän tekemistä. Vaikka tietoturvapolitiikassa olisikin painotettu käyttäjille sitä, että organisaatio käsittelee arkaluontoista tietoa ja organisaation olemassaolo saattaa pahimmillaan loppua johonkin tietoturvatapahtumaan, voidaan silti teknisillä toimenpiteillä pienentää riskiä esimerkiksi niin, että käyttäjillä, jotka eivät ole niin valveutuneita tietoturvan osalta, ei ylipäätään olisi pääsyä arkaluontoisiin tietoihin.

Haastatteluissa ilmeni, että teknisempien organisaatioiden tai IT-alalla toimivien organisaatioiden oli helpompi toteuttaa teknisiä toimenpiteitä ympäristöönsä ja ottaa uutta teknologiaa käyttöön. Eräs haastateltava kuitenkin korosti, että vaikka IT-alalla toimivilla organisaatioilla on hyvät valmiudet teknologian käyttöönottoon ja hallintaan, niiden tietoturva- ja IT-osastot saattavat kuitenkin olla hyvinkin erillään muusta organisaatiosta, jolloin ne eivät välttämättä ole aina aktiivisessa vuorovaikutuksessa muiden osastojen kanssa. Tämä voi johtaa vääriin oletuksiin tai harhaluuloihin tietoturvan tasosta, koska monet organisaatiot luottavat siihen, että heidän tietoturvansa on kunnossa perustuen esimerkiksi siihen, että he käyttävät turvallisia ohjelmointikäytäntöjä, jolloin hallinnollisempia tietoturvaprosesseja tai vaikkapa johdon sitoutumista ei oteta huomioon. ISO27001-sertifioidut yritykset ovat yleensä paremmassa asemassa, koska hallinnollinen puoli on tällöin väkisinkin otettu huomioon, mutta monet IT-yritykset saattavat olettaa virheellisesti olevansa hyvin suojattuja ilman todellista perustaa tai ymmärrystä tietoturvan laajuudesta, jolloin näkemys voi jäädä hyvin yksipuoliseksi. Muilla organisaatioilla taas saattaa olla puutteita teknisemmässä tietoturvaosaamisessa, mikä voi estää heitä näkemästä kaikkia mahdollisia teknologisia ratkaisuja tietoturvahaasteisiin.

Tekniset keinot eivät aina kuitenkaan toimi yksinään. Vaikka teknologia nopeuttaa rutiinitehtäviä, hallinnolliset toimet takaavat yksilöllisten tilanteiden huomioimisen ja kokonaisvaltaisen seurannan. Eräs haastateltava nosti esimerkkinä pääsyoikeuksien hallinnan. Esimerkissä pääsyoikeuksien

hallintaprosessi jakautuu kolmeen vaiheeseen: 1) pääsyoikeuspyynnön tekeminen, 2) pyynnön käsittely ja myöntäminen ja 3) oikeuksien ylläpito ja päivitys tarvittaessa, esimerkiksi työntekijän roolin muuttuessa tai työsuhteen päättyessä. Tekniset ratkaisut voivat helpottaa ja nopeuttaa tämän prosessin alkuvaiheita, kuten pääsyoikeuspyyntöjen tekemistä ja käsittelyä automaation avulla, mutta ne eivät välttämättä yksinään kykene huomioimaan kaikkia tilanteita, kuten työntekijän roolin muuttumista tai työsuhteen päättymistä, mikä on keskeistä oikeuksien ajantasaisuuden kannalta. Tässä kohtaa tarvitaan myös hallinnollisia prosesseja, jotka mahdollistavat yksityiskohtaisemman seurannan ja dokumentoinnin siitä, kenellä on pääsy mihinkin järjestelmään, jotta myöntämistä, seurantaa ja päivittämistä voidaan hallita keskitetysti. Integroimalla tekniset ja hallinnolliset prosessit, organisaatiot voivat luoda kokonaisvaltaisia hallintajärjestelmiä, jotka eivät ainoastaan tehosta prosesseja vaan myös varmistavat toiminnan turvallisuuden muuttuvissa olosuhteissa.

3.12 Teknisten ratkaisujen valintakriteerit

Organisaatioiden tietoturvaa koskevien ratkaisujen valintaan vaikuttavat monenlaiset tekijät. Ensimmäinen askel on ymmärtää, mitä organisaatio todella tarvitsee ja riskejä, joita teknologian käyttöönotto tulee pienentämään. Haastatteluissa korostui, että teknisiä komponentteja miettiessä organisaatiot usein tarkastelivat aluksi, onko suunniteltu muutos mahdollista toteuttaa hyödyntämällä jo käytössä olevia teknisiä ratkaisuja tai mukauttaa niitä uuteen tarpeeseen sopiviksi. Jos sopiva tekninen ratkaisu on jo käytössä, pyritään sitä hyödyntämään. Erityisesti isoissa organisaatioissa voi olla haastavaa perustella uuden, erillisen ratkaisun hankintaa ilman sitä, että se tarjoaa selkeästi lisäarvoa. Sen jälkeen on tärkeä kartoittaa kustannukset ja niiden jakautuminen. Päätös teknisen ratkaisun käyttöönotosta perustuu usein sen yksinkertaisuuteen, suoraviivaisuuteen, skaalautuvuuteen, mutta myös kustannusrakenteeseen. Organisaatiot pyrkivät löytämään sellaisia ratkaisuja, jotka vastaavat heidän ongelmiinsa mahdollisimman kustannustehokkaasti.

Myös organisaation toimintakulttuuri ja sisäiset kannustimet vaikuttavat merkittävästi ratkaisujen käyttöönottoon. Haastatelluissa myös ilmeni, että päätökset saattavat perustua vakiintuneisiin toimintatapoihin ja -kulttuuriin, vaikka se ei olisikaan tehokkain tai taloudellisin vaihtoehto. Organisaatiot saattavat kohdata haasteita, kun on kyse ihmisten työtuntien ja manuaalisten prosessien tehokkuuden arvioinnista. Esimerkiksi osastot, joita mitataan tuottavien tai laskutettavien työtuntien mukaan, eivät välttämättä ole halukkaita ottamaan käyttöön ratkaisuja, jotka vähentäisivät näennäisesti heidän tuottavuuttaan, vaikka kokonaisuuden kannalta ratkaisu olisikin hyödyllinen.

Haastateltavat nostivat useita muita kriteereitä miettiessään teknisiä ratkaisuja. Suosituksia ja tietoa eri järjestelmien toimivuudesta ja luotettavuudesta kerättiin useista kontaktiverkostoista. Muun muassa seuraavia asioita haastateltavat ottivat huomioon teknisiä ratkaisuja miettiessään:

- **Toimittajan tausta ja toimitusketjut.** Toimittajan koko, sijainti, toimintakyky, sertifikaatit ja mahdolliset alihankkijat on hyvä analysoida. Sijainnilla on vaikutusta niin palvelun tasoon ja saatavuuteen kuin myös tietosuojaan, jotta voidaan varmistua siitä, että noudatetaan GDPR-vaatimuksia. Myös potentiaaliset yrityskaupat ja niiden vaikutukset tuotteen tai palvelun laatuun on hyvä ottaa huomioon jatkuvuuden arvioimiseksi. Koska teknologia kehittyy huomattavaa vauhtia, on myös sopimuksissa hyvä varmistua siitä, että sopimuksesta pääsee tarvittaessa helposti irtaantumaan. Kriittisten teknologisten järjestelmien kohdalla myös toimittajien tietoturvasertifikaatit koettiin tärkeiksi.

- **Käytettävyys ja helppokäyttöisyys**. Teknisen ratkaisun käytettävyyden tulee olla korkealla tasolla. Järjestelmien on oltava helposti ja nopeasti käyttöön otettavia, jolloin ne eivät vaadi liikaa personointia tai opettelua. Huonosti toteutetut ratkaisut, jotka tekevät käytöstä hankalaa ja aikaa vievää, vähentävät käyttäjien motivaatiota ja johtavat helposti kiertoteiden etsimiseen tai tehtävien laiminlyömiseen. Käyttökokemuksen optimointi ja käyttäjäpalautteen huomioiminen koettiin hyvin tärkeäksi tietoturvakäytäntöjen kehittämisessä ja käyttöönotossa.

- **Rajapinnat ja integroitavuus**. On tärkeää, että uudet tekniset ratkaisut integroituvat sujuvasti organisaation nykyiseen IT-infrastruktuuriin ja olemassa oleviin järjestelmiin. Lisääntyvät järjestelmät kasvattavat sekä hyökkäyspinta-alaa että ylläpidettävien järjestelmäkokonaisuuksien monimutkaisuutta. Tietoturvan valvonnan vaikeudet myös korostuvat, jos järjestelmiä ei ole integroitu keskenään.

- **Pilotointi ja testausmahdollisuudet**. Kaikki haastateltavat pilotoivat järjestelmiään ennen laajempaa käyttöönottoa pienemmillä käyttäjäryhmillä, jolloin voidaan varmistua järjestelmän helppokäyttöisyydestä ja soveltuvuudesta oman organisaation tarpeisiin. Loppukäyttäjien kokemukset ovat keskeisiä tekijöitä, jotka vaikuttavat järjestelmän valintaan.

3.13 Ulkoistaminen

Hallinnollisten ja teknisten keinojen lisäksi, haastatteluissa nousi esiin myös se, että organisaatiot käyttävät myös ulkoisia konsultteja tietoturvaprojekteissaan ja nykyisin myös ulkoistavat tiettyjä toimintojaan tietoturvan osalta, kuten esimerkiksi tietoturvaheikkouksien havaitsemisen. Myös tietoturvakoulutus voidaan ostaa palveluna. Tämä helpottaa tai vähentää organisaation omaa työtaakkaa, mutta samalla vaatii valvontaa ja ymmärrystä palvelun laadusta. Ulkoistaminen edellyttää siis silti sopimussuhteen ja palvelun tason aktiivista seurantaa, esimerkiksi tarkastelemalla palvelutasosopimuksia ja varmistamalla, että palvelut toimivat tietyllä tavalla. Ottaen huomioon työvoiman suuret kustannukset, organisaatioiden kannattaa punnita kustannuksia ja hyötyjä suhteessa omiin

resursseihinsa ja tarpeisiinsa. Ulkoistaminen kuitenkin parhaimmillaan mahdollistaa yrityksille keskittymisen ydinliiketoimintaansa samalla kun ne hallitsevat tietoturvariskejään.

3.14 Hallintajärjestelmätyökalut

Organisaation tietoturvan hallintajärjestelmän luomiseen ja jalkauttamiseen on myös olemassa teknisiä hallintajärjestelmätyökaluja, jotka mahdollistavat muun muassa jokaisen käytännön ja prosessin dokumentoinnin, vastuuttamisen, jalkauttamistavan valinnan sekä säännöllisen tarkistuksen. Esimerkiksi Digiturvamalli-nimistä palvelua voi käyttää tietoturvan hallintajärjestelmän hallinnointiin, jalkauttamiseen ja myös jatkuvaan parantamiseen. Tällöin jokainen vaatimuksen mukainen tietoturvakäytäntö arvioidaan ja priorisoidaan yksilöllisesti, jonka jälkeen päätetään sen vastuutus ja jalkauttamistapa. Tämän jälkeen hallintakeinot jalkautetaan tehtävinä organisaatioon. Jalkauttamisvaihtoehtoja ovat esimerkiksi ihmislähtöiset tehtävät, kuten ohjeistaminen, hallinnolliset tehtävät, kuten politiikkojen tai eri suunnitelmien valmistelu tai tekniset tehtävät, kuten jonkun suojausjärjestelmän käyttöönotto ja sen kuvaus. Jalkauttamistavaksi voidaan myös valita tietyissä tilanteissa esimerkiksi eri yksiköiden vastuuhenkilöiden kautta tapahtuva jalkauttaminen, jolloin päävastuulliset huolehtivat siitä, että käytäntö toteutuu heidän yksikössään halutulla tavalla. Kaikkien käytäntöjen tai prosessien kohdalla järjestelmään voidaan myös määritellä tarkastussyklin määräpäivät, jolloin vastuuhenkilöt kuittaavat, että prosessi toimii ja toimenpiteet ovat tehty. (Digiturvamalli, 2023)

3.15 Mittarointi

Haastateltavien kanssa keskusteltiin myös mittaroinnin ja seurannan merkityksestä tietoturvan tehokkaassa hallinnassa ja tietoisuuden lisäämisessä organisaatiossa. Pätevien mittareiden kehittäminen on usein aikaa vievää ja vaikeaa, sillä mittareiden tulee olla merkityksellisiä, kuvastaa todellisuutta ja myös johtaa järkeviin toimenpiteisiin. Joskus on pysähdyttävä myös pohtimaan, onko tietyn asian mittaaminen edes mahdollista. Mittareiden tarkkuuden ja validiteetin tärkeyttä korostettiin, jotta ne voivat oikeasti auttaa parannusten seurannassa. Mittareita on myös säännöllisesti tarkasteltava uudelleen niiden relevanssin varmistamiseksi, sillä jos yhdellä osa-alueella päästään hyvälle tasolle, mittari ei välttämättä ole enää validi tietyn ajan kuluttua. Yksi haastateltava jakoi myös kokemuksensa siitä, kuinka organisaatioissa voi olla erilaisia näkemyksiä mittareista, jolloin voi olla vaikeaa kehittää yksimielisyyttä mittaustavoista.

Haastateltavilla oli käytössä sekä teknisiä että hallinnollisia mittareita tietoturvakulttuurin arviointiin. Useampi haastateltavista mainitsi käyttävänsä sellaisia teknisiä mittareita, jotka tulevat tiettyjen liiketoimintasovellusten tai virustorjuntatuotteiden mukana. Esimerkkinä mainittiin Microsoftin Security Score -mittari, joka perustuu muun muassa järjestelmän konfiguraatioihin tai käyttäjien toimintaan. Se ei kuitenkaan ole absoluuttinen ja täydellinen mittari, sillä se enemminkin kuvaa, missä

määrin organisaatio on ottanut käyttöön tietoturvatoimenpiteitä Microsoft-tuotteissaan. Tärkeänä pidettiin, että organisaatiot panostaisivat erityisesti sellaisiin teknisiin mittareihin, joiden avulla dataa on saatavilla helposti ja poikkeamia pystytään tunnistamaan. Tekniset mittarit keskittyvät haavoittuvuuksien ja poikkeamien seurantaan ja teknisten mittareiden käyttö ja seuraaminen koettiin suhteellisen helpoksi ja sujuvaksi sen takia että ne tulevat usein teknisten ratkaisujen mukana valmiina. Vaikka henkilöstöä on ohjeistettu, mittarit voivat auttaa todentamaan, toimitaanko ohjeiden mukaisesti. Jos näin ei ole, voidaan puuttua tilanteeseen joko suoraan loppukäyttäjien kanssa tai tarjoamalla kohdennettua tietoturvakoulutusta. Ilman seurantaa, valvontaa ja mittareita tietoturvakoulutus voi jäädä liian yleiselle tasolle, eikä viesti välity tehokkaasti loppukäyttäjille. Kun taas on dataa, joka osoittaa esimerkiksi arkaluontoisen tiedon lähettämistä järjestelmästä ulos, voidaan tarkastella, pitäisikö puuttua suoraan tiettyyn tapaukseen vai lähettää yleinen muistutusviesti kaikille. Haasteena teknisissä mittareissa korostui järjestelmien välisen integraation puute. Kun kaikkien järjestelmien keskinäinen integrointi ei ole mahdollista, käyttäjien on siirryttävä useiden eri järjestelmien välillä saadakseen tarvitsemansa tiedot raporteista.

Lähes kaikki haastateltavat olivat yhtä mieltä siitä, että tietoturvakulttuurin mittaaminen on haastavaa. Hallinnollisempien mittareiden osalta useat käyttivät esimerkiksi tietoturvakoulutuksiin osallistumista mittarina. Myös kalasteluhyökkäysten simulointiharjoitusten tuloksista on saatu dataa tietoturvakulttuurin mittareihin. Yksi haastateltava mainitsi myös heillä puolen vuoden välein järjestettävät ja ISO27001-standardin vaatimuksen mukaiset sisäiset auditoinnit tärkeänä välineenä tietoturvakulttuurin mittaamisessa. Auditoinneissa on esimerkiksi selvitetty miten ohjeistuksia ja käytäntöjä on omaksuttu ja heillä oli hyviä kokemuksia siitä, kuinka muutaman vuoden jälkeen yleinen tietoturvatietoisuus oli saatu nostettua vahvemmaksi organisaatiossa.

3.16 Haasteet jalkauttamisessa

Eräs haastateltava nosti tietoturvaprosessien jalkauttamisen suurimmaksi haasteeksi muutosvastarinnan, joka syntyy työntekijöiden huolesta lisääntyneestä työmäärästä, työvelvoitteista ja mahdollisesta vaikutuksesta heidän pääasiallisiin työtehtäviinsä. Tämä koetaan realistisena ongelmana, joka voi estää prosessien sujuvan toteutuksen. Haastateltava kertoo, että työntekijät saattavat tuntea, että uudet tietoturvaprosessit tekevät heistä kiireisempiä ja estävät heitä suorittamasta päätehtäviään, mikä johtaa helposti muutosvastarintaan. Tämän seurauksena organisaatiot joutuvat pohtimaan, onko prosessien toteuttaminen mahdollista tehdä helpommaksi tai automatisoidummaksi. Konkreettisena esimerkkinä automatisaatiosta haastateltava viittaa Liitteen 1 ensimmäiseen esimerkkiin automaattisen sähköpostien salauksen käyttöönotosta. Kun automaatio tai yksinkertaistaminen ei ole mahdollista ja prosessit vaativat lisätyötä, paineiden hallinta ja viestintä nousevat keskeisiksi haasteiksi. Haastateltava korostaa, että tärkeää on johdon ja esihenkilöiden tuki sekä

selkeä kommunikaatio siitä, miksi tietyt prosessit ovat tärkeitä ja miten ne vaikuttavat työntekijöiden arkeen. Tietoturvastressin hallinta ja työntekijöiden huolenaiheiden vähentäminen vaativat, että johto antaa selkeitä perusteluita muutoksille ja pyrkii integroimaan tietoturvatehtävät osaksi normaalia työpäivää ilman, että se koetaan lisätaakkana. Isoissa organisaatioissa haasteisiin vastataan yleensä hakemalla tukea johdolta ja korostamalla johdon päätösten välttämättömyyttä, mikä ei aina ole elegantti ratkaisu, mutta on tarpeellinen massiivisissa organisaatioissa. Pienemmissä organisaatioissa, joissa on henkilökohtaisempi suhde työntekijöihin, haasteisiin voidaan vastata eri tavoin, ottaen huomioon ihmisluonteen pyrkimyksen harmoniaan ryhmissä.

Eräässä pienemmässä organisaatiossa työskentelevän haastateltavan mukaan tietoturvaprosessien jalkauttamisessa suurimmat haasteet ilmenivät prosessien kuvaamisessa, niiden noudattamisessa ja dokumentoinnissa. Vaikka tekniset ratkaisut ymmärrettiin hyvin, prosessien määrittely, muutosten hallinta ja niiden dokumentointi toivat haasteita. Esimerkiksi tietoturvapoikkeamien tai -häiriöiden ilmoittamisen prosessi voi olla teoriassa yksinkertainen, mutta käytännössä haastava. Hän kuvasi tilanteen, jossa esimerkiksi IT-järjestelmässä ilmenee häiriö, josta järjestelmä kyllä antaa hälytyksen asianosaisille, mutta hälytyksen saajat eivät ilmoita tästä eteenpäin määritellyn sisäisen prosessin mukaisesti, joko huolimattomuuden, ymmärryksen puutteen tai prosessien laiminlyönnin vuoksi. Vaikka tekninen järjestelmä toimii oikein havaitessaan poikkeaman, organisaation sisäinen prosessi pettää, eikä poikkeamaa käsitellä suunnitellulla tavalla. Myös dokumentointi nähtiin yleisenä haasteena. Esimerkiksi erilaisten konfiguraatioiden muutoksen yhteydessä voi olla ajansäästöllisistä syistä houkuttelevaa ohittaa nykytilan dokumentointi, vaikka prosessit edellyttäisivät tarkkaa kirjaamista muutosten yhteydessä. Nämä esimerkit korostavat tarvetta viestiä selkeästi prosessien tarkoituksesta ja niiden merkityksestä.

ISO27001-standardin vaatimukset, kuten riskienhallinta, sisäinen auditointi ja jatkuva parantaminen, nostettiin myös esille haasteina, jotka vaativat erityistä huomiota. Vaikka nämä prosessit ovat vaativia, ovat ne myös äärimmäisen tärkeitä organisaation tietoturvan kannalta. Haasteet liittyivät erityisesti laajempiin prosesseihin, joissa useiden ihmisten tulee toimia yhdessä, verrattuna teknologian käyttöönottoon, joka koettiin helpommaksi. Eräs haastateltava kertoi, että tietoturvan jalkauttamisprosessi meni yllättävän hyvin heidän organisaatiossaan, ilman merkittäviä poikkeamia ensimmäisessä auditoinnissa. Haasteeksi muodostui kuitenkin prosessin ylläpito ja jatkuva parantaminen sertifikaatin saamisen jälkeen. Motivaation ylläpitäminen ja tiukka linja tietoturvan suhteen puoli vuotta sertifikaatin saamisen jälkeen sujui hyvin, mutta myöhemmin saatettiin huomata, että tietyt toimet, kuten riskienarviointi, oli toteutettu liian nopeasti tai poikkeamiin ei oltu reagoitu asianmukaisesti. Haastateltava koki haasteita tasapainoillessa tietoturvan hallintajärjestelmän ylläpidon ja muiden työtehtävien välillä. Resurssit jouduttiin jakamaan näiden kahden kesken, mikä aiheutti vaikeuksia. Lisäksi johto saattaa olettaa, että työntekijöillä olisi lisäkapasiteettia suurten projektien

päätyttyä, mikä ei aina vastaa todellisuutta. Tämä johtaa tilanteisiin, joissa työntekijöiden odotetaan ylläpitävän tietoturvan hallintajärjestelmää samalla, kun heidän pitää hoitaa muita kasvaneita työtehtäviä, mikä asettaa paineita heidän työkapasiteetilleen. Haastateltava korosti, että jatkuva parantaminen ja tiimin säännölliset kokoukset ovat olennaisia ISO27001-standardin ja muiden laatuvaatimusten täyttämiseksi, koska sertifikaatin menettäminen on mahdollista, jos ylläpitotoimia ei tehdä asianmukaisesti. Tämä osoittaa, että tietoturvan jalkauttamisen haasteet eivät rajoitu pelkästään alkuvaiheeseen, vaan myös ylläpito ja jatkuva kehittäminen ovat keskeisiä onnistumisen kannalta.

4 Uuden toimintamallin kehittäminen

Tämän opinnäytetyön toisena tavoitteena oli kehittää teoreettisen viitekehyksen ja haastatteluissa ilmenneen tiedon pohjalta uusi, toimiva ja tietoon perustuva toimintamalli, jota voitaisiin hyödyntää jatkossa tietoturvaprosesseja jalkauttaessa. Alussa haluttiin siis luoda malli sille, mitä jalkauttamistapaa kannattaisi käyttää missäkin tilanteessa. Toimintamallin oli tarkoitus perustua teoreettisessa viitekehyksessä esiin tulleisiin sekä haastatteluissa tunnistettuihin tekijöihin, jotka vaikuttavat tietoturvan jalkauttamiseen. Opinnäytetyötä kirjoittaessa ja tiedon lisääntyessä kuitenkin tuli ilmi, että tietoturvan jalkauttaminen kaikkiin organisaatioihin yhtenäisen toimintamallin kautta olisi vähintäänkin haastavaa, koska kuten haastatteluissa ilmeni, jalkauttamiseen vaikuttaa hyvin moni asia, kuten muun muassa organisaation koko, ikä, toimiala ja sen vaatimukset, erilaiset työskentelykulttuurit, johtaminen, budjetti ja muut resurssit. Tämän lisäksi mallia sille, mitä jalkauttamistapaa kannattaisi käyttää missäkin tilanteessa oli liki mahdoton luoda, kun tuloksista selvisi, että hallinnolliset ja tekniset keinot täydentävät toisiaan, jolloin ideaalitilanteessa molempia keinoja käytetään, eikä vain toista. Oli siis hyvin hankala luoda yhtä ja ainoaa toimintamallia, joka toimisi tehokkaasti jokaisessa organisaatiossa ja jokaisessa tilanteessa.

Konstruktiiviseen tutkimukseen kuuluu uuden ratkaisun toimivuuden arviointi markkinoilla tai kohdeorganisaatiossa ja myös uuden ratkaisun testaamista esikokein suositellaan. (Ojasalo ym., 2014, 67–68) Ennen kuin lopullinen malli syntyi, olin luonnostellut alustavan mallin teoreettisen viitekehyksen pohjalta. Alkuperäinen malliluonnos näytettiin myös osalle haastateltavista haastatteluiden lopuksi ja useammilta tuli palautetta liittyen siihen, että malli näytti liian raskaalta ja monivaiheiselta, eikä siltä, että se sopisi eri kokoisiin organisaatioihin, jolloin sitä tuskin olisi hyödynnetty. Toteutus olisi vaatinut vähintäänkin pienille ja suurille organisaatioille omat mallinsa.

Tästä syystä yhtenäisen toimintamallin vaatimuksia päätettiin keventää, jotta opinnäytetyöstä kuitenkin syntyisi jokin konkreettinen ja hyödyllinen lopputuotos. Koska tietoturvan jalkauttamiseen vaikuttavia tekijöitä oli kuitenkin tunnistettu ihan kiitettävästi, lopullinen toimintamalli keskittyi prosessin alkuvaiheeseen, eli suunnitteluun ja siihen, millaisia asioita on hyvä ottaa huomioon silloin kun lähdetään miettimään jalkauttamisen prosessia. Tämä ”muistilista” voi helpottaa organisaatioita omien prosessiensa suunnittelussa, varsinkin jos muutoksen toteuttaja on tullut esimerkiksi aivan uutena organisaatioon, eikä tunne vielä niin hyvin sen erityispiirteitä.

Kuten haastatteluissakin ilmeni, jalkauttamistapa riippuu aina kyseisestä käytännöstä. Jotkin käytännöt saattavat vaatia vain politiikan ja ohjeiden päivityksen ja koulutuksen, kun taas isommat muutokset saattavat vaatia paljon järeämmät tekniset keinot. Ennen kuin konkreettista muutosta lähdetään tekemään, on tärkeää, että tapahtuva muutos suunnitellaan perusteellisesti ja mietitään konkreettisesti, mitä ollaan lähdössä tekemään. Suunnitteluvaihe antaa perustan tuleville

toimenpiteille ja varmistaa sen, että muutos johtaa haluttuihin tuloksiin. Suunnitteluvaiheen apuna voi käyttää seuraavien kappaleiden lopussa olevia kysymyksiä. Nämä varmistavat, että oleellisimmat näkökohdat tulevat käsitellyiksi ennen toteutusvaihetta. Mallista on tehty myös visuaalisempi tiivis muistilistaversio, joka löytyy liitteestä 2.

4.1 Jalkauttamiseen vaikuttavien tekijöiden tunnistaminen

Alussa on hyvä tunnistaa ja ymmärtää organisaation erityispiirteet ja ne tekijät, jotka vaikuttavat merkittävästi siihen, miten jalkauttamista lähdetään tekemään. Näitä tekijöitä ovat muun muassa organisaation koko, ikä, toimiala, työ- ja tietoturvakulttuuri, johtamisen tavat sekä käytettävissä olevat resurssit. Vaikka nämä tekijät vaihtelevat organisaatiokohtaisesti, niiden tunnistaminen ja ymmärtäminen on kriittistä muutosstrategiaa miettiessä, sillä niillä on suuri merkitys jalkauttamistavan valintaan, organisaation muutoksensietokykyyn ja siihen, millaisia odotuksia organisaatiolle voidaan asettaa.

Tutkimustuloksista ilmeni, että hallinnolliset ja luottamuspohjaiset keinot saattavat toimia pienissä organisaatioissa paremmin kuin isoissa, johtuen henkilökohtaisemmista ihmissuhteista ja ihmisten luontaisesta pyrkimyksestä pienen ryhmän sisäiseen koheesioon ja yhteisten tavoitteiden saavuttamiseen. Myös valvonta voi olla helpompaa pienessä organisaatiossa. Pienissä ja nuorissa organisaatioissa etuina on niiden ketteryys ja nuorissa erityisesti se, että kun prosessit luodaan alusta asti uusina, muutosvastarinta voi olla vähäisempää. Suurissa organisaatioissa hallinnollisten keinojen käyttö yksinään voi olla jo paljon haastavampaa, kun kaikki ihmiset eivät voi mitenkään tuntea toisiaan, jolloin samanlaisia joukkoon kuulumisen ja sääntöjen noudattamisen paineita ei välttämättä ole. Tällöin muutoksen toteutus voi vaatia alusta asti järeämpiä teknologisia keinoja, joilla poistetaan ihmisten väärinkäytösten riski. Myös toteutuksen valvonta on paljon mutkikkaampaa johtuen suuresta henkilömäärästä ja mahdollisista useista eri sijainneista.

Myös toimialalla, työ- ja turvallisuuskulttuurilla saattaa olla vaikutuksia jalkauttamistavan valintaan. Tutkimustulokset osoittivat, että teknologiaorientoituneiden yritysten oli helpompaa ja luonnollisempaa toteuttaa teknisiä toimenpiteitä. Teknologia- ja turvallisuusalan organisaatiot voivat myös asettaa henkilöstölleen paljon korkeampia odotuksia teknisen osaamisen ja tietoturvan suhteen. Toimiala siis vaikuttaa vahvasti organisaation tietoturvakulttuuriin. Työkulttuurin vaikutus saattaa taas näkyä esimerkiksi siinä, että työntekijöille asetetaan korkeita tehokkuus- tai laskutusvaatimuksia. Jos tietoturvavaatimukset hidastavat tai estävät vaatimusten täyttämisen, muutosvastarinta voi kasvaa. Tällöin työntekijät mahdollisesti ohittavat tietoturvaan liittyvät prosessit, eli rikkovat sääntöjä ja oikeuttavat tämän tekemisen omassa päässään Siposen ja Vancen tutkimuksessa (2010, 287–498) mainituilla neutralisointitekniikoilla. Darcyn & Greenen (2014, 484-486) tutkimus osoitti, että työntekijöiden työtyytyväisyys myös vaikuttaa heidän aikomuksiinsa noudattaa

tietoturvakäytäntöjä, joten organisaation on myös tiedostettava tämä muutosta suunnitellessa. Jos esimerkiksi organisaatiossa on käynnissä isoja strategisia muutoksia tai vaikka muutosneuvottelut, jolloin työntekijät todennäköisesti ovat tyytymättömiä, voi tällä olla suuri vaikutus siihen, saadaanko tietoturvakäytäntöihin liittyvää muutosta tapahtumaan.

Johtamisen vaikutuksia jalkauttamiseen kannattaa pohtia myös erittäin syvällisesti, sillä sekä teoria että haastatteluiden tulokset olivat samaa mieltä siitä, että johtamisella on erittäin suuri merkitys tietoturvan kehittämiseen ja tietoturvaa kannattaa kehittää ylhäältä alas -lähestymistavalla, jolloin tietoturvan tavoitteet eivät ole ristiriidassa liiketoiminnan muiden tavoitteiden kanssa. Kuten teoreettisessa viitekehyksessä esitetyn Hun ym. (2012, 647–648) tutkimus osoitti, ylimmän johdon osallistuminen oli merkittävin ulkoinen tekijä, joka vaikutti työntekijöiden käyttäytymiseen. Myös haastateltavat korostivat johtamisen merkitystä jalkauttamisessa. Johdon on oltava sitoutunut muutokseen ja näytettävä omalla esimerkillään mallia työntekijöille, sillä tämä vaikuttaa suuresti heidän muutoksensietokykyyn. Johdon on ymmärrettävä prosessin kriittisyys ja varmistettava, että muutoksen toteuttamiseen on osoitettu riittävästi henkilöstöä, aikaa ja taloudellisia resursseja. Tämä vaatii sen, että johdolle myös selitetään tarpeeksi selkeästi, mitkä prosessin riskit ovat.

- Millaisia hyötyjä tai haasteita organisaation kokoon liittyy?
- Ymmärtääkö johto selkeästi mitä varten muutosta tarvitaan?
- Onko johto sitoutunut edesauttamaan muutosta omalla toiminnallaan, esimerkillään ja viestinnällään?
- Onko johto valmis resursoimaan tarpeeksi henkilöstöä, aikaa ja rahaa niin muutoksen toteuttamista kuin sen valvontaa varten?
- Miten työntekijät suhtautuvat muutoksiin?
- Ymmärtävätkö työntekijät tietoturvan merkityksen heidän päivittäisissä työtehtävissään?

4.2 Kriittisyyden ja riskien arviointi

Haastatteluista kävi ilmi, että suurin osa prosesseista lähtee riskiarvioinnista. Ennen muutoksen toteuttamista on tärkeää tunnistaa mahdolliset riskit ja haasteet, jotka voivat syntyä siitä, että muutosta ei toteuteta, eli arvioitava tietoturvakäytännön tai -prosessin kriittisyys. Riskiarvioinnissa voidaan hyödyntää organisaation itse määrittelemää riskiarviointiprosessia, jossa arvioidaan riskin todennäköisyys ja vaikutukset. Prosessin kriittisyys ja riskit vaikuttavat kuitenkin suuresti siihen millaisilla resursseilla muutosta lähdetään toteuttamaan ja ne auttavat muutoksen tarpeen perustelemisessa johdolle. Jos kyseessä on pieni toimintatapojen muutos, johon ei liity suurta riskiä esimerkiksi ihmisten väärinkäytöksestä, muutos ei välttämättä vaadi muuta kuin muutaman hallinnollisen toimenpiteen, eli ohjeistuksen päivityksen ja kouluttamisen. Jos muutokseen liittyy merkittävä riski

siitä, että ihmiset eivät toimi ohjeiden mukaisesti, mikä taas voi johtaa vakaviin tietoturvaloukkauksiin, on järkevämpää kehittää monitasoisempia turvatoimia ja miettiä hallinnollisten keinojen lisäksi myös teknisiä keinoja.

Kriittisyyttä ja riskejä pohdittaessa voidaan käydä läpi vastaukset seuraaviin kysymyksiin:

- Kuinka kriittinen prosessi on?
- Mitkä ovat riskit, joita muutoksella lähdetään pienentämään tai poistamaan?
- Mitkä ovat riskin vaikutukset toteutuessaan?
- Kuinka todennäköisesti riski toteutuu?
- Mitkä tekijät vaikuttavat riskiin?

4.3 Tavoitteiden määrittely

Kriittisyys- ja riskiarvioinnin jälkeen määritellään selkeät tavoitteet, jotka ohjaavat muutosprosessia ja valmistelevat myös valvonnan ja mittareiden sekä viestintästrategian miettimiseen. Tavoitteen on oltava erittäin selkeä, jotta kaikki sidosryhmät ymmärtävät, mitä muutoksella pyritään saavuttamaan. Teoreettisessa viitekehyksessä mainitun Hun ym. (2012, 647) tutkimuksen mukaan selkeitä sääntöjä ja tavoitteita painottava organisaatiokulttuuri vaikuttaa olennaisesti työntekijöiden suhtautumiseen tietoturvaan. Tutkimus osoitti, että kun organisaatiossa määritellään tavoitteet ja toimintatavat tarkasti ja niitä arvostetaan, työntekijöiden halukkuus noudattaa tietoturvakäytäntöjä kasvaa.

Tavoitteita miettiessä voidaan käyttää seuraavia kysymyksiä:

- Mikä on tavoitteen konkreettinen lopputulos?
- Onko tavoite selkeä ja ymmärrettävä?

4.4 Hallinnollisten keinojen suunnittelu

Kuten haastatteluista ilmeni, hallinnolliset keinot ovat aina läsnä, sillä teknisenkin ratkaisujen taustalla on usein jokin ylätason tietoturvapolitiikka tai vastaava. Tämän takia hallinnollisten keinojen miettimistä ei voida ohittaa täysin, vaikka mietitäänkin teknistä toteutusta. Teknisetkin toteutukset vaativat dokumentointia ja kuten eräs haastateltava totesi kysyttäessä suurimmista haasteista, niin teknisten ratkaisujen ymmärtäminen ei tuottanut ongelmia, mutta prosessin määrittely, muutosten hallinta ja niiden asianmukainen dokumentointi olivat vaikeita. Tämän haasteen välttääkseen on siis hyvä suunnitella myös, mitä kirjallista dokumentaatiota tarvitaan prosesseista, nykytilasta ja tulevaisuudesta.

Haastateltavat korostivat selkeyden merkitystä henkilöstön ohjeistamisessa ja erään haastateltavan organisaatiossa oli hyviä kokemuksia tietoturvaohjeistuksen tiivistämisestä 20-sivuisesta 10-sivuiseksi. Tiivistetyt ja ymmärrettävät ohjeistukset lisäävät todennäköisyyttä, että työntekijät todella lukevat ja noudattavat niitä, sillä ne ovat helpommin omaksuttavissa käyttäjäystävällisyytensä vuoksi. Ohjeistuksia päivittäessä on siis hyvä muistaa pitää ne tiiviinä ja äärimmäisen selkeinä, jotta ihmiset eivät käyttäisi Siposen ja Vancen tutkimuksessa (2010, 287–498) lueteltuja neutralisointitekniikoita, kuten esimerkiksi vastuun kieltämistä, jolloin henkilö oikeuttaa toimintansa sillä, että tietoturvakäytäntö on epäselvä. Myös Darcyn ym (2014, 288–289) tutkimuksessa kehotettiin välttämään jargonia ja tekemään helposti ymmärrettäviä ohjeita, jotta ihmisille ei synny monimutkaisuuteen liittyvää tietoturvastressiä.

Teoriaosiossa painotettiin, että tietoturvakoulutus ja tietoturvatietoisuuden kehittäminen parantaa niin henkilöstön asenteita kuin työntekijöiden itsetehokkuutta. Koulutusten suunnitteluun kannattaa panostaa ja myös monialaista lähestymistapaa kannattaa harkita, varsinkin jos IT-asiantuntijat eivät ole kovin vakuuttavia esiintyjiä tai kokeneita kouluttajia. Jos tuleva muutos on kovin iso ja vaatii esimerkiksi paljon työtapamuutoksia henkilöstöltä, on myös johdon hyvä olla koulutuksissa läsnä korostamassa asioiden tärkeyttä. Räätälöityjen ja kohdennettujen tietoturvakoulutusten järjestämistä on hyvä miettiä, sillä niin teoria kuin haastattelutkin antoivat ymmärtää, että kohdennettu tai räätälöity tietoturvakoulutus on tehokas tapa jalkauttaa. On turha kouluttaa koko henkilöstölle sellaisia prosesseja tai järjestelmiä, jotka eivät liity heidän työtehtäviinsä. Teoreettisessa viitekehyksessä muutamakin lähde suositteli räätälöimään myös koulutuksen mahdolliset esimerkkiskenaariot tai harjoitukset vastaamaan työntekijöiden konkreettisia työtehtäviä, jolloin ne ovat henkilökohtaisesti merkityksellisempiä koulutettaville ja oppiminen muuttuu käytännönläheisemmäksi ja tuloksekkaammaksi.

Seuraavia kysymyksiä voidaan käyttää hallinnollisia keinojen pohtimisen tukena:

- Millaisia hallinnollisia keinoja (tietoturvapolitiikan päivittäminen, ohjeistaminen, kouluttaminen, testaaminen) muutoksen toteuttaminen vaatii?
- Ovatko ohjeet tarpeeksi selkeät ja ymmärrettävät?
- Riittävätkö hallinnolliset keinot yksinään?
- Onko hallinnollisten keinojen toteutumista mahdollista valvoa?

4.5 Teknisten keinojen suunnittelu

Haastateltavat suosivat teknisten hallintakeinojen käyttämistä aina kun se on mahdollista, varsinkin jos niillä voidaan pienentää ihmisen väärinkäytöksen tai manuaalisten virheiden riskiä. Teknisillä rajoituksilla voidaan täysin poistaa riski siitä, että joku toimisi ohjeiden vastaisesti, mikä yleensä on

organisaation tahtotila. Teknisten keinojen käyttäminen voi olla myös perusteltavaa tehokkuussyistä, jos sillä voidaan poistaa jokin manuaalinen prosessi, joka lisää työntekijöiden työmäärää. Tällä vältetään myös liiallisen tietoturvastressin aiheuttaminen työntekijöille. Teknisiä järjestelmiä kartoittaessa voidaan käyttää apuna haastateltavien mainitsemia teknisten ratkaisujen valintakriteereitä, jotka löytyvät kappaleesta 3.12.

Haastateltavien mukaan tekniset keinot eivät kuitenkaan aina toimineet yksin, sillä tekninen prosessi, kuten eräänä esimerkkinä esitetty pääsyoikeuksien hallintaprosessi, voi kuitenkin vaatia myös hallinnollisen tarkistusprosessin ja manuaalista työtä, jotta se ottaisi kaikki tilanteet huomioon. Myös toisen haastateltavan esittämä esimerkki siitä, kun IT-järjestelmä antaa hälytyksen tietoturvapoikkeamista tai -häiriöistä, mutta hälytyksen saaja ei ilmoita tästä oikeaoppisesti eteenpäin, korostaa hallinnollisten taustaprosessien tärkeyttä teknisten keinojen tukena.

Alla olevia kysymyksiä voidaan käyttää tukena teknisiä keinoja mietittäessä:

- Onko tavoite mahdollista saavuttaa myös teknisin keinoin (esim. rajoittamalla käyttäjien tekemistä, automaatiolla tai ottamalla käyttöön järjestelmiä)?
- Onko teknistä prosessia mahdollista valvoa?
- Millaisia hallinnollisia prosesseja tekninen keino vaatii?
- Täyttyvätkö teknisten ratkaisujen valintakriteerit (kappaleessa 3.12)?

4.6 Valvonnan ja mittauksen suunnittelu

Teknisten prosessien valvonta saattaa olla helpompi järjestää, sillä kaikesta digitaalisesta tekemisestä jää aina jälki, jolloin lokien seuraaminen onnistuu. Useampi haastateltavista mainitsi käyttävänsä sellaisia teknisiä mittareita, jotka tulevat tiettyjen liiketoimintasovellusten tai virustorjuntatuotteiden mukana. Järjestelmien mukana on nykyisin hyvin usein jonkinnäköinen raportointi- tai valvontaominaisuus, jolla pystyy seuraamaan järjestelmien käyttöä.

Valvonta koettiin ennemmin hallinnollisten keinojen heikkoudeksi, sillä pelkkiä hallinnollisia keinoja käyttämällä on vaikea todentaa, että ihmiset totisesti toimivat ohjeiden mukaisesti. Laaksosen ym. (2006, 278–279) mukaan, työntekijöiden käyttäytymisen mittaaminen on hyvä tapa mitata hallinnollisten toimenpiteiden tehokkuutta. Mittauksen tulosten tulisi edustaa laajempaa joukkoa ja mittaaminen ei saisi herättää työntekijöissä negatiivisia tai syyllisyyden tunteita. Esimerkkeinä hän mainitsi työasemien lukitsemisen tarkastamisen tai tietoturvatietämyksen testaamisen esimerkiksi kyselyiden avulla. Haastatteluissa kävi ilmi, että organisaatioilla on harvemmin resursseja valvoa niin tehokkaasti työntekijöitään. Jos käytännön toteutumista ei voida valvoa ja todistaa esimerkiksi teknisillä raporteilla, että ihmiset toimivat ohjeiden mukaisesti, on jonkinnäköinen testaus kuitenkin

hyvä suunnitella, jotta voidaan varmistua siitä, että ihmisten käyttäytymisessä on tapahtunut muutosta. Henkilöstön osaamisen testaus esimerkiksi digitaalisilla kyselytyökaluilla ei vaadi suuria investointeja, vaikkakin se vaatii jonkun valvomaan ja koordinoimaan vastauksia. Testaamisen voi myös ulkoistaa siihen erikoistuville palveluntarjoajille, kuten osa haastateltavistakin teki.

Valvontaa ja miettiessä voidaan kysyä seuraavat kysymykset:

- Miten onnistumista mitataan?
- Ovatko mittarit päteviä, merkityksellisiä ja kuvastavatko ne todellisuutta?
- Voiko mittareista johtaa järkeviä toimenpiteitä?

4.7 Resursointi ja budjetointi

Ajan, osaamisen ja resurssien puute tekee tietoturvan jalkauttamisesta haastavaa. Nykyorganisaatioiden työntekijöillä on useita eri velvoitteita ja henkilöresurssien pula on todellisuudessa yleistä. Tämä on hyvä tiedostaa jo suunnitteluvaiheessa, jotta tarpeet mietitään ennen kuin lähdetään toteuttamaan muutosta. Jos organisaatiolla ei ole tarpeeksi omia henkilöstö-, aika- tai asiantuntemusresursseja, on hyvä myös pohtia ulkoistamista tai konsulttiavun pyytämistä, josta haastateltavilla oli positiivisia kokemuksia. Organisaatioiden on myös mietittävä taloudellisia resurssejaan. Vaikka ennaltaehkäiseminen on varmasti edullisempaa kuin vahingon korjaaminen, voivat tietoturvaprojektit erityisesti teknologian osalta tulla organisaatioille hyvinkin kalliiksi ja erityisesti isoissa organisaatioissa päätöksen läpivienti saattaa olla hidasta, kun mukaan pitää ottaa hankintaosastojen useat hyväksyntäkierrokset.

Resursoinnin ja budjetoinnin miettimisen tukena voidaan käyttää seuraavia kysymyksiä:

- Onko organisaatiolla tarvittavasti sisäisiä resursseja (henkilöstö, asiantuntemus, teknologia ym.) muutoksen toteuttamiseen ja toteutuksen valvontaan vai tarvitaanko myös ulkopuolista apua ja lisähankintoja?
- Mitä resursseja tarvitaan muutoksen toteuttamiseen ja valvomiseen ja paljonko projektiin menee aikaa?
- Mitkä ovat mahdollisten lisähankintojen kustannukset ja millainen tuotto tai lisäarvo sijoituksesta saadaan?

4.8 Muutoksen vaikutusanalyysi ja pilotointi

Mahdollisimman käyttäjäystävällisen muutoksen toteuttaakseen, on tärkeä käyttää aikaa myös sen pohtimiseen, miten muutos tulee konkreettisesti näkymään henkilöstön työssä. Muutos ei saisi haitata työntekijöiden työntekoa tai olla ristiriidassa heidän työtehtävien päätavoitteiden kanssa, joissa heitä mitataan. Jos esimerkiksi uuden prosessin myötä työntekijöiden työnteko hidastuu, on riskinä

se, että prosessi pyritään ohittamaan ja henkilöstö tulee toimimaan ohjeiden vastaisesti. Samoin, jos uuden järjestelmän käyttö edellyttää esimerkiksi päivittäin toistuvia kirjautumisia ja monivaiheista tunnistautumista käyttäen eri laitteita, voi motivaatio sen käyttöön merkittävästi heikentyä. Jos prosessi kuitenkin on välttämätöntä toteuttaa ja se vaatii ylimääräistä työaikaa henkilöstöltä, on huolehdittava siitä, että johto tai esihenkilöt allokoivat heille enemmän aikaa tietoturvavelvoitteidensa suorittamiseen.

Pilotointi tarjoaa mahdollisuuden testata ja arvioida uutta prosessia tai järjestelmää ennen laajempaa käyttöönottoa. Pilotointi on hyvä tapa testata muutosta käytännössä ja saada uutta näkökulmaa oman pohdinnan tueksi. Kun testataan prosessia ensin pienemmällä käyttäjäryhmällä, voidaan mahdolliset ongelmat tunnistaa ja korjata ajoissa ennen käyttöönottoa. Tämä lisää projektin onnistumisen mahdollisuuksia. On tärkeää, että pilotointivaiheeseen osallistuu monenlaisia käyttäjiä ja eri tehtävissä toimivia henkilöitä, jotta muutoksen eri vaikutukset voidaan ymmärtää mahdollisimman laajasti.

Muutoksen vaikutuksia miettiessä voidaan käyttää näitä kysymyksiä:

- Miten muutos tulee vaikuttamaan henkilöstön työtapoihin, käyttökokemukseen, työmäärään, tietoturvastressiin, organisaation tietoturvakulttuuriin?
- Mitkä ovat mahdolliset haasteet, joita muutoksesta voi seurata?

4.9 Viestintästrategian suunnittelu

Ennakoitu ja kohdennettu viestintä auttaa välttämään suuren muutoskuorman syntymisen. Kun viestintä aloitetaan hyvissä ajoin ja keskitytään olennaisen tiedon jakamiseen oikeille kohderyhmille oikeassa kohtaa, voidaan tarpeeton hämmennys ja muutosvastarinta minimoida. Selkeä viestintä edistää lisäksi ymmärrystä ja myönteistä suhtautumista muutoksiin parantaen näin myös tietoturvakulttuuria. Kun henkilöstölle selitetään muutosten syyt ja ne esitetään selkeästi ja johdonmukaisesti, on todennäköisempää, että he omaksuvat uudet toimintatavat ja suhtautuvat muutoksiin positiivisesti. Tietoturvan kaltaisella kriittisellä alueella tämä on erityisen tärkeää.

Seuraavat kysymykset auttavat viestintästrategiaa miettiessä:

- Ketkä kuuluvat viestinnän kohderyhmiin?
- Mitä tietoa kohderyhmät tarvitsevat ymmärtääkseen muutoksen merkityksen?
- Milloin on paras aika viestiä muutoksista?

4.10 Muutoksen aikataulutus ja vastuutus

Lopuksi, kun tulevasta muutoksesta on parempi käsitys, voidaan muutoksen toteuttamista alkaa aikatauluttamaan ja vastuuttamaan. Haastateltavat korostivat, että jokaiselle käytännölle olisi nimettävä vastuuhenkilö, oli se sitten teknologinen tai hallinnollinen, muuten toteutus voi jäädä epämääräiseksi. Sekä teoriassa että haastatteluissa korostui erityisen paljon se, että kaikkien on ymmärrettävä mikä heidän vastuunsa on ja mitä heiltä odotetaan. Darcyn & Greenen (2014, 484-486) tutkimuksessa havaittiin, että työntekijät saattavat laiminlyödä tietoturvakäytäntöjä, koska he luottavat IT-osaston hoitavan ongelmatilanteet. Tämän takia erityisesti työntekijöille on korostettava heidän omaa vastuutaan organisaation tietoturvan toteutumisesta.

Seuraavia kysymyksiä voi miettiä vastuunjakoa suunnitellessa:

- Kuka on vastuussa projektin läpiviennistä, diplomatiasta ja yleisestä koordinoinnista?
- Kuka on vastuussa muutoksen dokumentoinnista ja politiikka- ja ohjedokumenttien päivittämisestä?
- Kuka on vastuussa muutoksen viestinnästä ja kouluttamisesta?
- Mitkä ovat johdon tai esihenkilöiden vastuut?
- Mitkä ovat työntekijöiden vastuut?

5 Johtopäätökset

Tässä opinnäytetyössä tutkittiin ilmiötä, joka liittyy tietoturvan jalkauttamisen haasteisiin organisaatioissa. Organisaatioiden tietoturvatavoitteiden saavuttaminen voi epäonnistua inhimillisen toiminnan, kuten esimerkiksi ohjeiden noudattamattomuuden takia. Tutkimuksessa kiinnitettiin erityistä huomiota teknisiin ja hallinnollisiin keinoihin näiden haasteiden ratkaisemiseksi.

5.1 Yhteenveto

- K1 – Millaisilla eri keinoilla organisaatiot jalkauttavat tietoturvaprosesseja?

Organisaatiot jalkauttavat tietoturvaprosessejaan hallinnollisin ja teknisin keinoin ja tämä ilmeni niin teoreettisessa viitekehyksessä kuin myös haastattelujen tuloksista. Organisaatiot jalkauttivat prosessejaan joko omilla sisäisillä resursseillaan tai ulkopuolisia palveluntarjoajia käyttämällä. Hallinnollisia keinoja ovat muun muassa päätöksenteko, tietoturvapolitiikkojen ja ohjeiden luominen, viestintä, henkilöstön kouluttaminen sekä heidän osaamisensa testaus käytännön harjoitusten kautta. Organisaatiot järjestivät esimerkiksi harjoituksia, joissa simuloitiin huijausviestien tunnistamista, jotta henkilöstö oppisi tunnistamaan ja välttämään mahdollisia kalasteluhyökkäys-skenaarioita sekä ilmoittamaan näistä asianmukaisesti eteenpäin. Teknisiä keinoja voivat olla esimerkiksi erilaiset konfiguraatiomuutokset, käyttäjien toimien tekninen rajoittaminen, uusien järjestelmien käyttöönotto tai prosessien automatisointi. Teknisistä keinoista puhuttaessa on otettava huomioon se, että teknisten ratkaisujen potentiaali kasvaa erittäin nopeasti teknologian kehittyessä. Lähes kaikki haastateltavat olivat sitä mieltä, että teknisiä keinoja kannattaa käyttää aina, kun se on mahdollista, sillä teknologiaa hyödyntämällä voidaan parhaimmillaan pienentää riskiä siitä, että ihmiset eivät toimi tietoturvakäytäntöjen mukaisesti tarkoituksellisesti tai vahingossa sekä vähentää myös virheitä, joita voi koitua manuaalisista prosesseista.

Tutkimustulokset osoittivat, että organisaatiot ovat hyvin tunnollisia ISO/IEC 27001 -standardin mukaisia prosesseja ja tietoturvapolitiikkoja luodessaan, mutta käytännön elämässä prosessien ja käytäntöjen toteutumisen valvonta voi olla haastavaa. Esimerkiksi ohjeistuksien ja sääntöjen heikkoutena nähtiin se, että niiden noudattamisen seuranta vaatii paljon resursseja, joita organisaatioilla ei aina ole riittävästi käytössään. Teknisten ratkaisujen kohdalla taas heikkoutena voi olla se, että jos teknologiaan luotetaan liikaa, eikä prosessia valvota hallinnollisin keinoin, voi prosessissa ilmetä heikkouksia. Tämä huomattiin kahdessa esimerkissä. Yksi oli tietoturvaheikkouksien ilmoittamisen prosessi, jossa järjestelmä kyllä hälytti, mutta henkilö, jolle hälytys tuli, ei ilmoittanut hälytyksestä eteenpäin sisäisen prosessin mukaisesti. Toinen esimerkki automatisoidusta käyttöoikeuksien myöntö- ja hallinnointiprosessista havainnollisti sen, että alkuvaihe, eli oikeuksien anominen ja myöntäminen, oli helppo automatisoida, mutta kun pääsyoikeuksia pitäisi myös arvioida

uudelleen esimerkiksi työtehtävien muuttumisen yhteydessä tai työsuhteen päättyessä, on tämä hankalampaa toteuttaa ilman hallinnollista prosessia ja ihmistä, joka valvoo prosessia. Tärkeimpänä oivalluksena tutkimustuloksissa kuitenkin oli se, että hallinnolliset ja tekniset keinot täydentävät toisiaan ja integroimalla nämä prosessit organisaatiot voivat luoda kokonaisvaltaisia hallintajärjestelmiä, jotka tehostavat toimintaa.

- K2 – Mitkä tekijät vaikuttavat jalkauttamiseen?

Jalkauttamiseen vaikuttavia asioita tunnistettiin runsaasti niin teoreettisessa viitekehyksessä kuin myös empiirisessä osiossa. Tämän opinnäytetyön tutkimustuloksista ilmeni, että jalkauttamistavat valitaan aina käytännön ja sen vaatimusten mukaisesti. Toisinaan käytännöt edellyttävät vain politiikan ja ohjeistuksen päivittämistä, kun taas joskus tilanne vaatii järeämpiä teknisiä keinoja. Tutkimustuloksista nousi esille myös se, että tietyt organisaation erityispiirteet, kuten organisaation ikä, koko ja toimiala vaikuttavat jalkauttamistavan valintaan. Luonnollisesti myös käytettävissä olevat resurssit vaikuttavat siihen, millaisin keinoin tietoturvaa kehitetään. Uusissa organisaatioissa etuna on se, että toimintatavat voidaan määritellä alusta alkaen tiukasti, jolloin vältytään muutosvastarinnalta, mikä ilmenisi vanhemmissa organisaatioissa. Pienissä organisaatioissa on etuna prosessien luomisen ja muuttamisen ketteryys sekä helppo tiedonjako. Luottamuspohjaiset, hallinnolliset keinot saattavat toimia paremmin, kun ihmiset tuntevat toisensa paremmin ja pyrkivät ryhmän sisäiseen koheesioon ja harmoniaan. Hallinnolliset keinot saattavat toimia pienissä organisaatioissa paremmin. Myös käytäntöjen noudattamisen valvonta on helpompaa pienissä organisaatioissa, kun valvottavia on vähemmän. Isompien organisaatioiden kohdalla niin ihmisten tavoittaminen, kouluttaminen kuin myös käytäntöjen noudattamisen valvonta pelkästään hallinnollisin keinoin voi osoittautua erittäin haastavaksi, jolloin teknisten ratkaisujen käyttö voi olla perustellumpaa. Toimiala saattaa näkyä jalkauttamistavan valinnassa siten, että esimerkiksi turvallisuus- tai teknologiaorientoituneet organisaatiot voivat vaatia henkilöstöltään enemmän niin muutoksensietokyvyn kuin teknisen osaamisen osalta. He saattavat näin ollen asettaa hyvinkin tiukkoja tietoturvakäytäntöjä sekä suosia teknisiä keinoja erityisen paljon, sillä heille uuden teknologian käyttöönotto on helpompaa. Teknologisemmat organisaatiot saattavat kuitenkin luoda virheellisiä oletuksia omasta tietoturvan tasostaan luottamalla pelkästään teknisiin ratkaisuihin ja jättäen hallinnolliset prosessit taka-alalle ja jos prosessissa luotetaan liikaa teknologiaan ilman hallinnollista valvontaa, siinä voi ilmetä heikkouksia.

Johtaminen ja johdon sitoutuminen on erittäin oleellista tietoturvaprosessien jalkauttamisessa, teki sen sitten hallinnollisin tai teknisin keinoin. Sekä teoriaosiossa esitetyt tutkimukset että tämän tutkimuksen aineisto osoittivat, että tietoturvan kehittämisen tulee perustua ylhäältä alas -lähestymistapaan, jossa ylimmän johdon määrittelemät politiikat ohjaavat tietoturvakäytäntöjä. Tämä varmistaa sen, että tietoturva tukee organisaation muitakin tavoitteita ja mahdollistaa resurssien tehokkaan

käytön. Johdon tulee myös aktiivisesti ja näkyvästi korostaa tietoturvan tärkeyttä omassa viestinnässään sekä omalla esimerkillään, sillä johdon tuella on iso vaikutus työntekijöiden muutoksensietokykyyn, asenteisiin ja siihen, kuinka tunnollisesti he noudattavat itse käytäntöjä ja ohjeita. Tärkeä haastatteluissa ilmennyt havainto oli se, että myös johtoa on kuitenkin tuettava ymmärtämään heidän roolinsa tietoturvan edistämisessä muun muassa selittämällä heille asiat mahdollisimman selkeästi, sillä tämä lisää taas heidän motivaatiotaan tukea muutosta.

Myös organisaation työ- ja tietoturvakulttuureilla on merkitystä siihen, miten tietoturvakäytäntöjä jalkautetaan. Teoreettisessa viitekehyksessä korostui se, että ylimmän johdon sitoutumisen ja tehokkaan viestinnän lisäksi organisaation turvallisuuskulttuuriin vaikuttaa työntekijöiden työtyytyväisyys. Työtyytyväisyys lisää työntekijöiden motivaatiota noudattaa tietoturvakäytäntöjä, jolloin olisi suositeltavaa, että organisaation eri sidosryhmät, kuten esimerkiksi henkilöstöhallinto, otetaan mukaan tietoturvan kehittämisprojekteihin, sillä heillä saattaa olla parempi käsitys vallitsevasta yleistunnelmasta. Henkilöstöhallintoa suositeltiin otettavaksi mukaan muissakin tutkimuksissa, sillä monitieteellisellä lähestymistavalla voidaan kehittää kokonaisvaltaisempia ratkaisuja, jotka ottavat huomioon teknisten seikkojen lisäksi myös ihmisiin liittyvät näkökulmat. Ihmisten omaa vastuuta tietoturvallisuuden toteutumisessa tulisi kuitenkin korostaa, sillä teoreettisen viitekehyksen tutkimuksissa korostui, että ihmiset saattavat laiminlyödä tietoturvakäytäntöjä, jos kokevat organisaation tuen liian vahvaksi, sillä tällöin he olettavat, että IT-osasto hoitaa kaiken, eikä heidän oma roolinsa ole niin kriittinen. Tämän opinnäytetyön tutkimustuloksissa korostui myös se, että tietoturvan jalkauttamisen haasteet kasvavat silloin kun tietoturvaprosessit ovat ristiriidassa vallitsevan työkulttuurin ja esimerkiksi tehokkuusvaatimusten kanssa. Tämä voi lisätä henkilöstön ylikuormittavaa tietoturvastressiä, jolloin he alkavat käyttämään neutralisointitekniikoita, kuten välttämättömyyden pakkoa rationalisoimaan tietoturvakäytäntöjen noudattamatta jättämisen. Jos siis tiedetään, että organisaation tehokkuusvaatimukset ovat erittäin tiukat ja esimerkiksi henkilöstön tyytyväisyys on kärsinyt jonkin organisaatioon vaikuttavan tekijän vuoksi (muutosneuvottelut, yrityskaupat ym.) pelkästään hallinnollisten ja luottamukseen perustuvien keinojen käyttö ei välttämättä tuota haluttua lopputulosta.

5.2 Tutkimuksen rajoitteet ja validiteetti

Vaikka konstruktiivinen tutkimus ei rajaa ulos mitään tiedonkeruumenetelmiä, opinnäytetyön tekijä päätyi haastatteluun, sillä koki että muut menetelmät eivät olisi toimineet yhtä hyvin. Tähän opinnäytetyöhön liittyi paljon abstrakteja käsitteitä, jotka ovat vaikeasti hahmotettavissa ilman perusteellista taustatietoa. Syvällinen ymmärrys kontekstista oli tärkeää tutkimustulosten laadun varmistamiseksi ja mahdollisimman syvällisen tiedon saamiseksi. Haastatteluja varten oli avattava haastateltaville haastattelussa käytettyä termistöä ja esiteltävä Liitteen 1 esimerkkitapaukset, jotta

haastateltavat saisivat paremman käsityksen tutkittavasta aiheesta ja käsitteistä. Myös haastateltavat käyttivät omia esimerkkejään havainnollistamaan vastauksiaan. Tietoturvaan ja teknologiaan liittyvät termit ja käytännöt voivat olla haastavia useista syistä. Ensinnäkin termejä ja käsitteitä lainataan ja käännetään ensisijaisesti englannin kielestä, mikä voi johtaa merkityserojen syntymiseen termejä käännettäessä. Toiseksi samat termit voivat saada erilaisia merkityksiä riippuen kontekstista. Kontekstisidonnaisuus voi johtaa tilanteisiin, jossa ihmiset tulkitsevat termit eri tavoin. Kyselyn käyttäminen laajemman otoksen saamiseksi olisi saattanut myös olla mahdollinen menetelmä, mutta tällöin yhtä syvällisen tiedon kerääminen ei olisi ollut mahdollista ja riskinä olisi myös ollut se, että teema, esimerkit ja termit olisi ymmärretty väärin. Ryhmähaastattelu olisi soveltunut hyvin, jos esimerkiksi useampi henkilö samasta organisaatiosta olisi osallistunut yhteen haastatteluun. Valitettavasti haastateltavien löytäminen oli jo itsessään haastavaa, mikä teki ryhmähaastattelujen järjestämisen epärealistiseksi. Uskon myös, että ryhmähaastattelujen pidempi kesto olisi voinut lisätä vaikeuksia haastateltavien saamisessa.

Tutkimus rajattiin koskemaan ISO/IEC 27001-sertifioituja tai tietoturvaansa standardin mukaisesti kehittäviä organisaatioita, jotta haastateltavien vastaukset olisivat mahdollisimman vertailukelpoiset ja jotta voitaisiin varmistua siitä, että haastateltavilla oli kokemusta vastaavanlaisien vaatimusten toteuttamisesta. Rajoituksen myötä haastateltavien löytämisessä kuitenkin kohdattiin haasteita, joista suurin liittyi haastateltavien löytämiseen. ISO/IEC 27001-sertifioiduista organisaatioista ei ollut olemassa mitään helposti saatavilla olevaa listaa, jota hyödyntämällä olisi voinut kontaktoida mahdollisia haastateltavia. Aluksi siis opinnäytetyön tekijä hyödynsi omia verkostojaan ja oli yhteydessä organisaatioihin, joilla tiesi olevan ISO/IEC 27001-sertifikaatti tai joiden tiesi olevan tavoittelemassa sertifikaattia. Omista verkostoista haastateltaviksi suostui kaksi henkilöä. Tämän jälkeen otettiin yhteyttä organisaatioihin, jotka olivat mahdollisesti julkaisseet tiedotteen ISO/IEC 27001 -sertifikaatin saamisesta. Lähteinä käytettiin hakukoneiden tuloksia ja LinkedIn-julkaisuja. Näistä haastateltavaksi suostui kolme lisää. Suurin osa pyydetyistä joko jätti kokonaan vastaamatta tai kieltäytyi kohteliaasti vedoten päällekkäisiin kiireisiin. Haastattelun kesto saattoi olla pyydetyille liian pitkä, sillä tunnin vapauttaminen omasta työviikosta on varmasti kenelle tahansa asiantuntijatyötä tekevälle vaikeaa. Kukaan haastateltavista ei kuitenkaan antanut negatiivista palautetta haastattelun kestosta. Muutama haastateltava kertoi, että aiheesta oli miellyttävää jakaa ajatuksia, koska teemaa ei välttämättä tule pohdiskeltua niin syvällisesti muuten. Tietoturva aiheena saatetaan kuitenkin kokea itsessään niin sensitiivisenä, että aiheesta ja oman organisaation tietoturvan tasosta ei haluta jakaa kokemuksia tai tietoa kovin helposti edes tutkimustarkoituksiin. Tämäkin saattoi omalta osaltaan vaikuttaa haastateltavien määrään.

Haastatteluiden määrä ei kuitenkaan korvaa laatua tai vaikuta siihen. Kun pohditaan haastattelujen määrää, tärkeintä on analysoida haastatteluaineiston kyllääntymistä, eli saturaatiopisteen

saavuttamista, joka on saavutettu silloin, kun haastattelut eivät tuo enää mitään uutta oleellista tietoa. (Ojala ym. 2014, 111) Vaikka haastattelujen osallistujamäärä oli odotettua pienempi, se oli kuitenkin riittävä antamaan arvokasta tietoa tutkittavasta ilmiöstä tietyssä erityisryhmässä, eli ISO/IEC 27001 -sertifioiduissa organisaatioissa. Kaikki haastateltavat työskentelivät eri asiantuntijaorganisaatioissa, jolloin kaikilla oli eri näkökulmat ja kokemukset. Suurin osa haastateltavista työskenteli IT- tai teknologiapainotteisissa organisaatiossa, mikä oli opinnäytetyön rajauksen myötä myös luonnollista, sillä kuten teoreettisessa viitekehyksessäkin mainittiin, Suomen ISO/IEC 27001-sertifioiduista yrityksistä 70 % toimii tietotekniikka-alalla. Haastateltavat työskentelivät ja olivat aiemmin työskennelleet sekä pienissä että suurissa organisaatioissa, jolloin molempien kokemusten näkökulmat saatiin huomioitua, mikä oli myös mallin kehittämisen kannalta erittäin tärkeää. Neljä haastattelua järjestettiin ajallisesti melko lähekkäin ja suurin osa dokumenttianalyysista oli jo tehty ennen viidettä haastattelua. Viimeisen haastattelun kohdalla opinnäytetyöntekijä huomasi, että vastaukset ja näkemykset olivat hyvin samankaltaisia kuin aiemmin haastatelluilla, jolloin saturaatiopiste oli näiden haastattelujen osalta melko hyvin saavutettu. Haastattelujen lisäksi tietoa kerättiin suorittamalla kirjallisuuskatsaus, joka johti teoreettisen viitekehyksen muodostumiseen. Tämä mahdollisti haastattelutiedon ja teoreettisen tiedon välisen yhteyden ja samankaltaisuuksien löytämisen, mikä omalta osaltaan vahvistaa tutkimuksen validiteettia. On kuitenkin tärkeää huomioida, että rajoitettu määrä haastatteluja saattaa vaikuttaa tutkimustulosten yleistettävyyteen.

5.3 Tutkimuksen tavoitteiden saavuttaminen

Konstruktiivisen tutkimuksen päämääränä on kehittää uusi, teoreettisesti perusteltu ratkaisu käytännön ongelmaan. Ratkaisun tulisi tuoda niin liiketoimintaan kuin myös tiedeyhteisöön uutta tietoa, mikä lisääkin lähestymistavan haasteellisuutta. Oleellista on kuitenkin saada käytännön ongelma ja ratkaisu sidottua teoreettiseen tietoon. Ihanteellisessa tapauksessa ratkaisu olisi sovellettavissa useassa eri organisaatiossa, vaikka sen toimivuuden testaaminen olisi käytännössä hyvin työlästä. (Ojasalo, Moilanen & Ritalahti, 2014, 65)

Konstruktiivinen tutkimus oli tälle opinnäytetyölle sopiva lähestymistapa ja mielestäni teoreettinen tieto ja käytännön ongelma saatiin sidottua yhteen hyvin. Opinnäytetyöllä oli kaksi tavoitetta. Ensimmäiseksi kerätä ilmiöstä tietoa, eli selvittää miten asiantuntijaorganisaatiot, jotka ovat kehittäneet tietoturvaansa ISO/IEC 27001 standardin mukaisesti, valitsevat ja soveltavat erilaisia keinoja tietoturvaprosessiensa jalkauttamiseen. Tämä tavoite täyttyi. Teoreettista viitekehystä varten löytyi kattavasti tietoa ja erityisesti ihmisten tietoturvakäyttäytymistä on tutkittu aiemmin kiitettävästi, mikä mahdollisti hyvän tietopohjan haastatteluja varten. ISO/IEC 27001-standardin käyttöönottamisen avuksi on myös kirjoitettu useita oppaita, joista oli apua teoreettista viitekehystä kirjoittaessa. Oppaat eivät kuitenkaan ole niin yksityiskohtaisia siinä mielessä, että niistä saisi suoraan vinkkejä

jalkauttamiseen ja kuten Chopra & Chaudarykin (2020, luku 1) totesivat, ISO/IEC 27001-standardi ei ole ohjaileva siinä mielessä, että se kertoisi suoraan millaista teknologiasta ratkaisua kannattaisi käyttää tai miten usein varmuuskopiointeja kannattaisi suorittaa. Nämä päätökset ja soveltamistavat joutuvat organisaatiot tekemään itse.

Opinnäytetyön toinen tavoite oli kehittää teoreettisen viitekehyksen ja haastatteluista saatujen tietojen pohjalta uusi, toimiva ja tietoon perustuva toimintamalli, jota voidaan hyödyntää jatkossa tietoturvaprosesseja jalkauttaessa. Tämä tavoite täyttyi myös, vaikka mallin painopiste muuttuikin varsinaisesta jalkauttamisesta sen suunnitteluun. Opinnäytetyöprosessin edetessä ja kattavamman tietopohjan kertyessä kävi selväksi, että tietoturvan jalkauttaminen kaikkiin organisaatioihin yhden toimintamallin avulla olisi lähes mahdotonta, koska niin organisaatiot kuin jalkautettavat käytännöt ovat hyvin erilaisia. Myöskään alkuperäisessä suunnitelmassa määriteltyä mallia sille, mitä jalkauttamistapaa kannattaisi käyttää missäkin tilanteessa oli turha lähteä kehittämään, koska tuloksista ilmeni, että haasteiden ratkaisemiseksi on suositeltavaa, sen ollessa mahdollista, käyttää sekä teknisiä että hallinnollisia keinoja, sillä ne täydentävät toisiaan. Koska jalkauttamisprosessiin vaikuttavia tekijöitä oli kuitenkin tunnistettu ihan kiitettävästi, oli näiden pohjalta kuitenkin mahdollisuus luoda malli, joka keskittyi jalkauttamisprosessin suunnitteluvaiheeseen, eli vaiheeseen ennen varsinaista jalkautusta.

5.4 Toimintamallin jatkokehittäminen

Tämän opinnäytetyön tuloksena syntyneen toimintamallin kehittäminen oli vaikeaa lähtökohtaisesti sille asetettujen vaatimusten vuoksi. Toimintamallin toimivuuden arviointia ei aikataulullisten syiden vuoksi ehditty tehdä markkinoilla tai organisaation sisällä, kuten konstruktiiviselle tutkimukselle suositellaan. Ojasalon ym. (2014, 67–68) mukaan näin voi kuitenkin opinnäytetöiden tai muiden aikatauluihin sidottujen töiden kohdalla tapahtua. Ratkaisun toimivuuden arvioinnin markkinoilla voi kuitenkin myös toteuttaa jälkikäteen. Ratkaisun ideaa kannattaa testata esikokein ennen varsinaista testaamista.

Toimintamallin ensimmäisestä luonnoksesta kuitenkin kerättiin palautetta haastattelujen lopuksi, mikä oli myös lopullisen toimintamallin syntymisen osalta kriittistä. Jos tätä palautetta ei olisi saatu, olisi alkuperäinen toimintamalli ollut varmasti paljon hyödyttömämpi ja soveltumattomampi käytännön työelämään.

Tämän opinnäytetyö ja sen mukana syntynyt toimintamalli voi tarjota oivalluksia ja työkaluja tietoturvan kehittämisestä tai muutoksen johtamisesta vastaaville asiantuntijoille, jotka pyrkivät optimoimaan tietoturvaprosessiensa jalkauttamista. Vaikka jokaisella organisaatiolla on omat riskinsä, on ihmisten tietoturvakäyttäytymiseen liittyvät riskit kuitenkin melko universaaleja ja nämä on pyritty

ottamaan huomioon toimintamallia kehittäessä. Mallia voisi jatkokehittää ensin testaamalla sitä käytännössä ja miettimällä, mitä asioita siitä mahdollisesti vielä puuttuvat tai mitkä asiat tuntuvat turhilta tai ylimääräisiltä. Malli saattaa olla liian raskas jokaiseen tietoturvan jalkauttamisprosessiin, sillä joskus prosessin mukana tuoma muutos on sen verran pieni, että jokaista mallin vaihetta ei välttämättä ole pakollista miettiä, mutta mallin kehittämisessä on kuitenkin pyritty siihen, että mahdollisimman moni asia otettaisiin huomioon, sillä hyvällä suunnittelulla parannetaan projektin onnistumisen edellytyksiä.

Lähteet

Adarsh N., Greeshma M. 2023. Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing. E-kirja. Luettu 20.9.2023.

Aksela, M., Marchal, S., Patel, A. Rosenstedt, L. & WithSecure. 2022. Tekoälyn mahdollistamat kyberhyökkäykset. Liikenne- ja viestintävirasto Traficom. Helsinki. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TRAFICOM_Teko%C3%A4lyn_mahdollistamat_kyberhy%C3%B6kk%C3%A4ykset%202022-12-12_web.pdf Luettu: 4.7.2023.

Ali, R., Dominic, P., Ali, S., Rehman, M., Sohail, A. 2021. Information Security Behaviour and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. Applied Sciences, 11, 8, s. 1–38.

Beyer, R., & Brummel, B. 2015. Implementing effective cyber security training for end users of computer networks. SHRM-SIOP science of HR series: Promoting evidence-based HR, 3, 10.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS quarterly, 34, 3, s. 523–548.

Brown, J. W. 2022. The Security Leader’s Communication Playbook. Bridging the Gap between Security and the Business. 1. painos. Taylor & Francis Group, LLC. Boca Raton.

Chopra, A. & Chaudhary, M. 2020. Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. Apress. E-kirja. Luettu: 4.7.2023.

Da Veiga, A., Astakhova, L., Botha, A., Herselman, M. 2020. Defining organisational information security culture – Perspectives from academia and industry. Computers & security, 92.

D'Arcy, J., Herath, T., Shoss, M., 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. Journal of management information systems, 31, 2, s. 285–318.

D'Arcy, J. & Greene, G. 2014. Security culture and the employment relationship as drivers of employees’ security compliance. Information management & computer security, 22, 5, s. 474–489.

D'Arcy, J. & Lowry, P. 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information systems journal. 29, 1, s. 43–69.

Digiturvamalli.fi. Hallintakeinojen toteutus ja varmistus. 2023. Luettavissa: https://www.digiturvamalli.fi/kayttotavat/hallintakeinojen-toteutus Luettu 4.2.2024.

Flowerday, S. & Tuyikeze, T. 2016. Information security policy development and implementation: The what, how and who. Computers & security, 61, s. 169–183.

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

Hengstler, S., Kuehnel, S., Masuch, K., Nastjuk, I. & Trang, S. 2023. Should I Really do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior. Computers & security.

Hu, Q., Dinev, T., Hart, P. & Cooke, D. 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture: Managing Employee Compliance with Information Security Policies. Decision sciences, 43, 4, s. 615–660.

Hyppönen, M. 2022. If it’s smart, It’s Vulnerable. Wiley. E-kirja. Luettu: 19.4.2024.

International Organization for Standardization. ISO/IEC 27001 Information security management systems. Luettavissa: https://www.iso.org/standard/27001 Luettu: 4.7.2023.

International Organization for Standardization. ISO Survey 2019 results – Number of certificates and sites per country and the number of sector overall. 5.10.2022. Luettavissa: https://www.iso.org/committee/54998.html?t=Z_B0DEkNvy-kWI__P05ktfa3ZGF69esptNwgfRs4GaPEv1Tc_PNUsxGMg6sI0fup&view=documents#section-isodocuments-top Luettu: 4.7.2023.

International Organization for Standardization. ISO Survey 2020 results – Number of certificates and sites per country and the number of sector overall. 15.9.2022. Luettavissa: https://www.iso.org/committee/54998.html?t=3UNptZ5DkNcbZFbWqu2aVSC9HR4DCKo1tnN_-wHJxu63vas2WEYXBQwMsh1TZDJ0&view=documents#section-isodocuments-top Luettu: 4.7.2023.

International Organization for Standardization. ISO Survey 2021 results – Number of sectors by country for each standard. 15.9.2022. Luettavissa: https://www.iso.org/home.isoDocumentsDownload.do?t=rrypdD0jIaHfA7y_jN6MI_tuAA_XGV2nOwlddQJWZyBeNQrv-

yeVyvUTP19rw3k0&CSRFTOKEN=IK8G-1Z07-NNRK-OR7R-4G0X-IYXS-NKLC-CCXN Luettu: 4.7.2023.

International Organization for Standardization. ISO Survey 2021 results – Number of certificates and sites per country and the number of sector overall. 21.1.2023. Luettavissa: https://www.iso.org/committee/54998.html?t=KomURwikWDLiuB1P1c7SjLMLEAgXOA7em-ZHKGWyn8f3KQUTU3m287NxnpA3DIuxm&view=documents#section-isodocuments-top Luettu: 4.7.2023.

ISMS.online. s.a. ISO 27001:2022 Annex A Explained. Luettavissa https://www.isms.online/iso-27001/annex-a/ Luettu 20.9.2023.

Järvinen, P. 2022. Yrityksen tietoturvaopas. Keskuskauppakamari. Helsinki. E-kirja. Luettu: 3.7.2023.

Kenyon, B. 2019. ISO 27001 controls – A guide to implementing and auditing. IT Governance Publishing. E-kirja. Luettu: 6.7.2023.

Kolehmainen, A. 8.2.2023 Tietoturvasertifikaatit käyvät kaupaksi – niihin liittyy kuitenkin väärinymmärryksiä. Tivi. Luettavissa: https://www.tivi.fi/uutiset/tietoturvasertifikaatit-kayvat-kaupaksi-niihin-liittyy-kuitenkin-vaarinymmarryksia/a8607aa5-da7b-41cb-9781-5d00941d9a0a Luettu: 3.7.2023.

Kranz, J., Haeussinger, F. 2014. Why Deterrence is not Enough: The Role of Endogenous Motivations on Employee's Information Security Behavior. In Proceedings of the 35th International Conference on information systems (ICIS). s. 1–11. Luettavissa: https://www.researchgate.net/publication/266679589_Why_Deterrence_is_not_enough_The_Role_of_Endogenous_Motivations_on_Employees_Information_Security_Behavior Luettu: 18.7.2023.

Laaksonen, M., Nevasalo, T., Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Edita Publishing. Helsinki.

Landoll, D. J. 2016. Information Security Policies, Procedures, and Standards. Auerbach Publishers, Incorporated. E-kirja. Luettu 11.9.2023.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus 2020. Tietoturva. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva Luettu: 4.7.2023.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3. uudistettu painos. Sanoma Pro. Helsinki.

Omnistruct, 2020. NIST, ISO, CIS Or COBIT? Comparing Comprehensive Cybersecurity Frameworks. Luettavissa: https://omnistruct.com/nist-iso-cis-or-cobit-comparing-comprehensive-cybersecurity-frameworks/ Luettu: 19.4.2024.

Puhakainen, P. & Siponen, M. 2010. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. MIS quarterly, 34, 4, s. 757–778.

Raggad, B. 2010. Information security management: Concepts and practice. Boca Raton, Fla: CRC Press. E-kirja. Luettu: 4.7.2023.

Siponen, M. & Vance, A. 2010. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS quarterly, 34, 3, s. 487–502.

Son, J. 2011. Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & management. 48, 7, s. 296–302.

Suomen Standardisoimisliitto SFS ry. s.a ISO/IEC 27000 Tietoturvallisuuden standardisarja. Luettavissa: https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/ Luettu: 3.7.2023.

Suomen Standardisoimisliitto SFS ry, 2022. ISO/IEC 27001:2022:fi Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.

Tessian, Hancock, J. 2022. Psychology of human error. Tessian. Luettavissa: https://www.tessian.com/resources/psychology-of-human-error-2022/ Luettu: 4.7.2023.

Vaasan yliopisto 2015. Väitös: Viranomaisten tulisi karsia tietoturvaohjeistuksia. Luettavissa: https://www.uwasa.fi/fi/news/kinnunenvaitos Luettu 18.7.2023.

Valtiovarainministeriö 2007. Tietoturvallisuudella tuloksia – Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Luettavissa: https://www.suomidigi.fi/sites/default/files/2020-06/mainbook_3_2007.pdf Luettu: 6.7.2023

Vance, A., Siponen, M. T. & Straub, D. W. 2020. Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & management, 57, 4, s. 1–9.

Yeniman Yildirim, E., Akalp, G., Aytac, S. & Bayram, N. 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International journal of information management. 31, 4, s. 360–365.

Liitteet

Liite 1. Haastatteluissa läpikäydyt sovellettavat esimerkkitapaukset

Tavoite	Esimerkki hallinnollisesta toteutuksesta	Esimerkki teknisestä toteutuksesta
Tietojen siirtäminen Tietojen siirtoon liittyen organisaation menettelytavaksi halutaan ottaa se, että henkilötietoja sisältäviä viestejä ei saisi ikinä lähettää salaamattomana.	Kirjataan tietoturvaohjeeseen, että kaikki henkilötietoa sisältävät sähköpostit on lähetettävä salattuna viestinä. Muistutetaan tästä säännöllisesti tietoturvakoulutuksissa.	Otetaan käyttöön automaattinen sähköpostien salaus, kun sähköpostijärjestelmä tunnistaa, että viestissä tai liitteessä on arkaluontoista tietoa (esimerkiksi henkilötunnuksia)
Tietoturvatapahtumista raportointi Organisaatio toivoo henkilöstön raportoivan havaittuja tai epäiltyjä tietoturvatapahtumia/häiriöitä eteenpäin asianmukaisten kanavien kautta.	Määritellään mahdolliset tietoturvahäiriöt, luodaan prosessi häiriöiden ilmoittamiseksi. Ohjeistetaan ja koulutetaan henkilöstöä tietoturvaheikkouksista ja –häiriöistä ja näistä ilmoittamisesta.	Otetaan käyttöön järjestelmänvalvontatyökaluja ja lokitiedostojen analysointiohjelmia, jotka keräävät ja analysoivat tietoturvapoikkeamia auttaen tunnistamaan heikkoudet ja raportoimaan näistä eteenpäin.
Kapasiteetinhallinta Organisaatiolla on tiettyjen tietojen arkistointivelvollisuus ja tiettyjen dokumenttien maksimisäilytysajat. Tietyt dokumentit on poistettava säilytysajan täyttyessä myös vapauttaakseen tallennuskapasiteettia.	Luodaan prosessit ja ohjeistukset siitä, millaisia dokumentteja on poistettava säilytysajan täyttyessä.	Otetaan käyttöön ohjelmistotyökalu/automaatio, joka suorittaa säännöllisesti tietojen poistamisen ja varmistaa, etteivät poistetut tiedot ole palautettavissa.
Verkkopalvelujen turvaaminen Organisaatiossa halutaan, että tiettyihin kriittisiin järjestelmiin (esim. dokumentinhallintajärjestelmä tai CRM) ei pääsisi muuten kuin organisaation sisäverkosta.	Ohjeistetaan, että etätöissä ja työmatkoilla olisi hyvä käyttää VPN-yhteyttä.	Estetään toimiston ulkopuolella ollessa pääsy kriittisiin tietojärjestelmiin ilman VPN-yhteyttä, joka varmistaa tietoliikenteen salaamisen etätyöskentelyn aikana.
Käyttäjien päätelaitteet Haittaohjelmilta suojautuakseen organisaatiossa halutaan estää työntekijöiden ohjelmistojen lataus koneelle, jolloin asennuksia pystyisivät tekemään ainoastaan IT-tukihenkilöt ja ohjelmiston asentamiselle olisi aina oltava perusteltu syy.	Ohjeistetaan työntekijöitä, että mitään ohjelmistoja ei saa asentaa itse koneille.	Tehdään tekninen rajoitus, joka estää työntekijöitä asentamasta tietokoneilleen mitään ohjelmistoja.
Verkkosuodatus Organisaatio haluaa lieventää riskiä siitä, että henkilöstö käy verkkosivustoilla, jotka saattavat sisältää laitonta tietoa, viruksia tai kalastelumateriaalia.	Laaditaan säännöt verkkosivujen turvallista ja asianmukaista käyttöä varten, ohjeistetaan ja koulutetaan verkkoresurssien turvallisesta käytöstä.	Estetään haitallisten verkkosivustojen IP-osoitteet tai verkkoalueet palomuurilla tai muilla konfiguraatioilla.
Mobiililaitteet ja etätyö Organisaatiossa halutaan varmistaa, että mobiililaitteiden käyttö on turvallista ja että ne eivät aiheuta ylimääräistä riskiä organisaation tietoturvalle.	Määritellään ja viestitään selkeä politiikka mobiililaitteiden käytölle ja niiden suojausvaatimuksille. Järjestetään koulutuksia työntekijöille mobiililaitteiden turvallisesta käytöstä.	Otetaan käyttöön mobiililaitehallintajärjestelmä, joka pakottaa tietynlaiset suojausvaatimukset, jotka on täytyttävä, jotta laite olisi turvallinen käyttää.

Liite 2. Toimintamalli tietoturvaprosessin jalkauttamisen suunnittelun avuksi

TIETOTURVAPROSESSIN JALKAUTTAMISEN SUUNNITELMA 2/2