Tampereen yliopisto

AKSELI ERIKKILÄ

TIETOTURVAPOLITIIKAN RAKENTAMINEN SUOMESSA TOIMIVISSA YRITYKSISSÄ

Informaatioteknologian ja viestinnän tiedekunta
Diplomityö
Kesäkuu 2019

TIIVISTELMÄ

Akseli Erikkilä: Tietoturvapolitiikan rakentaminen Suomessa toimivissa yrityksissä
Diplomityö
Tampereen yliopisto
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Kesäkuu 2019

Diplomityössä tutkittiin Suomessa toimivien yritysten tietoturvapolitiikan tilaa. Tietoturvapolitiikka on tietoturvallisuuden hallintaan käytetty määräys, joka määrittelee tietoturvallisuuden, sen tavoitteet ja vastuut. Työssä haastateltiin kymmentä Suomessa toimivaa yritystä ja selvitettiin, miten niissä tietoturvapolitiikka on rakennettu. Haastattelut analysoitiin ja niistä nostettiin esiin erilaisia haasteita. Näiden pohjalta ja kirjallisuuden avulla toteutettiin tietoturvapolitiikalle malli, jolla pyritään kuvaamaan eri tietoturvapolitiikan osa-alueiden olennaisimmat osat.

Haastattelut jaoteltiin kolmeen osaan: suunnitteluun, toteutukseen ja seurantaan. Kustakin alueesta kysyttiin kysymyksiä, jotka pitkälti selvittivät, miten tietoturvapolitiikan siirtämistä käytäntöön oli huomioitu kussakin vaiheessa. Yleisenä havaintona kaikista haastatteluista nousi esiin johdon tuen vähyys, jota voi parantaa muun muassa näyttämällä esimerkkiä enemmän alaisille. Tällöin henkilöstöä on helpompia saada sitoutettua tietoturvallisuuteen.

Suunnitteluun liittyvissä kysymyksissä kysyttiin, millaista suunnitteluprosessia käytettiin ja millaisia aineistoja suunnittelussa käytettiin. Tästä osioksi haasteeksi nousi erilaisten sidosryhmien ottaminen mukaan suunnitteluun. Kaikki erilaiset käyttäjäryhmät ovat tärkeitä tietoturvallisuudelle, sillä he lopulta toteuttavat tietoturvaprosesseja ja vastaavat sen onnistumisesta. Sidosryhmien tarpeita pitäisi kuulla ja sovittaa tietoturvallisuus sopimaan heidän prosesseihinsa, jotta toimintatavat onnistuisivat parhaiten.

Toteutukseen liittyvissä kysymyksissä kysyttiin, millainen rakenne politiikalla on ja miten sen toteuttamisesta on kommunikoitu ja lopulta, miten se on koulutettu. Tässä suurimmaksi haasteeksi nousi koulutusten määrä ja laatu. Useimmat yritykset järjestivät koulutuksia hyvin vähän, jopa vain kerran. Tätä varten ehdotettiin, että koulutuksia tulisi järjestää tasaisemmin ja hyväksikäyttää verkkopohjaisia oppimisalustoja, jotka mahdollistavat ajasta ja paikasta riippumattomia koulutuksia.

Seurantaan liittyvissä kysymyksissä kysyttiin, miten tietoturvapolitiikan noudattamista seurataan ja miten pyritään varmistamaan, että henkilöt voisivat noudattaa politiikkaa. Suurimmaksi haasteeksi nousi itse mittaaminen. Tietoturvapolitiikan toimivuuden mittaaminen on vaikeaa, ellei jopa mahdotonta, joten tätä varten ehdotettiin toisenlaista lähestymistapaa. Tietoturvaongelmia tai erilaisia virheitä tulisi voida tuoda esiin ilman pelkoa sanktioista ja virheet tulisi nähdä positiivisina oppimistapahtumina. Tällöin henkilöstö voisi tuoda ongelmia enemmän esiin ja toimintaa olisi helpompi seurata.

Mallipolitiikassa opittu tiivistettiin kuusiosaiseksi tietoturvapolitiikan pohjaksi, jossa kuvataan kunkin osan tärkeys tietoturvallisuuden onnistumiselle. Osat ovat: tietoturvallisuuden ja sen osien määrittely, tietoturvapolitiikan sisältö, vastuiden määrittely, politiikan määräykset, valvonta ja tietoturvapolitiikan kehittäminen.

Avainsanat: tietoturvapolitiikka, tietoturvakulttuuri, tietoturvahallinto

ABSTRACT

Akseli Erikkilä: Building information security policy in companies operating in Finland
Master's thesis
Tampere University
Master's degree programme in Information technology
June 2019

This Master's thesis explores the status of information security policy in companies operating in Finland. An information security policy is used in information security management to define information security, its targets and responsibilities related to it. In the thesis, ten companies were interviewed to find out how information security policies are crafted there. The interviews were analyzed, and several challenges were identified. Based on these and other background material, a model for information security policy was defined. The model aims to define the essential parts of an information security policy.

The interviews were divided into three parts: planning, execution and monitoring. Each of the sections had questions that were used to find out how information security was moved from a policy to practice. As a general finding from the interviews was that higher management support was lacking in many of the companies. This could be improved by being more of an example to employees which would make them more committed to it.

In the planning section, the interviewees were asked what kind of processes they had in planning and what kind of material they used to support it. The biggest challenge from this section was the lack of engaging different stakeholders into the planning process. Different stakeholders are important in the success of information security as they are the ones that implement the policy into practice. The stakeholders should be heard more and intertwine the information security practices into their processes to make the implementation as successful as possible.

In the execution section, the interviewees were asked about the structure of the policy, how employees were communicated to and how they were trained about the policy. The biggest challenge here was the amount and quality of the trainings. Many of the companies had very few trainings, in worst cases only one. To improve on this, it was suggested that companies should have trainings more often and to utilize e-learning platforms that make it possible to have trainings regardless of time and place.

In monitoring section, the interviewees were asked how the compliance to the policy was monitored and how they made sure people would comply with it. The biggest challenge was related to the monitoring itself. Monitoring information security policy compliance is hard, or even impossible, so a different approach was suggested. Problems and mistakes related to information security should be reported without a fear of sanctions and they should be positive learning experiences. Then the employees could bring them forth more and the activities would be easier to monitor.

In the information security policy model, all that was learned was condensed into six parts, each explaining the importance to the success of information security. The parts are: definition of information security and its parts, the contents of the policy, definition of responsibilities, the specifications of the policy, monitoring and the development of the policy.

Keywords: information security policy, information security culture, information security management

ALKUSANAT

Syksyllä 2018 kunnolla alkanut diplomityöni jatkui pitkälle keväälle 2019, kun työelämä oli viedä mennessään. En olisi saanut työtäni valmiiksi ilman tukea perheeltäni ja ystäviltäni, jotka jaksoivat kannustaa työn kanssa eteenpäin. Näiden lisäksi haluaisin kiittää työnantajaani, Exovea, joka rahoitti diplomityön parissa työskentelyn. Diplomityöni ohjaajat Jukka Koskinen Tampereen yliopistolta ja Mikko Hämäläinen Exovelta ovat mahdollistaneet työlleni parhaan mahdollisen lopputuloksen ja tahdon myös kiittää heitä tekemästään työstään.

Nimeämieni henkilöiden lisäksi haluan kiittää haastatteluihin osallistuneita yrityksiä, joita ilman työni ei olisi onnistunut. Useat haastattelut ja käydyt keskustelut opettivat tietoturvallisuuden alasta enemmän kuin itse työssä saattaa näkyä. Diplomityöni tiivistää vain osan oppimastani, sillä tietoturvallisuus on niin laaja aihe, ettei kaikkea oppimaani voinut tuoda siihen mukaan.

Ennen kaikkea tämä työ on koko tähänastisten opintojeni huipentuma. Siitä on hyvä lähteä kohti seuraavia haasteita.

Helsingissä, 20.6.2019

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
ISO-27000	Standardiperhe tietoturvallisuuden johtamiseen ja hallinnointiin
htp	Henkilötyöpäivä eli 7,5 tuntia.
GDPR	General Data Protection Regulation eli Euroopan tietosuoja-asetus
PK-HAAVA	Pienille ja keskisuurille yrityksille suunnattu riskianalyysimalli
CIA	Confidentiality, integrity, availability

1. JOHDANTO

Tietoturvallisuus on viime vuosina muuttunut koko ajan tärkeämmäksi ja siksi siihen liittyvä tutkimus on kasvattanut merkitystään. Yrityksille tietoturvasta on muodostunut elinehto ja sen suunnitteluun, ohjaamiseen ja kehittämiseen panostetaan enemmän kuin koskaan [1]. Tästä syystä tietoturvallisuuden hallinta organisaatioissa on entistä tärkeämpää, koska kokonaisuus kasvaa eikä sitä voi enää hallita ilman selkeätä suunnitelmaa.

Kun yrityksen tietoaineistot, kuten sopimukset, suunnitelmat, asiakastiedot, tutkimustulokset ja muut arvokkaat aineistot, ovat digitaalisessa muodossa ja niihin tarvitsee olla pääsy mistä päin maailmaa tahansa ja milloin tahansa, muuttuvat tietoturvallisuuden liittyvät haasteet vaikeammiksi. Yritysten henkilöstölle annetaan työkalut ja ohjeet, miten aineistoihin pääsee käsiksi ja miten niiden kanssa tulee toimia. Tässä työssä päästään hyvin pitkälle teknisillä keinoilla ja rajoituksilla, jotta tiedot eivät päädy vääriin käsiin. Mutta jossain vaiheessa tekniset hallintakeinot loppuvat ja henkilö itse on vastuussa tietoaineistojen tietoturvasta. Tässä vaiheessa henkilön tietoturvatietoisuus ja koulutetut prosessit nousevat tärkeään rooliin ja ovat viimeinen ratkaiseva tekijä tietoturvallisuuden onnistumisessa.

Yrityksen tietoturvallisuus rakentuu henkilöiden hallinnasta ja teknisistä ratkaisuista, joilla pääsy tietoaineistoihin rajataan, mahdollistetaan ja tietoaineistot pidetään ajantasaisina. Tietoturvallisuuden hallinnalla taataan, että tämä kokonaisuus pysyy toiminnassa ja tukee yrityksen toimintaa. Hallinnan pohjana toimii yksi määräys, tietoturvapolitiikkaa, jonka avulla koko toimintaa ohjataan ja muita määräyksiä ja ohjeita rakennetaan.

Tässä diplomityössä tutkitaan tietoturvapolitiikkaa ja sen merkitystä tietoturvallisuuden onnistumiseen yrityksissä. Onnistumisella tarkoitetaan, että tietoturvallisuuden periaatteet, ohjeet ja käytännöt ovat vahvasti osa jokaisen työntekijän toimintaa ja tietoturvalla tuetaan yrityksen toimintaa. Työssä tutkitaan, miten Suomessa toimivissa yrityksissä tietoturvapolitiikka on rakennettu, otettu käyttöön ja miten sitä kehitetään. Tämän avulla selvitetään, miten on mahdollista rakentaa mahdollisimman toimiva ja yrityksen toimintaa tukeva tietoturvapolitiikka.

Työn saavutuksina tietoturvallisuuden hallinnalle ovat tilannekatsaus Suomessa toimivien yrityksien tietoturvapolitiikkoihin ja niiden haasteisiin sekä näytetään, että käytännössä hyödynnetään työssä tutkittuja konsepteja. Nämä opit voivat olla hyvin myös

yleistettävissä muuallekin maailmalla, sillä tietoturvallisuuden käsitteet ovat hyvin globaaleja.

Työn rakenne on tämän luvun jälkeen seuraava: toisessa luvussa esitellään tietoturvapolitiikan taustat. Miten tietoturvapolitiikan voi rakentaa, mitä se voi sisältää, miksi se rakennetaan, mikä sen tavoite on ja mikä sen rooli on tietoturvallisuuden kokonaiskuvassa. Tätä varten avataan työn kannalta merkittäviä aineistoja, joiden avulla monia tutkimuksen päätelmiä on voitu tukea. Tämän jälkeen esitellään tietoturvapolitiikan rakentamisen osa-alueita: suunnittelu, politiikan rakenne ja politiikkaan liittyvät taustatekijät, kuten lait. Kun tietoturvapolitiikan rakentaminen on esitelty, esitellään erilaisia hallintokeinoja, joilla tietoturvapolitiikkaa tuetaan ja otetaan osaksi käytäntöjä. Lopuksi määritetään tietoturvapolitiikan mittaaminen, joka on tärkeä osa tätä työtä. Mittaamisen avulla voidaan tutkia ja kehittää olemassa olevia käytäntöjä ja luoda tavoitteita tietoturvallisuudelle.

Kolmannessa luvussa esitellään tutkimusmenetelmä. Työtä varten haastateltiin kymmentä Suomessa toimivaa yritystä ja pyydettiin heitä kertomaan, miten he ovat suunnitelleet, rakentaneet ja seuranneet tietoturvapolitiikkaansa. Haastattelun avulla pyrittiin saamaan kattavaa kuvaa tietoturvapolitiikan rakentamisen kokonaisuudesta ja löytämään mahdollisia haasteita sen kanssa.

Neljännessä luvussa käsitellään haastattelun tuloksia. Tulokset ovat jaettu haastattelun mukaisesti osioihin, joissa ensiksi käydään läpi tulokset ja niistä esiin nousseita havaintoja. Näistä nostetaan luvun toisessa puoliskossa esiin yleisimmät haasteet ja esitellään ratkaisuehdotuksia näille haasteille.

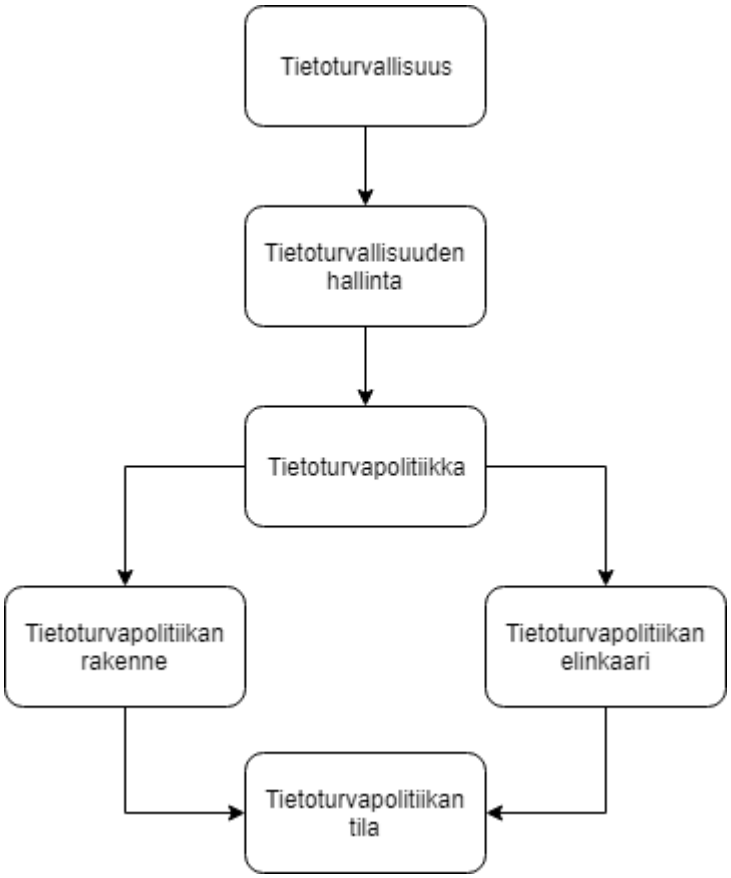
Viidennessä luvussa kuvataan mallipolitiikka, joka perustuu toisen luvun teoriaosuuteen ja neljännessä luvussa esiin nousseisiin havaintoihin. Mallipolitiikassa kuvataan politiikan rakenne, syyt rakenteen eri osille ja mitä kunkin osan tulisi sisältää. Luvussa pohditaan myös, miten tietoturvapolitiikkaa tulisi ottaa käyttöön.

Viimeisessä luvussa työn havainnot kootaan yhteen, pohditaan mahdollisuuksia parantaa työtä ja millaisia haasteita tulevaisuus tuo mukanaan tietoturvallisuudelle ja sen hallinnalle.

2. TIETOTURVAPOLITIIKKA

Yrityksen tietoturva tarvitsee toimiakseen paljon määrittelyjä ja dokumentteja, joiden avulla voi viestiä yrityksen henkilöstölle, miten tietoa tulee suojata ja millaisia toimia se vaatii. Tärkein tällainen määräys on tietoturvapolitiikka, jonka varaan rakennetaan koko yrityksen tietoturva. Sen avulla asetetaan yrityksen tietoturvatavoitteet, vastuut ja turvattavat aineistot ja laitteet [2].

Tietoturvapolitiikka jakautuu tässä työssä kahteen osaan: tietoturvapolitiikan rakenteeseen ja sen elinkaareen. Näitä mittaamalla ja tutkimalla saadaan tietoturvapolitiikan tilasta tietoa. Näistä muodostuu tämän diplomityön aihe. Kuvassa 1 on esitetty, kuinka tietoturvallisuus jakautuu hallintoon ja siitä tietoturvapolitiikkaan ja sen osa-alueisiin. Tämän jaon perusteella tämän luvun alaluvuissa määritellään tietoturvapolitiikka ja siihen läheisesti liittyviä käsitteitä, sen yleiset suunnitteluperiaatteet ja millaiset toimintaedellytykset se vaatii. Lopuksi kuvataan, miten tietoturvapolitiikan suorituskykyä voi mitata.



Kuva 1. *Tietoturvallisuuden jakautuminen tietoturvapolitiikkaan*

2.1 Tietoturvapolitiikan määritelmä ja sitä tukevat käsitteet

Tietoturvallisuus vaatii toimiakseen erilaisia hallinnon keinoja, kuten ohjeita ja järjestelmiä, jotta kokonaisuus on selkeästi hallittavissa ja mahdollista saavuttaa. Tietoturvapolitiikka on yrityksen tietoturvallisuuden kulmakivi, sillä ”sen päälle rakennetaan turvallisuuden suunnitelmat ja ohjeet” [3, s. 25]. ISO/IEC 27000 määrittelee, että tietoturvapolitiikka on ”organisaation ylimmän johdon esittämä organisaation tarkoitus ja suunta” ja se on standardin mukaan yksi tietoturvallisuuden hallintajärjestelmän menestyksen kannalta tärkeistä tekijöistä [4].

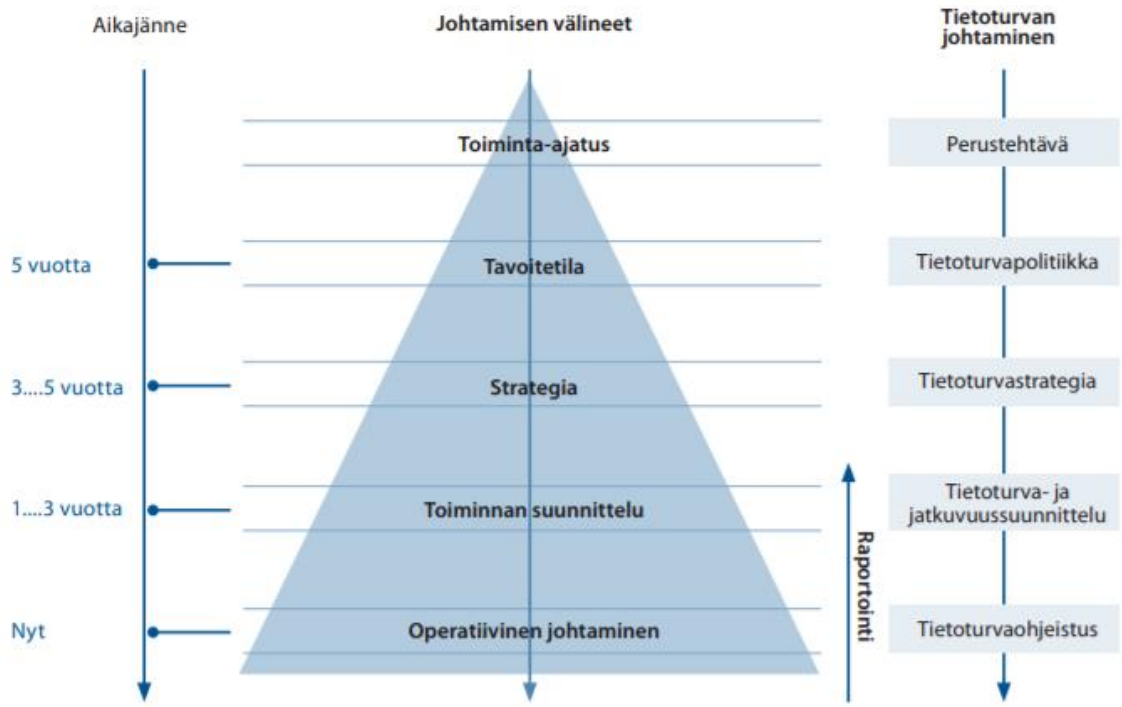
Tietoturvallisuus on tietoaineistojen, -järjestelmien ja palveluiden riskeihin pohjautuvaa toimintaa, jolla varmistetaan kyseisten toimintojen luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability) eli CIA-periaate [5]. Se siis tarkoittaa erilaisten tietoaineistojen ja niiden hallintaan tarkoitettujen järjestelmien turvaamista. Tietoa voi kuitenkin sijaita muussakin kuin digitaalisessa muodossa, kuten fyysisenä paperilla tai ihmisiin sitoutuneena aineettomana tietona, johon tietoturvallisuus pyrkii myös vaikuttamaan.

Tietoturvallisuuden hallinta, tai tietoturvahallinto, kuvaa keinoja, joilla tietoturvaa ja sen toimintoja pyritään hallitsemaan. ISO/IEC 27000 sanoo tietoturvan hallinnasta seuraavaa:

”Tietoturvallisuuden hallintajärjestelmien kannalta hallinta tarkoittaa valvontaa ja liiketoimintatavoitteiden saavuttamiseen tarvittavien päätösten tekemistä siten, että suojataan organisaation tieto-omaisuutta”. Standardi puhuu ”tieto-omaisuudesta”, joka kattaa aiemmassa kappaleessa kuvatut tietoaineiston muodot. Myös liiketoimintatavoitteiden saavuttamisen korostaminen kuvaa sitä, miten tärkeää on sitoa tietoturvallisuus osaksi liiketoiminnan tavoitteita. Näin tietoturvallisuudesta muodostuu tärkeä osa yrityksen toimintaa ja sen hallinta asettuu osaksi koko toiminnan ohjaamista.

Tietoturvapolitiikan merkitys hallinnon keinona on siinä, että se määrittelee perusteet organisaation tietoturvalle. Kuvassa 2 on kuvattu tietoturvallisuuden suhde johtamisjärjestelmiin ja siitä voi nähdä, miten korkealla tasolla tietoturvapolitiikka on organisaation johtamisessa. Tietoturvapolitiikkaa korkeammalla on vain perustehtävä eli toiminnan jatkuvuuden turvaaminen. Politiikasta johdetaan tietoturvastrategia, jonka tarkoitus on kuvata prosessi, jolla tietoturvapolitiikan asettaman tavoitetilan voi saavuttaa. Vaikka ne voivat olla voimassa yhtä kauan, tietoturvapolitiikka muuttuu harvoin yhtä paljon kuin tietoturvastrategia, sillä strategiaa saatetaan vaihtaa, kun teknologia tai osaaminen kehittyy, jolloin lähestymistapaa tulee muuttaa. Strategia muutetaan konkreettisiksi tehtäviksi suunnittelun ja ohjeistuksen kautta. Mitä operatiivisemmaksi, eli lähemmäksi itse käytäntöä mennään, sitä lyhytikäisemmiksi toiminnot muuttuvat.

Tietoturvapolitiikka on korkein johtamisen väline, heti perustehtävän jälkeen, ja tästä syystä, jos tietoturvaa ja sen tarvetta ei täsmennetä ensimmäisenä, on organisaatiolle vaikeata määritellä tietoturvallisuuden toiminnot ja henkilöstön on vaikea nähdä tietoturvan tarpeellisuus eikä mahdollisia ohjeita seurata. Tämän takia on myös tärkeätä, että tietoturvapolitiikka on rakennettu organisaatiolle sopivaksi, jotta se punoutuisi parhaiten yrityksen vallitsevaan kulttuuriin ja vastaa yrityksen tarpeita [3, s. 25]. Tietoturvapolitiikan tavoitteena tulisi olla työskentelyn tekeminen mahdollisimman turvalliseksi, kuitenkaan sitä liikaa rajoittamatta.



Kuva 2. *Johtamisjärjestelmien ja tietoturvallisuuden välinen suhde [3]*

Tietoturvan määritelmä vaihtelee organisaatioiden välillä. Ennen kuin tietoturvapolitiikkaa voi alkaa suunnittelemaan, tulee organisaation selventää, mitä tietoturva merkitsee heille. Kirjallisuudessa tietoturvan merkitys organisaatioille on usein yksiselitteinen: turvataan tietoaineistot CIA-periaatteen mukaan. Tämän periaatteen pohjalta voi luoda monta tulkintaa siitä, mikä tietoturvan tehtävä liiketoiminnalle on.

Tietoturvapolitiikan rakenne ja sisältö vaihtelee organisaatioittain, riippuen muun muassa yrityksen tarpeista, tavoitteista ja liiketoimintaympäristöstä. VAHTI-ohjeissa [3] on esitetty pohja tietoturvapolitiikalle, jossa määritellään muun muassa tavoitteet, ohjaavat tekijät, uhat, tietoturvallisuuden merkitys ja vastuut. Myös muussa kirjallisuudessa on mainittu samoja elementtejä. Lopes ja Oliveira [6] huomasivat, että tutkituissa politiikoissa yleisimmät osat olivat politiikan tarve, politiikan laajuus, vaatimukset, ohjeet ja vastuut. Vastuisiin liittyy usein myös erilaisia rooleja, jotka ovat vastuussa eri tietoturvallisuuden osista [7]. Myös politiikan noudattamisen valvonta on huomioitu usein, koska ihmisen toiminnan tiedetään olevan kriittinen osa tietoturvan onnistumista organisaatiossa [8, 9].

Perustarpeena kaikilla on taata tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyminen [3, s. 13], mutta yksityiskohtaiset tarpeet vaihtelevat ja ne tunnistetaan liiketoiminnan kautta, sillä ”tietoturvallisuus ei ole IT:n ongelma vaan liiketoiminnan ongelma” [10, s. 1]. Tästä syystä tietoturvallisuuden johtamista lähestytään usein riskienhallinnan näkökulmasta [11], mutta tarpeita voi nousta myös lainsäädännöstä, esimerkiksi valtion laitosten tapauksessa [3, s. 26], tai asiakkaiden tarpeista, kun

asiakasyritys tahtoo ylläpitää omaa korkeaa tietoturvallisuuden tasoa [12]. Tarpeen näkökulma voi olla siis joko asiakas-, henkilöstö- tai markkinakeskeinen [7]. Lopputuloksena on tarkoitus ratkaista jokin olemassa oleva ongelma, jonka tietoturva voi ratkaista.

Tietoturvapolitiikasta johdetaan menettelytapoja ja luodaan tarkistuslistoja, sillä se ei itsessään ole usein hyvä kuvaamaan, miten tavoitteita tulisi toteuttaa. Näiden avulla tietoturvapolitiikka jalkautetaan osaksi jokapäiväistä toimintaa ja politiikasta saadaan yksiselitteiset ohjeet, joita kaikki voivat noudattaa [3, s. 25].

Jalkauttamisella tarkoitetaan toimenpiteitä, joilla jokin suunnitelma tai strategia saadaan osaksi yrityksen prosesseja eli teoria saadaan käytäntöön. Tämä voi sisältää koulutuksia, ohjeistuksia ja dokumentteja määräyksistä. Kaikki toimenpiteitä, joilla määräyksiä, strategioita ja suunnitelmia saadaan osaksi normaaleja prosesseja. Jalkauttaminen on olennainen osa tietoturvapolitiikan rakentamista ja se tulee usein esille tässä työssä.

2.2 Tietoturvapolitiikkaan liittyvä tutkimus

Tietoturvapolitiikka on erittäin tutkittu tietoturvallisuuden osa-alue. Aiheesta tuotteliaasti kirjoittaneita ovat muun muassa Richard Baskerville ja Mikko Siponen, jotka ovat tutkineet paljon tietoturvapolitiikkoja yleisesti. Elina Niemimaan väitöskirja [13] käsittelee tietoturvapolitiikan rakentamista, ja Kenneth Knappin ym:n [14] tutkimus käsittelee tietoturvapolitiikan kehittämisprosessia. Mainittujen kirjoittajien työt ovat pohjana suurelle määrälle päätelmiä, joita työssä esitetään ja tästä syystä kirjottajien töitä avataan tässä luvussa enemmän.

Knappin ym:n tutkimus [14] kuvaa, millainen prosessi ja millaiset tahot vaikuttavat tietoturvapolitiikan suunnitteluun. Tämän malli kautta nähdään, miten monimutkainen prosessi tietoturvapolitiikan rakentaminen on. Tutkimus toimii hyvänä yleispohjana tietoturvapolitiikan ymmärtämisessä, sillä se ottaa huomioon myös muiden mainittujen kirjoittajien esiin tuomat tärkeät politiikkaan vaikuttavat tahot ja asiat, kuten johdon tuen, kulttuurin ja liiketoiminnan tukemisen. Tutkimusta voi käyttää indeksinä tärkeiden tutkimusalueiden löytämiseksi, sillä se ei mene yksityiskohtiin esiin nostetuissa aiheissa, mutta tutkimus varmistaa, että siinä esitetty teoria on olennaista tietoturvapolitiikan kannalta.

Baskervillen ja Siposen tutkimus [15] tietoturvallisuuden metapolitiikasta on yksi yleisimmin esiin nousevista tutkimuksista, kun haetaan aineistoa tietoturvapolitiikkaan liittyen. Työ kerää ja määrittelee paljon tietoturvapolitiikan abstraktiotasoihin liittyviä konsepteja, kuten korkea- ja matalatasoiset tietoturvapolitiikat sekä metapolitiikan. Tästä on myöhemmin johdettu paljon käsitteitä, kuten kokonaiset ja järjestelmäkohtaiset politiikat, jotka ovat muussa kirjallisuudessa esillä (esimerkiksi [7]). Baskerville on tämän lisäksi tehnyt paljon tutkimusta tietojärjestelmiin ja niiden tietoturvallisuuteen

liittyen. Tietojärjestelmät ovat olennainen osa nykyaikaista liiketoimintaa ja niitä hyödynnetään myös tietoturvallisuuden hallinnassa.

Metapolitiikan tutkiminen on tuonut tietoturvapolitiikan kentälle uutta pohdittavaa ja se on auttanut ymmärtämään tietoturvapolitiikan suunnittelun rajojen määrittelemistä, sillä tutkimus toteaa, että vaikka standardit nopeuttavat tietoturvapolitiikan kehittämistä, eivät ne auta ratkaisemaan olennaista ongelmaa: yritysten ainutlaatuisia toimintaympäristöjä [15]. Toimintaympäristöt vaikuttavat tietoturvapolitiikkaan ja sen laadintaan, sillä ne sekä mahdollistavat että rajoittavat erilaisia tietoturvallisia ratkaisuja. Toki korkean tason politiikassa tämä vaikutus voi olla pienempi, koska abstraktiotaso on korkeampi, mutta toimintaympäristö tekee tietoturvapolitiikasta uniikin jokaisessa organisaatiossa.

Siponen on tämän lisäksi tutkinut paljon tietoturvahallintoon liittyviä aiheita. Hänen tutkimuksensa [16] yhdessä Puhakaisen kanssa käsittelee koulutusten merkitystä tietoturvapolitiikan noudattamisen kontekstissa. Työ korostaa ihmisen merkitystä tietoturvapolitiikan onnistumiselle ja pyrkii näyttämään, miten merkityksellinen toimiva koulutus on osana tietoturvapolitiikan sisäistämistä. Tietoturvapolitiikan noudattaminen on myös muussa Siposen tutkimuksessa [17, 18] esillä. Näissä tutkimuksissa on selvitetty, mitkä asiat vaikuttavat tietoturvapolitiikan noudattamiseen ja kuinka ihmisten omat uskomukset omiin kykyihinsä ja niiden vaikuttavuuteen merkitsevät noudattamisen kontekstissa.

Vaikka koulutukset eivät liity suoraan tietoturvapolitiikkaan, ovat niiden käytännön merkitykset suuremmat. Jalkauttaminen on olennainen osa onnistuneen tietoturvapolitiikan suunnittelemista. Pelkästä kirjoitetusta määräyksestä ei ole yrityksen toiminnalle hyötyä vaan se pitää saada jatkuvaan käyttöön. Tämän lisäksi noudattamiseen vaikuttavat myös muut seikat kuin tietoisuus asiasta ja noudattamiseen voi vaikuttaa erilaisten motivointikeinojen kautta. Tässä työssä halutaankin korostaa, että onnistuneen tietoturvapolitiikan suunnittelussa tulee ottaa huomioon, miten jalkauttaminen toteutetaan.

Niemimaan väitöskirja [13] ja siihen liittyvät tutkimukset osoittavat vahvasti, miten merkityksellinen kulttuuri, sekä yritys- että tietoturvakulttuuri, on tietoturvapolitiikan kehittämisessä. Väitöskirjan mukaan ihmisten merkitys tietoturvapolitiikan täytäntöönpanossa on monialainen. Yrityksen hallinnon tulee tunnistaa voimassaolevat toimintatavat, jotta he voivat luoda tehokkaan politiikan [19]. Myös kansainvälisesti toimiviksi todettuja käytäntöjä tulee hyödyntää. Tästä Niemimaa E ja M puhuvat myös tutkimuksessaan [20], jossa kuvataan, miten standardeista ja muista toimivista tavoista saa yritykselle sopivia ratkaisuja. Henkilöstön tulee olla vahvasti mukana politiikan luomisessa, jotta politiikka hyväksyttäisiin helpommin ja että sen voi muuttaa tehokkaammin käytännön toiminnoiksi [21]. Näistä kolmesta tutkimuksesta Niemimaa rakensi tietoturvapolitiikan rakentamisen kolme pilaria: tietoturvallisuuden parhaista

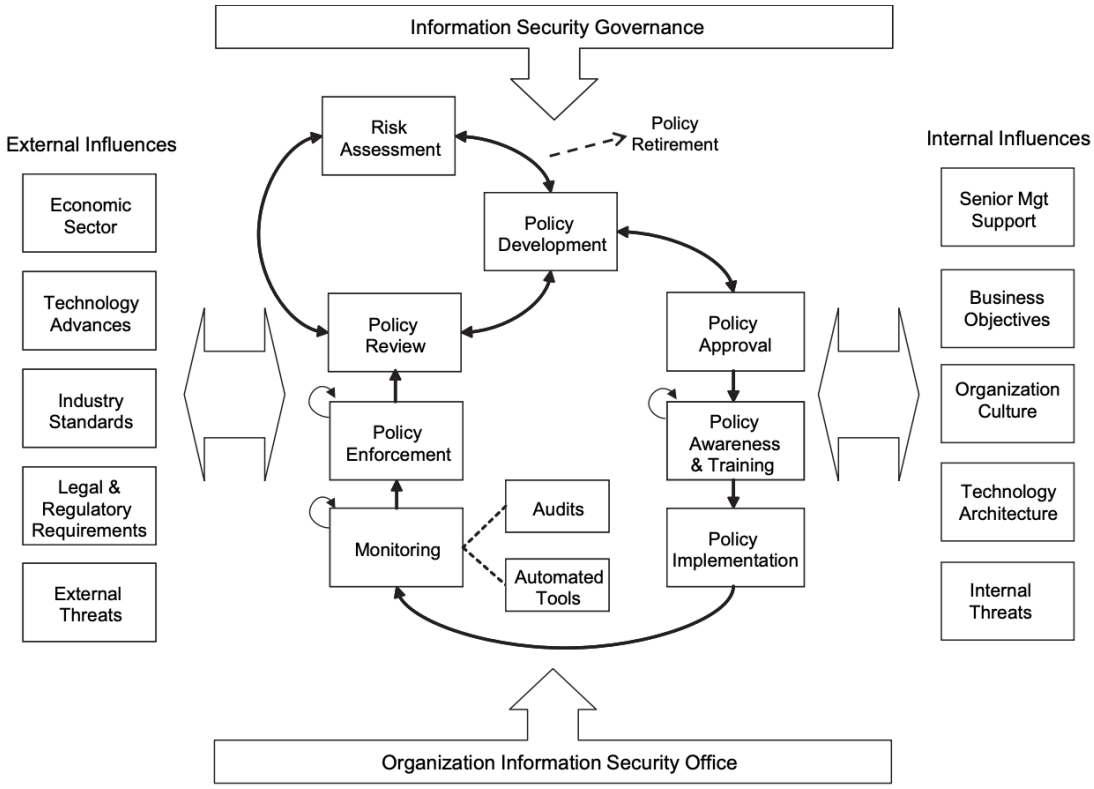
tavoista lainaaminen, sidosryhmien syvällinen osallistaminen ja politiikan legitimointi [13].

Niemimaa luonnehtii väitöskirjassa erinomaisesti nykyaikaisen tietoturvapolitiikan luontia, jonka tulee ottaa huomioon paljon pehmeitä arvoja ja ihmisten toimintaa eikä vain nojata johdon olettamuksiin. Tietoturvakulttuurin merkitys tietoturvapolitiikkaa kohtaan syntyvissä asenteissa on selkeä ja siksi tietoturvakulttuuria korostetaan tärkeänä osana tietoturvapolitiikkaa ja sen jalkauttamista. Sekä Siposen että Niemimaan tutkimukset korostavat, että tietoturvapolitiikkaan ei ole yhtä oikeata ratkaisua vaan se on yrityksensä näköinen ja sen tulee olla yrityksen tarpeiden mukainen.

Näistä tutkimusalueista – tietoturvapolitiikan rakentaminen, tietoturvapolitiikan noudattaminen ja tietoturvakulttuuri – rakentuu tietoturvapolitiikan jalkauttamiseen liittyvä teoria tämän työn yhteydessä. Muitakin konsepteja tuodaan esiin, mutta nämä kolme konseptia luovat pohjan jalkauttamisen lisäksi myös tietoturvapolitiikan luonnille. Luvussa 5 kuvataan rakenne tietoturvapolitiikalle, pohjautuen tässä luvussa mainittuihin lähteisiin ja haastatteluista esiin nousseisiin haasteisiin.

2.3 Rakentaminen

Tietoturvapolitiikan rakentamisella kiteytetään yrityksen tietoturva selkeiksi määräyksiksi, jotka muutetaan toiminnaksi ohjeiden ja koulutusten kautta. Rakentaminen koostuu useista osista, jotka yleensä ovat suunnittelu, toteutus ja seuranta [13]. Rakennusprosessista on myös hienojakoisempia versioita, joista yleisin on seitsemänosainen: kehitysryhmän kerääminen, riskianalyysi, organisaatiokulttuurin ja teknologioiden tunnistaminen, turvakontrollien tunnistaminen, politiikan rakentaminen, politiikan jalkauttaminen, seuranta ja kehitys [11]. Tässä työssä keskitytään kolmijakoiseen prosessiin, jossa on huomioitu hienojakoisen prosessin osia.



Kuva 3. *Tietoturvapolitiikan kehitysprosessi [14]*

Tietoturvapolitiikan kehitysprosessiin vaikuttavat monet tekijät ja tahot. Kuvassa 3 on esitetty tietoturvapolitiikan kehitysprosessi ja siihen vaikuttavat tahot. Tästä voi hyvin nähdä, että politiikan kehittäminen on hyvin monimutkainen kokonaisuus, johon vaikuttavat monenlaiset ulkoiset ja sisäiset tahot ja sen tuottaminen ja käyttöönotto vaatii useita vaiheita.

Jos kuvaa 3 lähtee purkamaan tarkemmin alkaen kohdasta politiikan kehittäminen (policy development), jota tehdään yhdessä riskiarvion (risk assessment) ja politiikan arvioinnin (policy review) kanssa. Riskiarvioinnissa sekä ulkoiset (external influences) että sisäiset (internal influences) tekijät vaikuttavat tunnistettuihin riskeihin. Liiketoiminnan ala (economic sector), teknologian kehitys (technology advances), ulkoiset ja sisäiset uhat (internal & external threats) tuovat mukanaan suoraan uusia riskejä. Toimialan standardit (industry standards), lait ja sääntely (legal & regulatory requirements) ja teknologia-arkkitehtuuri (technology architecture) voivat joko kasvattaa tai pienentää mahdollisten riskien määrää. Kehittämistä jatketaan, kunnes politiikka hyväksytään (policy approval), joka vaatii johdon tukea (Senior Mgt Support) ja politiikan pitää tukea liiketoiminnan tavoitteita (business objectives). Hyväksynnän jälkeen alkaa kouluttaminen ja tiedottaminen (policy awareness & training), jotka ovat osa politiikan jalkauttamista (policy implementation). Tähän vaikuttavat organisaation kulttuuri (organization culture), miten jalkauttaminen tapahtuu ja onnistuu. Jalkauttamisen jälkeen alkaa seuranta (monitoring), jota toteutetaan auditoinneilla (audits) ja automaattisilla työkaluilla (automated tools). Jos seurannalla havaitaan jotain, politiikan toimeenpano (policy

enforcement) vaatii, että rikkomuksista aiheutuu sanktioita. Tämän jälkeen palataan taas politiikan kehittämiseen, jotta seuranta ja valvonta asetetaan oikeille kohteille.

Kuvien 1 ja 3 välillä on yhtäläisyyksiä, joiden avulla ne kytkeytyvät yhdeksi kokonaisuudeksi. Kuvassa 1 esitettyyn tietoturvallisuuden hallintaan voidaan yhdistää kuvan 3 tietoturvahallinto (information security governance) ja organisaation tietoturvatoimisto (organization information security office), jotka molemmat vastaavat tietoturvallisuuden hallinnasta. Kuvan 3 prosessi on tiivistetty kuvassa 1 kohtiin tietoturvapolitiikan rakenne, elinkaari ja tila. Työssä käsitellään tietoturvapolitiikkaa näiden osa-alueiden kautta pääasiassa korkealta tasolta, mutta kuvan 3 esittämiä käsitteitä avataan seuraavissa alaluvuissa ja pohditaan, miten ne vaikuttavat tietoturvapolitiikkaan kokonaisuutena.

2.3.1 Politiikan suunnittelu

Tietoturvapolitiikan rakentaminen alkaa suunnittelusta. Politiikan suunnittelu ja toteutus ovat yhtä tärkeitä kuin itse lopullinen politiikka, sillä suunnittelu- ja toteutusvaiheissa luodaan pohjaa koko tietoturvakulttuurille ja ohjeita, jotka vaikuttavat tietoturvan kehittymiseen organisaatiossa [21]. Suunnittelun avulla määritetään politiikan tarpeet, rajoitukset ja sidosryhmät. Toteutuksen tulee olla niin kestävällä pohjalla, että politiikkaa tulisi voida käyttää kolmesta viiteen vuotta [3]. Tänä aikana liiketoiminta ja teknologia ehtii todennäköisesti muuttua niin paljon, että päivitystoimenpiteille on tarvetta.

Suunnittelun tärkeimmät osat ovat henkilöstön, johdon sekä muiden sidosryhmien kuuleminen. Henkilöstön tukea tarvitaan, jotta politiikasta tulee sellainen, jota voi ja haluaa noudattaa. Tietoturvapolitiikan vaikutus henkilöstöön on yksi suurimmista tekijöistä syntyvässä tietoturvakulttuurissa [22]. Kuten luvussa 2.2 todettiin, henkilöstö on tunnistettu yhdeksi suurimmaksi riskiksi yrityksen tietoturvalle. Tästä syystä henkilöstön sitouttaminen tietoturvapolitiikkaan on kriittistä sen onnistumiselle. Ensimmäinen askel tähän on ottaa henkilöstö mukaan tietoturvapolitiikan suunnitteluun [22]. Henkilöstöllä on myös paljon valmiita toimintatapoja ja ajatuksia tietoturvallisuudesta, jotka tulisi saada osaksi luotua politiikkaa, koska se on todettu tehokkaaksi legitimointistrategiaksi [19].

Johdon tukea tarvitaan, jotta tietoturvapolitiikka nähdään osana yrityksen strategiaa, ja että sille myönnetään riittävästi resursseja. Johto myös hyväksyy lopullisen politiikan. Politiikkaa luodessa tehdään usein riskiarvioita, joiden pohjalta luodaan hinta-hyöty-suhdeanalyyseja. Näiden pohjalta johto voi valita tarpeelliset tietoturvakontrollit. [22] Myös johdon osallistuminen tietoturvapolitiikan luomiseen vaikuttaa positiivisesti tietoturvapolitiikan jalkauttamiseen, johtuen johdon esimerkin tuomasta uskottavuudesta [7, 22]. Johto voi omilla toimillaan auttaa tietoturvapolitiikan jalkautumisessa. Jos johto noudattaa samoja sääntöjä kuin kaikki muut, on henkilöstö motivoituneempi noudattamaan ohjeita [12].

Erilaiset muut sidosryhmät ovat myös tärkeä osa tietoturvapolitiikan toteutusta. Tietoturva koskettaa koko yrityksen henkilöstöä ja myös yhteistyössä toimivia ryhmiä, kuten alihankkijoita. Tämän takia kaikkia oleellisia sidosryhmiä tulisi pyrkiä kuuntelemaan suunnitteluvaiheessa, jotta syntynyt näkemys vastaa oikeaa tarvetta ja politiikka tukisi toimintaa mahdollisimman tehokkaasti [23]. Ulkoiset toimijat tuovat mukanaan myös uudenlaista kokemusta [22], jota ei välttämättä yrityksen sisältä löydy.

Tietoaineistoihin liittyy aina riskejä, joiden tunnistamista varten tarvitsee toteuttaa riskianalyysi. Riskianalyysi on usein ensimmäinen suunnitteluun liittyviä vaihteita, kun politiikan kehitystiimi on valittu [11]. Tunnistamalla mahdolliset riskit, suojamekanismit voidaan asettaa riittävälle tasolle niin että niiden käyttö ei muutu liian hankalaksi eikä toteuteta liian kalliita suojamekanismeja. Riskianalyysin toteuttamiseen on monenlaisia ohjeita, monet niistä keskittyvät yleisiin riskeihin, kuten PK-HAAVA, mutta muun muassa Valtiovarainministeriö [24] tarjoaa ohjeet digitaalisen turvallisuuden riskienhallintaan ja analyysiin.

Riskianalyysin toteuttaminen vaatii laajasti tietoa yrityksen tietoaineistoista, toimintatavoista ja henkilöstöstä, jotta mahdollisimman suuri osa riskeistä tunnistetaan. Mahdollisimman laaja sidosryhmien käyttö näkyy myös riskienhallinnassa, koska eri sidosryhmät tuntevat omat toimintatapansa parhaiten ja pystyvät osoittamaan niihin liittyviä mahdollisia riskejä [22]. Riskejä tunnistetaan myös myöhemmin ja siksi riskienhallinnan tulee olla jatkuva prosessi, joka reagoi muutoksiin [24], ja siksi riskienhallinnan tulee olla mukana politiikan ylläpitoon liittyvissä prosesseissa. Tunnistetut riskit tulee analysoida, minkä perusteella voi määrittää riskien vaikutukset ja toimenpiteet riskien vaikutuksien vähentämiseksi tai poistamiseksi.

Toinen tärkeä suunnittelun osa on tietoturvallisuuden tarpeen määrittely. Aiemmin tuotiin esiin johdon tuen tärkeys, joka on myös tärkeä osa tietoturvan ja sen politiikan tarpeen määrittelyä. Kuten luvussa 2.1 mainittiin, organisaatioilla on erilaiset tietoturvatarpeet ja tämä pitää ottaa huomioon suunnittelussa ja tietoturvapolitiikka tulee rakentaa oikean tarpeen mukaisesti eikä vain kopioida olemassa olevia politiikoita. Tietoturvan perimmäinen tarkoitus on kuitenkin turvata koko liiketoiminta ja sen tehokas yhdistäminen bisnekseen on äärimmäisen tärkeätä tehokkaan tietoturvallisuuden luomiseksi. Tarve voi olla joko sisäinen tai ulkoinen. Sisäisenä motivaationa pidetään havaintoa, että tietoturvaa tarvitaan toimien varmistamiseen. Ulkoisena motivaationa toimii usein jokin asiakas tai muu sidosryhmä, joka vaatii tietyn tasoista tietoturvaa. Yhteistyösopimuksissa toinen osapuoli voi velvoittaa tiettyjä tietoturvatarpeita, jotka voivat vaikuttaa yritysten tietoturvapolitiikkaan. Tarpeen määritelmä on myös tärkeä politiikan lukijan ymmärryksen kannalta, kun tietoturvapolitiikka dokumentoidaan.

Kun tiedetään tarpeet, voi tietoturvan seuraamiseen ja ylläpitoon jakaa vastuita ja rooleja. Vastuilla pyritään asettamaan selkeitä omistajia tietyille toiminnoille, jotta niiden

toteutumista ohjataan ja seurataan aktiivisesti. Vastuualueita voivat olla tietoaineistot, tietojärjestelmät tai liiketoimintayksiköt. Jako vaihtelee yrityksen tarpeiden mukaan.

2.3.2 Politiikan rakenne

Tietoturvan tarve voi vaihdella organisaatioiden välillä. Organisaation tarpeet voivat muuttua ajan myötä paljon ja tietoturvapolitiikan pitää heijastaa tätä. Tätä varten on tutkittu sääntöjä politiikoille, jotta niitä voi muuttaa tarpeen vaatiessa nopeastikin ja silti niin, että ne noudattaisivat organisaation yleistä linjaa. Tällöin puhutaan metapolitiikasta, jolla määritellään politiikka politiikoille [15].

Tämän lisäksi voi olla järjestelmä- tai tapauskohtaisia politiikoita tai ohjeita. Järjestelmäkohtaiset politiikat toimittavat kahta tehtävää. Ensinnäkin ne toimivat perinteisen politiikan tavoin antaen ohjeita ja rajoituksia järjestelmien käyttöön. Kun järjestelmien tarve ja tavoitteet ovat kuvattu selkeästi, järjestelmien politiikkoja voi käyttää myös käytön suunnittelussa operatiivisella tasolla. Toiseksi ne tuottavat määrittelyjä järjestelmille, kuten järjestelmiin vaadittavat pääsyoikeudet. Nämä säännöt eivät kuitenkaan mene käyttäjätasolle vaan koskettavat enemmän käyttäjäryhmiä ja miten ne pääsevät järjestelmiin käsiksi. [7]

Tapauskohtaiset politiikat ovat tarkempia kuin tietoturvapolitiikka yleensä ja ne ottavat usein kantaa tiettyihin teknologioihin, kuten sähköpostiin tai Internetin käyttöön. Niiden tulee kuitenkin määritellä tarve politiikalle ja kuvata sen tarkoitusta, niin kuin tietoturvapolitiikkakin tekee. Tapauskohtaisella politiikalla on tarkoitus rajata ketkä käyttävät mitäkin teknologioita ja työkaluja ja mihin niitä käytetään. Näin päästään hyvin liiketoimintayksiköiden tarpeiden määrittelemiin rajoituksiin ja pyritään rajaamaan mahdollisimman laajasti kaikki haitalliset käyttötavat. Politiikan tehokkuus voi kuitenkin olla hyvin rajallista työmäärään suhteutettuna, koska sitä on vaikea hallita ja se saattaa jättää joitain tapauksia huomioimatta. [7]

Järjestelmä- ja tapauskohtaisia – matalatasoisia – politiikoita voivat tarvita yritykset, joilla on paljon erillisiä yksiköitä, jotka tarvitsevat omia määräyksiään ja rajoituksia tietoturvalliseen toimintaan. Suuri määrä erilaisia politiikoita voi osoittautua hallinnolliseksi haasteeksi, kun pitää jakaa, hallita ja valvoa kaikki määräyksiä [7]. Tästä tullaan politiikan rakenteen haasteisiin. Modulaarisen politiikan on huomattu olevan suotuisin politiikan rakenne kirjallisuudessa [6, 7], sillä ne ovat keskitetysti hallittuja sisältäen sekä yleisiä määräyksiä että järjestelmäkohtaisia vastuita ja käyttöohjeita [6]. Yksilölliset politiikat osoittautuvat haastavaksi suuremmissa organisaatioissa, mutta ne voivat toimia pienemmissä yrityksissä [7]. Viimeinen kirjallisuudessa tunnistettu rakenne on kokonainen rakenne, jossa määrätään keskitetysti yhdestä dokumentista kaikki käytetyt teknologiat ja annetaan yleisiä ohjeita käytettyihin järjestelmiin [6]. Tämä on Whitmanin ym:n [2001] mukaan yleisin käytetty tietoturvapolitiikan rakenne.

2.3.3 Standardit, kehykset ja lait

Toteutuksen taustalla voivat myös olla standardit, kehykset ja lait. Yksi yleisimmistä standardeista ovat jo aiemmin mainittu ISO 27000-standardiperhe, joka määrittelee standardit tietoturvallisuuden hallintajärjestelmälle. Standardiperheen ISO/IEC 27001 määrittelee vaatimukset järjestelmälle [25]. ISO/IEC 27001 asettamat vaatimukset helpottavat tietoturvapolitiikan suunnittelua, sillä se määrittelee selkeästi, mitä tietoturvapolitiikan tulee sisältää, miten sen kanssa tulee toimia ja miten sitä käytetään johtamisen tukena. COBIT:n viides versio tarjoaa kehyksen liiketoiminnan IT:n hallintaan ja johtamiseen [26]. Sitä käytetään tiedon laadun ja siihen liittyvien riskien hallintaan eikä se suoraan ole tietoturvapolitiikan pohjaksi soveltuva kehys, mutta siitä johdetaan erilaisia tarpeita ja tekniikoita tiedon suojaamiseen. NIST SP 800-53 ohjeet ovat alun perin Yhdysvaltojen julkisille tahoille suunniteltu julkaisu, joka tarjoaa kattavasti tietoturvaan liittyviä kontrolleja, joita monet yksityiset tahot käyttävät tietoturvan hallintaan [27]. Pelkillä standardeilla ja ohjeilla ei voi rakentaa onnistunutta tietoturvapolitiikkaa, sillä ISO/IEC 27001-vaatimukset sanovat, että tietoturvapolitiikan tulee ”soveltua organisaation toiminta-ajatukseen” eli se pitää suunnitella yrityksen tarpeisiin.

Valtionvarainministeriön julkaisussa [2007] listataan useita lakeja, joiden noudattamista vaaditaan julkisilta toimijoilta ja niiltä yksityisiltä toimijoilta, jotka ovat mm. ”mukana turvallisuusluokitellussa sopimuksessa” [28]. Tällaisia ovat ”Laki kansainvälisistä tietoturvallisuusvelvoitteista”, ”Laki viranomaisen toiminnan julkisuudesta”, ”Asetus viranomaisten toiminnan julkisuudesta ja hyvästä hallintotavasta” ja Suomen ja muiden organisaatioiden väliset sopimukset [3, s. 26]. Tämän lisäksi on lukuisia alakohtaisia lakeja, kuten pankki- ja vakuutusalalla.

Tietoturvapolitiikan rakentamisen jälkeen politiikka pitää jalkauttaa eli ottaa käyttöön koko organisaatioissa. Tähän liittyy paljon haasteita, jotta politiikka ottaisi kiinni käytäntöihin ja että siitä saataisiin rakennettua toimivia toimintatapoja. Seuraavassa luvussa esiteltävien hallintokeinojen avulla vaikutetaan, miten tietoturvapolitiikka otetaan vastaan ja miten rakentamisprosessi viedään onnistuneesti käytäntöön.

2.4 Hallintokeinot

Tietoturvan tärkein tehtävä on tukea yrityksen liiketoimintaa suojaamalla se erilaisilta tietovuodoilta ja hyökkäyksiltä. Tietoturvapolitiikan pitää pystyä tukemaan tätä ja siksi sen onnistumiselle on paljon erilaisia toimintaedellytyksiä. Tietoturvapolitiikan hallintokeinojen avulla hallitaan tietoturvapolitiikan jalkauttamista ja politiikan valvontaa. Tässä luvussa käydään läpi hallintokeinoja ja hallintoon vaikuttavia seikkoja.

2.4.1 Tietoturvakulttuuri

Tietoturvakulttuuri tarkoittaa niitä uskomuksia, havaintoja, asenteita, oletuksia, tapoja ja arvoja, jotka liittyvät tietoturvaan ja sitä, miten ne näkyvät ihmisten toiminnassa [29, 30]. Tämä on tärkeä osa tietoturvapolitiikan laadintaa, sillä olemassa olevat osat vaikuttavat uusien toimien laadintaan. Niemimaa [13] havaitsi, että yrityksessä vallitsevat tavat muovaavat politiikan rakentamista, mutta politiikan rakentaminen muovaa yrityksen vallitsevia tapoja.

Kulttuurin on huomattu olevan tärkein tekijä yrityksen koko toiminnan onnistumisessa [31]. Ihmisten toiminta ja asenteet vaikuttavat kaikkeen yrityksen toimintaan ja ne muovaavat myös kehityksen suuntaa. Tietoturvahallinto ei ole tästä toiminnasta mitenkään erillään ja siksi siihen vaikuttavat samat haasteet kuin muihinkin organisaation toimintojen hallintoon. Motivaatiot ja asenteet vaikuttavat tietoturvatoimintojen muutokseen yhtä lailla kuin yrityksen työajan seurantaan. Tästä syystä tietoturvakulttuurin kehittäminen pitää ottaa huomioon, kun tietoturvapolitiikkaa kehitetään. Kulttuuri ei kuitenkaan synny lyhyessä ajassa vaan se on pitkäjänteisen työn tulos. Toimintoja tulee peilata ihmisten arvoihin, kun uusia toimintoja suunnitellaan ja vanhoja kehitetään. Tähän käytetään usein Hofsteden ym:n [32] organisaation kulttuurin kehystä, jossa kuvataan kuusi dimensiota yrityksen suuntauksista. Nämä dimensiot on esitelty taulukossa 1. Esitellyt organisaatiokulttuurin dimensiot vaikuttavat tietoturvakulttuuriinkin. Tiukoissa organisaatioissa uusien sääntöjen käyttöönotto voi olla helppoa, mutta lopputulos ei välttämättä tue toimintaa. Toisaalta, löyhemmissä organisaatioissa uusien määräysten käyttöönotto voi olla haastavampaa, koska uskotaan vapaaseen työskentelyyn ja täten uudet ohjeet eivät tule osaksi jokapäiväistä toimintaa.

Taulukko 1. *Organisaatiokulttuurin kuusi dimensiota*

Dimensio eli onko, organisaatio…	**Selite**
…prosessi- vai tulospainotteinen?	Kuvaa, miten yritys suhtautuu työtapoihin. Noudatetaanko olemassa olevia tapoja vai innovoidaanko uusia tapoja, joilla saadaan parempia tuloksia.
…henkilöstö- vai työpainotteinen?	Kuvaa, miten yritys suhtautuu henkilöstöön. Tuleeko yrityksen pitää huolta henkilöstöstään vai koetaanko, että yritystä kiinnostaa vain työn tulokset.
…yhteisö- vai ammattilaisuuspainotteinen?	Kuvaa, millaisia jäseniä työyhteisössä tulee olla. Otetaanko huomioon ihmisen sosiaaliset taustat vai keskitytäänkö vain ammatilliseen kokemukseen.
…järjestelmältään avoin vai suljettu?	Kuvaa, millainen yrityksen ilmapiiri on. Jaetaanko tietoa ja kokemuksia avoimesti vai onko käytös sulkeutuneempaa.

…kontrolliltaan löysä vai tiukka?	Kuvaa, miten tarkasti sääntöjä ja hierarkiaa tulee noudattaa. Seurataanko kaikkea tarkasti vai joustetaanko esimerkiksi kellonajoissa.
…ohjeellinen vai käytännönläheinen?	Kuvaa, miten asiakasta halutaan palvella. Noudatetaanko vain tiukasti prosesseja vai joustetaanko prosesseista asiakaspalvelun parantamiseksi.

Tietoturvapolitiikalla ja siihen pohjautuvilla hallinnon keinoilla vaikutetaan vahvasti myös yrityksessä vallitsevaan tietoturvakulttuuriin. Schlienger ja Teufel [29] toteavat tietoturvakulttuurin hallinnan koostuvan viidestä osasta: esiarvio, strateginen suunnittelu, operatiivinen suunnittelu, toteuttaminen ja jälkiarvio. Tietoturvapolitiikan kehittäminen kuuluu strategiseen suunnitteluun. Taulukon 1 dimensioiden avulla tunnistetaan tehokkaita keinoja tietoturvakulttuurin kehittämiseen, mutta politiikan pitää myös olla linjassa näiden dimensioiden kanssa. Jos huomataan, että yrityksessä noudatetaan tarkasti prosesseja, voi olla esimerkiksi hyvä tutustua näihin prosesseihin ja asettaa tietoturvallisempia toimintoja osaksi näitä prosesseja. Avoimissa yrityksissä esimerkiksi keskustellaan koko organisaation kesken, millaiset tavoitteet tietoturvalle halutaan asettaa.

Kuvan 3 perusteella tietoturvakulttuuri vaikuttaa tietoturvapolitiikkaan ja myös toisinpäin. Yrityksessä voi esimerkiksi vallita vahva tietoturvallisten toimintatapojen kulttuuri, kuten pankkialalla voi olettaa olevan. Tiedetään, että käsiteltävät asiat ovat tärkeitä monille tahoille ja tunnistetaan käsiteltävän tiedon arvo. Kun tällaisessa ympäristössä laaditaan ja otetaan käyttöön tietoturvapolitiikkaa, sen tuomat muutokset hyväksytään helpommin, jos ne parantavat tietoturvaa jokapäiväisessä toiminnassa. Tämä vaikuttaa myös toiseen suuntaan. Vahvan tietoturvakulttuurin takia halutaan vaikuttaa aktiivisesti tietoturvapolitiikkaan ja sen johdannaisiin. Tällöin on mahdollista, että mielipiteitä syntyy paljon ja voi olla vaikea koota kokonaisuus, joka miellyttää kaikkia.

2.4.2 Tietoturvatietoisuus

Tietoturvatietoisuus on tärkeä osa tietoturvapolitiikan onnistumista. Tietoisuus käsitteenä tarkoittaa tietoa ja ymmärrystä, asenteita ja näkemyksiä tietoturvasta eikä se ole pelkästään opettamista ja koulutuksia [33]. Lisäämällä tietoisuutta ihmisten käyttäytymistä voi muuttaa eri tilanteissa ja tietoturvallisuuden kontekstissa tämä voi tarkoittaa tapojen muuttumista esimerkiksi tietojen kalastelun yhteydessä. Yksi vuoden 2018 isoimmista tietoturvauhista oli erilaiset yrityksille kohdistetut kalastelu- ja huijausviestit, kuten Microsoft Office 365 -kalasteluviestit [34]. Tämän takia Suomen Kyberturvallisuuskeskus on julkaissut paljon materiaalia, jolla kehitetään kansallista tietoutta. Yritykset ovat myös pyrkineet levittämään tietoisuutta asiasta. Nämä ovat hyviä

esimerkkejä siitä, miten tietotoisuuden lisäämisellä pyritään vähentämään tietoturvariskien määrää ja vaikutusta.

Tietoturvallisuustietoisuuden kehittämisohjelmia järjestetään useissa organisaatioissa. Niissä pyritään kehittämään koulutuksia, tiedottamista ja yleistä tietoturvaviestintää niin, että organisaation osaamista voi kehittää ja ylläpitää. McIlwraith [33] toteaa kirjassaan, että tietoisuuden lisääminen on tehokkain tapa luoda positiivista muutosta organisaatiossa. Tästä syystä tietoturvapolitiikan luominen ei itsessään riitä tietoturvan parantamiseen vaan tietoturvatietoisuutta pitää lisätä samalla. Tietoisuutta lisätään pitkälti kouluttamalla, joko virallisesti tai epävirallisesti [35]. Viralliset koulutukset ovat hallittuja ja jäsenneltyjä kokonaisuuksia, kuten luentoja tai verkkopohjaisia koulutuksia. Epäviralliset koulutukset ovat tarkoituksenmukaisia, mutta niitä ei rajata tiettyihin prosesseihin, kuten virallisia koulutuksia. Epävirallisia koulutustyyppejä ovat muun muassa julisteet ja ”kotivideot”, eli kotikutoisen oloiset ja usein humoristiset opetusvideot.

Jatkuva kouluttaminen on kriittinen osa onnistunutta tietoturvaohjelmaa [16]. Aikuisten kouluttamisessa on tärkeää pitää mielessä, että aikuiset oppivat asioita eri tavalla kuin lapset. Aikuisilla on vahva itsetietoisuus ja organisaation kulttuurin tavoin, tietoisuus tuo mukanaan tietoa ja asenteita, jotka vaikuttavat siihen, miten tilanteet koetaan [33]. Tästä syystä, kun koulutuksia suunnitellaan, tulee ottaa huomioon organisaation jäsenten osaamisen taso [16] ja suunnitella eritasoisille oppijoille omanlaiset kokonaisuudet. Kun oppija kokee koulutuksella olevan jonkinlaista arvoa, hän on huomattavasti halukkaampi oppimaan uutta [33]. Koulutuksia on kahdentyyppisiä: passiiviseen ja aktiiviseen oppimiseen perustuvia.

Passiiviseen kouluttamiseen perustuvat koulutukset ovat tilanteita, joissa osallistujat kuuntelevat yhtä tai useampaa kouluttajaa, joka luennoi aiheesta. Tällaisia koulutuksia voi järjestää joko paikan päällä tai verkossa. Paikan päällä pidetyissä koulutustilaisuuksissa voi käyttää aktivoivia tai mielenkiintoa herättäviä tekniikoita, kuten esimerkkivideoita tai tarinankerrontaa [35]. Täysin passiiviset opetustavat, eli kuunteluun tai lukemiseen perustuvat koulutukset, on huomattu tehottomiksi ja siksi luennoidessakin tulisi käyttää yleisön kanssa interaktiivisia keinoja. Yleisölle esitettyjen kysymyksien tai avoimen keskustelun avulla voi lisätä oppimistilaisuuksia koulutusten aikana. Näin opiskelijat pysyvät keskittyneinä aiheeseen ja auttaa heitä muistamaan aiheen myös tulevaisuudessa [36].

Aktiivisessa oppimisessa osallistuja pääsee itse tekemään asioita, kuten harjoituksia tai testejä. Tällöin osallistuja joutuu hyödyntämään juuri kuulemaansa tai lukemaansa ja keksimään ratkaisuja ongelmiin, mikä parantaa oppimista [35]. Harjoitusten tulee kuitenkin olla opiskelijalle jollain tavalla henkilökohtaisia, jotta niiden aiheuttamat seuraamukset ovat selkeästi ymmärrettävissä ja jäävät näin paremmin mieleen [16].

Aktiivisen oppimisen suunnittelu on haastavaa, sillä opiskelijoilla voi olla useita erilaisia oppimistapoja. Näitä on seitsemän tapaa: visuaalinen eli henkilö suosii kuvia ja tiloja, auditiivinen eli henkilö suosii ääniä ja musiikkia, sanallinen eli henkilö suosii kirjoitettua ja puhuttua kieltä, fyysinen eli henkilö suosii kehon ja käsien käyttöä ja koskemista, looginen eli henkilö suosii päättelyä ja järjestelmiä, sosiaalinen eli henkilö suosii yhdessä oloa ja yksinoppiminen eli henkilö suosii toimia itsenäisesti [35]. Jokainen käyttää oppiessaan yhtä tai useampaa näistä tavoista ja siksi koulutusten suunnitteleminen vaatii organisaation henkilöstön tuntemista. Oikeiden oppimistapojen löytämiseksi tulee yhdistää useita eri tapoja koulutuksissa ja kokeilla, mitkä yhdistelmistä toimivat parhaiten.

2.4.3 Viestintä

Viestintä on tärkeä osa sekä suunnittelua että jalkauttamista. Jos organisaation jäsenet eivät tiedä politiikan olemassa olosta jo ennen sen luomista, voi motivaatio sen noudattamiseen laskea. Kun politiikan tekemisestä viestitään, organisaation jäsenet voivat antaa ehdotuksia ja he kokevat myös olevansa tärkeitä tietoturvan kehityksen kannalta. Ilman tiedottamista ei myöskään tiedetä politiikan olemassaolosta eikä henkilöstö voi tutustua siihen oma-aloitteisesti. Viestintä on myös tärkeä osa jatkuvaa kouluttamista, sillä sitä voi hyödyntää edellisessä luvussa mainitussa tietoisuuden lisäämisessä. Tästä syystä viestintä on ehdoton osa sekä osallistamista että tietoisuuden lisäämistä, sillä tietoa ei voida jakaa ilman viestintää.

Tietoturvaviestintä ei kuitenkaan saa olla irtonaista muusta yrityksen viestinnästä. Puhakainen ym. [16] osoittavat, että kun tietoturvasta viestitään samassa yhteydessä muun yrityksen viestinnän kanssa, sen koetaan olevan osa normaalia työskentelyä eikä se tunnu irtonaiselta aiheelta. Tässä korostuu yhteistyö muun organisaation kanssa. Kun halutaan viestiä tietoturvallisuuteen liittyvissä aiheissa, tulisi tehdä yhteistyötä muiden yrityksen osastojen, kuten viestinnän, kanssa. Näin tietoturvaviestintä suunnitellaan luontevasti osaksi muuta viestintää.

Koulutusten lisäksi tietoturvakäytänteistä tiedottaminen on myös tärkeä osa tietoturvapolitiikan jalkauttamista. Tätä voi tehdä esimerkiksi verkossa intranetissä tai fyysisesti ilmoitustaulujen kautta. Näin asiat saadaan jatkuvasti esiin ja organisaatiota ohjataan kohti haluttua tilaa. Erilaisten viestinnän keinojen tehokas käyttö auttaa tietoturvapolitiikan ja sen johdannaisten tuomisessa esiin, jolloin sen integroituminen osaksi jokapäiväistä toimintaa kasvaa.

2.4.4 Noudattamisen valvonta

Valvonta on keino saada tietoturvapolitiikalle voimaa taakseen. Jos tietoturvapolitiikan noudattamista ei valvota, menettää politiikka merkityksensä [14]. Usein

tietoturvapolitiikasta tehdään työsopimuksen ehto ja sen rikkomisesta voi seurata rangaistuksia.

Tietoturvapolitiikan rikkomisesta aiheutuvat seuraamukset ovat yksi paljon tutkittu tietoturvahallinnon alue. Politiikan noudattamisen varmistamiseksi on useimmiten kaksi eri lähestymistapaa: työntäminen (pushing) ja vetäminen (pulling) [37].

Perinteisesti on uskottu, että rangaistuksen, eli työntävän lähestymistavan, asettaminen on tehokkainta. Näin mahdollisesti politiikan vastaisesti käyttäytyvä henkilö huomaa, että organisaatio ”pyrkii hallitsemaan epämieluisaa käytöstä ja on täten epätodennäköisemmin toteuttamassa politiikanvastaista toimintaa” [37]. Rangaistukset voivat olla työsuhteeseen liittyviä sanktioita, kuten kertyvät varoitukset, joita voi käyttää irtisanomisen perusteena, tai vuosibonuksiin vaikuttavat vähennykset. Tämän tekniikan tehokkuus perustuu peloteteoriaan, jonka mukaan henkilö on vähemmän todennäköinen toimimaan epäsopivasti, jos tästä seuraa sanktioita [38].

Kuitenkin on huomattu, että palkitseminen, eli vetävä lähestymistapa, voi olla tehokkaampaa. Kun työntekijöitä ja muita tietoturvapolitiikan alaisuudessa toimivia henkilöitä osallistetaan ja palkitaan sopivista teoista, voivat nämä teot auttaa työntekijöitä ymmärtämään tietoturvapolitiikan tavoitteen ja sisäistämään sen paremmin [8, 37]. Oikeista asioista palkitseminen on kuitenkin tärkeää, ettei asioita tehdä vain palkintojen toivossa vaan ne nähdään positiivisena lisäetuna tavallisesta toiminnasta.

Osallistamisella tarkoitetaan johdon osoittamaa halua ottaa mukaan muita päätöksen tekoon ja päästä vaikuttamaan oman työnsä kehittämiseen. Lahtinen [39] puhuu pro gradu -työssään paljon osallistamisesta johtamisen tekniikkana ja käy läpi tarkasti, millaisia eri muotoja osallistamisella on. Osallistamisessa korostuu tärkeys, että yhteistoiminta mahdollistaa kaikille osapuolille oikean mahdollisuuden osallistua suunnitteluun ja toteutukseen eikä oikeassa osallistamisen järjestelmässä jätetä yhteistyötä vain näennäiseksi.

Tietoturvapolitiikkaa ei tulisi nähdä rangaistuksen muotona vaan tapana ”suojata organisaation omaisuutta ja täten kasvattaa organisaation liiketoimintaa” [22]. Siksi noudattamisen suunnittelua ei tulisi jättää täysin binäärisen ”rankaise tai palkitse” mallin rajoihin vaan tulisi miettiä työntekijöiden muita motivaatiota. Siksi suositellaan suunnittelemaan tietoturvan tietoisuutta kehittäviä ohjelmia, joilla tietoturvan merkitystä levitetään ja kehitetään organisaatiossa [8].

2.5 Mittaaminen

Mittaaminen on tärkeä osa toiminnan kehittämistä, sillä jos ei seurata asioiden tilaa ja muutosta, ei näitä asioita voida kehittää tehokkaasti. Standardi ISO/IEC 27004 määrittelee, että mittaaminen on ”toiminto, joka suoritetaan toiminnan tason tai

vaikuttavuuden arvon, tilanteen tai kehityssuunnan määrittämistä varten, jotta voidaan tunnistaa mahdollisia parantamistarpeita" [40]. Tietoturvapolitiikan kannalta erityisesti tilanteen ja kehityssuunnan määrittäminen on tärkeää, sillä tietoturvapolitiikasta johdetaan niin paljon erilaisia ohjeita ja käytäntöjä, että politiikan tilanteen kehittyminen vaikuttaa kaikkiin siitä johdettuihin toimintoihin.

Tietoturvan mittaamisessa ei ole yhtä oikeaa mittaria ja Salmela [41] toteaa, ettei ole vakiintunutta määritelmää tietoturvamittareille. Vuoden 2016 versio ISO/IEC 27004-standardista [40] määrittelee mittareiden tavoitteet, jotta ne sopisivat yhteen ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmän kanssa. Tässä työssä tätä käytetään mittareiden määrittelyn pohjana. Mittareita on standardin mukaan kahta eri tyyppiä: suorituskykymittareita ja vaikuttavuusmittareita. Suorituskykymittareilla todistetaan erilaisten prosessien ja hallintokeinojen edistyminen [40]. Vaikuttavuusmittarit ilmaisevat vaikutuksen, joka suunniteluilla prosesseilla ja hallintokeinoilla on organisaation tietoturvatavoitteisiin [40].

Tavoitteiden asettaminen on yksi olennainen osa mittaamista. Kun mittarit ovat olemassa, toiminnoille asetetaan tavoitteita, joiden kehitystä mittareilla mitataan. Tietoturvapolitiikan kannalta nämä tavoitteet voivat olla parempi tietoturvaymmärrys, vähemmän tietoturvatapauksia, pienentyneet tietoturvakulut tai tietoturvatoimintojen osuus IT-budjetista.

Koska tietoturvallisuutta voi mitata usealla eri tavalla, niin myös tietoturvapolitiikkaa voi mitata eri tavoilla. Tässä työssä mittarit liittyvät politiikan jalkauttamisen onnistumiseen. Tätä tutkitaan rikkomusten määrän mittaamisella ja tietoturvapolitiikan kehitykseen käytetyn ajan mittaamisen kautta. Näiden mittareiden lisäksi politiikan jalkautumisen onnistumista tutkitaan teoriaan pohjatuvalla analyysilla.

Tietoturvatoiminnan ohjaamiseen tarvitaan aina resursseja, useimmiten työajan muodossa. Tietoturvapolitiikka tarvitsee työtä sen ylläpitämiseksi, jotta se heijastaa yrityksen tietoturvan haluttua tilaa. Tämän takia tietoturvapolitiikkaa tulee päivittää aika ajoin, mutta päivitysten tiheys ja muutosten määrä riippuvat siitä, miten muutoksia kerätään ja kuinka monia sidosryhmiä kuullaan.

Tietoturvapolitiikan ylläpidossa eniten aikaa kuluu tarpeiden keräämiseen, riskienhallintaan ja aineiston analyysiin. Itse politiikka ei kokonaisuutena välttämättä muutu paljoa päivitysten aikana vaan osia siitä päivitetään tai uusia osioita lisätään. Yrityksissä syntyy uusia tarpeita ja muutoksia teknologiassa tapahtuu jatkuvasti ja näiden muutosten analysointi ja nykyiseen politiikkaan peilaaminen vie aikaa. Kulunut aika riippuu paljon yrityksen tietoturvapolitiikan abstraktion tasosta. Jos tietoturvapolitiikka kuvaa asioita hyvin korkealta tasolta, voivat muutostarpeet olla hyvin pieniä. Jos taas politiikka on rakennettu hyvin matalalle ja tarkalle tasolle, muutosten määrä voi olla huomattavasti suurempi.

Toinen toimivuuden mittaamisen lähestymistapa on politiikan noudattamisen seuraaminen. Jos huomataan paljon tahallisia rikkomuksia, voidaan todeta, että tietoturvapolitiikka ei ole yrityskulttuurin mukainen ja on täten vaikuttavuudeltaan heikko. Tämän ehkäisemiseksi on monia keinoja, joista koulutukset ovat ehkä tärkein kommunikaation menetelmä.

Koulutusten avulla tietoturvapolitiikka ja sen ohjeet saadaan viestittyä tehokkaasti ja muistettavasti kaikille sidosryhmille. Seuraamalla koulutuksiin osallistuvien henkilöiden määrää ja koulutusten määrää, voidaan mitata niiden vaikuttavuutta tietoturvapolitiikan jalkautumisen onnistumiseen. Erityisesti virtuaaliset oppimisalustat, eli verkossa tapahtuvat koulutukset, tarjoavat helposti seurattavan ja kehitettävän koulutusympäristön, jonka sisältöä kohdennetaan ja kehitetään eri ryhmien tarpeiden mukaan. Käytettiin toteutukseen mitä tahansa välineitä, tulisi niiden noudattaa luvussa 2.4.2 esitettyjä tekniikoita.

Koulutusten tehokkuuteen vaikuttaa, miten se vastaa opiskelijan nykyistä taitotasoa [16]. Mitä enemmän erilaisia taitotasoja huomioidaan koulutusten suunnittelussa, sitä tehokkaammin katetaan suurempi osa koulutettavista ja tietoisuutta tietoturvallisuudesta edistetään huomattavasti. Taitotasoa mitataan esimerkiksi testien ja kyselyiden kautta. Mittaamalla henkilökunnan taitotasoa tasaisin väliajoin, voi organisaation tietoturvatietoisuutta seurata ja koulutusten sisältöä ylläpitää.

3. TUTKIMUSMENETELMÄ

Työssä tutkittiin kymmentä Suomessa toimivaa yritystä. Yrityksistä ja niiden tietoturvapolitiikan suunnittelusta, toteutuksesta ja seurannasta kerättiin tietoa haastatteluilla. Ne toteutettiin syksyn 2018 ja kevään 2019 aikana tutkittavien yritysten toimitiloissa pääkaupunkiseudulla yhtä puhelinhaastattelua lukuun ottamatta.

Haastateltavia kerättiin julkisesti saatavilla olevista rekistereistä sekä yhteistyöyrityksen henkilökunnan kautta. Koska haastattelussa haluttiin kuulla tietoturvapolitiikan rakentamisesta, tuli haastateltavien olla johtotehtävissä yrityksissään. Tämä osoittautui haastavaksi haastattelujen sopimisen kannalta, koska tutkimukseen osallistuminen oli harvalla ensimmäinen prioriteetti. Haastateltuja lähestyttiin sähköpostitse ja jälkeenpäin myös puhelimitse, sillä nykypäivän sähköpostitulvan takia viestit hukkuvat helposti ja asia ei pääse etenemään. Tutkimuksen aikana otettiin yhteyttä noin 30 yritykseen, joista 11 oli kiinnostunut osallistumaan, mutta lopulta kymmentä pystyttiin haastattelemaan.

Yritykset edustivat eri toimialoja ja olivat myös hyvin eri kokoisia. Pienimmällä tutkituista yrityksistä oli noin 100 työntekijää ja suurimmalla yli 10 000 henkeä. Keskimäärin yritykset olivat keskisuuria, noin 250 työntekijän suuruisia yrityksiä. Jokainen tutkittu yritys toimi eri toimialalla, jotta saataisiin mahdollisimman kattava kuva pienelläkin haastattelumäärällä. Haastattelut toteutettiin puolistrukturoidusti, eli kaikille esitettiin samat kysymykset samassa järjestyksessä, mutta haastateltaville annettiin vapauksia muun muassa perustella vastauksiaan. Haastattelujen muistiinpanojen pohjalta analysoitiin tietoturvapolitiikkojen tilaa tietoturvakulttuurin luonnin näkökulmasta.

Haastatteluista kerättiin muistiinpanot eikä niistä tehty äänitteitä. Tämä johtuu aiheen arkaluonteisuuden lisäksi siitä huomiosta, että nauhurien läsnäolo saa haastateltavat sulkeutuneemmiksi [42]. Muistiinpanoja tehtiin jatkuvasti haastattelujen aikana ja niihin pyrittiin kirjaamaan kaikki tutkimukselle olennainen.

Yrityksen koosta riippuen haastateltavat olivat joko yrityksen korkeimmalla portaalla tai he raportoivat suoraan ylimmälle johdolle. Taulukossa 1 on listattu haastateltujen roolit ja kuinka moni toimi kussakin roolissa. Yhteen haastatteluun osallistui enemmän kuin yksi haastateltava.

Taulukko 2. *Haastateltujen tittelit*

Titteli	**Tittelin omaavien lukumäärä**
CTO	1
Tietoturvajohtaja	1
Tietoturvapäällikkö	2
Tietohallinto/ICT-johtaja	2
Tietohallinto/ICT-päällikkö	3
Kehitysjohtaja	1
Perustaja	1

Useimpien haastateltujen roolit ja asemat yrityksissä antoivat mahdollisuuden saada tietoa ajasta ennen nykyistä tietoturvapolitiikkaa, sillä useimmat olivat olleet yrityksessä ennen sen luontia ja olivat olleet vahvasti mukana nykyisen politiikan kehittämisessä. Tämän takia monilla korostui haastatteluissa yrityksen tekemät kehitysaskeleet tietoturvan saralla ja monet olivatkin ylpeitä siitä, mitä olivat saavuttaneet. Ylpeys ei kuitenkaan tuntunut vaikuttavan vastauksiin, sillä kaikki uskalsivat myös myöntää kohtaamansa haasteet ja kehityksen tarpeet.

Haastattelut etenivät sujuvasti ja kysymykset koettiin pääosin selkeiksi, ainoastaan tietoturvapolitiikan rakenteeseen liittyvä kysymys, joka esitellään seuraavissa alaluvuissa, osoittautui haastavaksi vastata. Vastauksissa lähdettiin helposti poikkeamaan kysytystä, sillä vastaamista varten haastateltavat joutuivat valottamaan yrityksen toiminnan taustoja. Haastateltavat osoittivat luottamusta haastattelutilanteissa, mikä mahdollisti kattavampien vastauksien saamisen. Koska haastattelutilanteista oli tarvittaessa tehty salassapitosopimuksia, lisäsi tämä osaltaan mahdollisuuksia kertoa yksityiskohtaisempaakin tietoa yritysten tilanteista. Nämä tiedot siistittiin jo muistiinpanojen läpikäynnin aikana, jotta mahdollisia sopimusrikkomuksia ei pääse käymään.

Haastateltuja pyydettiin kuvailemaan yritystensä tietoturvatoimintaa yleisesti ennen kuin haastattelun kysymyksiä käytiin läpi. Näin luotiin hyvä pohja keskustelulle ja avattiin myös yrityksen toimintaa ja miksi tiettyjä toimintoja tehdään. Haastattelukysymykset jaoteltiin seuraavaan kolmeen osaan teoriaosuuden perusteella: suunnittelu (development), toteuttaminen (implementation) ja seuranta (monitoring) [13]. Haastattelukysymykset on esitetty liitteessä A. Seuraavissa alaluvuissa käydään kunkin haastatteluosan kysymykset ja niiden perustelut tutkimukselle.

3.1 Suunnitteluvaiheen kysymykset

Suunnitteluvaiheen kysymykset keskittyvät erilaisiin sidosryhmiin ja toteutusvaiheen suunnitteluun. Jalkauttamisen kannalta on erityisen merkittävää tietää sidosryhmiin liittyvistä asioista.

Ensimmäisen kysymyksen, ”Perustuuko tietoturvapolitiikka johonkin olemassa olevaan pohjaan?”, avulla halutaan selvittää, millaisia pohjia, kuten standardeja, ohjeita tai kehyksiä, on käytetty suunnittelussa. Tähän on kaksi syytä. Ensinnäkin halutaan nähdä, mitkä ovat yleisimmät standardit ja ohjeet, joita seurataan. Toiseksi haluttiin kuulla, miten paljon pohjia käytetään ja yritetäänkö politiikkaa sovittaa omiin tarpeisiin vai otetaanko jokin pohja vain käyttöön, ilman sen sovittamista. Myös kuvan 3 mukaisia ulkoisia tekijöitä pyrittiin löytämään tämän kysymyksen avulla.

Toisella kysymyksellä, ”Millaisia sidosryhmiä suunnittelutyöhön otettiin mukaan?”, halutaan selvittää, miten paljon erilaisia sidosryhmiä suunnittelutyöhön otettiin mukaan. Kuten luvussa 2.2 käytiin läpi sidosryhmien merkitys tietoturvapolitiikan rakentamiselle ja sen onnistumiselle, oli tämä tärkeää saada selville haastatteluissa.

Kolmas kysymys, ”Millainen johdon tuki oli, kun tietoturvapolitiikka luontiin?”, hakee myös samaa kuin toinen kysymys, mutta sen avulla oli tarkoitus selvittää, miten aktiivisesti ja millä tavoin johto osallistui projektiin. Johto terminä jätettiin avoimeksi, jotta kuultaisiin kaikkien mahdollisten johdon jäsenten osallistumisesta eikä vain esimerkiksi tietohallinnon johtajan osallistumisesta.

Suunnitteluvaiheen viimeisellä kysymyksellä, ”Millainen prosessi tietoturvapolitiikan suunnittelussa oli?”, pyritään saamaan kuvaa koko suunnitteluprosessista, jotta voitaisiin ymmärtää, miten erilaisia sidosryhmiä hyödynnettiin, mitä aineistoja käytettiin ja millaisia prosesseja yrityksillä oli. Tämän kuvauksen pohjalta pyrittiin löytämään mahdollisia haasteita, joita yritys kohtaa tietoturvapolitiikan jalkauttamisessa.

3.2 Toteutusvaiheen kysymykset

Toteutusvaiheen kysymyksissä keskityttiin kommunikointiin ja toteutuksen käytäntöihin. Tavoitteena oli saada kuvaa käytännöistä, joita toteutukseen liittyi. Jalkauttamisen kannalta merkittävimmät olivat sisällön monimutkaisuus, viestintä ja koulutus.

Ensimmäisen kysymyksen, ”Toteutettiinko riskianalyysia tietoturvariskien varalta?”, avulla kuullaan, onko riskianalyyseja tehty. Kuten luvussa 2.2 todettiin, on riskianalyysi tietoturvatoiminnan kulmakiviä ja sen avulla tunnistetaan tarvittavat toimet. Riskianalyysi on usein suunnitteluvaiheen toimia, mutta tätä työtä varten se nähtiin osana toteutusta, koska suunnittelu keskittyi paljon valmisteluun eikä niinkään itse politiikan sisältöön, johon riskianalyysi vaikuttaa.

Toinen kysymys, ”Millainen politiikan rakenne on?”, selvittää, millaisella tavalla politiikka on rakennettu. Rakenteella on vaikutusta, miten selkeä politiikka on sen lukijoille ja tästä haettiin yhteyttä jakelun vaikeuksiin. Rakenne perustuu Lopesin ym:n [6] esittämään kolmeen yleisimpään rakenteeseen. Rakenteen merkitys voi olla valtava siihen, miten tietoturvapolitiikka nähdään. Hyvin yksilöllinen politiikka saa tietoturvan tavoitteet tuntumaan erittäin hajanaisilta ja epätarkoilta, kun taas hyvin keskitetty saa tietoturvan tavoitteet tuntumaan kaukaisilta.

Kolmannessa kysymyksessä, ”Tiedotettiinko politiikan toteuttamisesta? Jos tiedotettiin, miten paljon ja mitä kautta?” selvitetään politiikan tiedottamiseen liittyviä tietoja, jotta tiedetään, miten yritysten sisäinen viestintä on toteutettu projektin eri vaiheissa. Tiedottaminen on tärkeä osa sitouttamista, koska kun henkilöstö pidetään ajan tasalla tulevista muutoksista, he kokevat olevansa tärkeitä kehitykselle ja kokevat politiikan omakseen.

Neljännessä kysymyksessä, ”Miten politiikka jaettiin kaikille sidosryhmille? Sähköisesti, paperilla? Oliko koulutusta?” kysytään politiikan jakamisesta sidosryhmille ja siihen liittyvästä koulutuksesta. Tämän avulla halutaan selvittää, miten paljon ja millaisia koulutuksia tietoturvapolitiikasta tehtiin, kun se julkaistiin. Kuvassa 3 esitetty tietoturvapolitiikan tietoisuus ja koulutus on tärkeä osa tietoturvapolitiikan elinkaarta, sillä koulutukset ovat yksi tärkeimmistä tavoista saada tietoturvapolitiikka ymmärrettävään muotoon ja osaksi jokaisen toimintaa. Koulutukset voivat olla joko tietoturvapolitiikan läpikäyntiä tai siitä johdettujen ohjeiden kouluttamista, joista jälkimmäinen on tehokkaampi tapa saada parempia tuloksia.

3.3 Seurantavaiheen kysymykset

Viimeisessä vaiheessa, seurannassa, keskityttiin tietoturvapolitiikan noudattamiseen ja rikkomuksiin sekä politiikan kestävyyteen ja tarvittavaan päivitystyöhön. Seurantavaihe on merkittävä osa tietoturvapolitiikan muodostumista osaksi tietoturvakulttuuria. Tässä vaiheessa nähdään, miten erilaiset toimet ovat vaikuttaneet politiikan jalkautumiseen ja miten tietoturvatoimintaa voi kehittää.

Ensimmäisellä kysymyksellä, ”Miten tietoturvapolitiikan noudattamista seurataan?”, selvitetään, millaisia toimenpiteitä yritykset tekevät tietoturvapolitiikan noudattamisen seuraamiseksi tai valvomiseksi. Tämän avulla pyritään saamaan kuvaa, miten paljon seuraamista tapahtuu vai tapahtuuko ollenkaan ja millaisia prosesseja siihen liittyy. Noudattamisen seuraaminen voi olla ratkaiseva tekijä tietoturvapolitiikan onnistumisessa organisaatiossa, joissa henkilöstöllä on matala tietoturvallisuuden taitotaso tai yrityskulttuuri ei tue tietoturvaa jo ennestään.

Toinen kysymys, ”Onko tiedossa, että politiikkaa olisi rikottu? Jos on, miten kuvailisit rikkomusten vakavuutta ja määrää?”, on hyvin suoraviivainen. Rikkomusten vakavuus ja

määrä kertoo paljon, miten tietoturvapolitiikka on onnistuttu jalkauttamaan yrityksiin. Jos rikkomuksia tapahtuu paljon, tarkoittaa se, että politiikka ei ole sopiva yritykselle tai sitä ei ole onnistuttu kouluttamaan kunnolla, jolloin sisäistys jää heikoksi. Kuitenkin, jos rikkomuksia on tapahtunut vain vähän, voi se tarkoittaa myös, että seurantaa ei tapahdu riittävästi tai seurataan vääriä asioita eikä oikeat tapaukset nouse esille.

Kolmannella kysymyksellä, ”Mitä toimia tehdään, että yrityksen henkilö voi kokea politiikan omakseen?”, selvitetään osallistamiseen liittyviä toimia. Kuten luvussa 2.3 todettiin, on paljon erilaisia toimintaedellytyksiä, jotta tietoturvapolitiikka olisi onnistunut. Kysymyksellä pyrittiin myös selvittämään, miten ihmiskeskeistä yrityksen toiminta on. Jos paljastuu, että toimia tehdään vähän, voi siinä olla syy, miksi tietoturvapolitiikka ei yrityksessä ole onnistunut.

Neljäs kysymys, ”Miten paljon aikaa politiikan ylläpitoon käytetään vuosittain (htp)?”, on selvä mittari työmäärän suhteessa saatuun tuotokseen. Jos politiikan ylläpitoon käytetään paljon aikaa eikä se silti tuota tuloksia, voi hyvin olla, etteivät päivitystoimet keskity oikeisiin asioihin. Jos politiikka ei ole päivitetty ja on huomattu, että yrityksessä tapahtuu paljon tietoturvarikkomuksia, on se selkeä merkki, että politiikkaa tulisi päivittää.

Viimeisellä kysymyksellä, ”Miten kauan nykyisen politiikan uskotaan kestävän?”, pyritään selvittämään, millaisia haasteita nähdään tulevaisuudessa, jotka voivat vaikuttaa tietoturvapolitiikan kestävyyteen. Tässä haastateltuja rohkaistiin miettimään asiaa joko hyvin faktapohjaisesti tai filosofisesti, eli pohtimaan asiaa myös perinteisten uhkakuvien ulkopuolelta. Näin pyrittiin löytämään erilaisia ajatuksia mahdollisista voimista, jotka vaikuttavat politiikan ajantasaisuuteen.

4. TULOKSET JA TARKASTELU

Luvussa käydään läpi, miten tutkittujen yritysten tietoturvapolitiikat vaikuttavat tietoturvakulttuurin syntymiseen ja millaisia kehitystarpeita nousee esiin. Tulosten tarkastelu on jaettu haastattelun mukaisesti yleisiin, suunnitteluvaiheen, toteutusvaiheen ja seurantavaiheen havaintoihin ja lopuksi niistä kerätään kehitystarpeet ja annetaan mahdollisia lähestymistapoja niiden kehittämiseen. Tulosten tarkastelua lähestytään luvun 2.5 mittareiden pohjalta.

4.1 Yleiset havainnot

Kaikissa tutkituissa yrityksissä tietoturva oli otettu huomioon ja se tunnistettiin toimintaedellytykseksi nykyaikaisessa liiketoiminnassa. Tietoturvapolitiikka oli kaikissa yrityksissä otettu käyttöön johtamisen tueksi ja sillä perusteltiin, miksi tiettyjä tietoturvaprosesseja noudatetaan. Luvussa 2 on pyritty tuomaan esiin, miten kokonaisvaltainen tietoturvapolitiikka on koko yrityksen tietoturvallisuuden kiteyttämisessä. Johtuen sen monimutkaisuudesta, haastateltujen yritysten lähestyminen politiikan tehokkaaseen käyttöön vaihteli suuresti. Tähän palataan yksityiskohtaisemmin eri osien havainnoissa.

Yritysten koot ja toimialat vaikuttivat hyvin oletetulla tavalla. Tietoturvallisen toiminnan taso riippui yrityksen koosta: mitä suurempi yritys, sitä korkeampi tietoturvallisuuden kypsyystaso. Mutta tähänkin oli poikkeuksia, kuten yksi keskikokoinen yritys, jonka tietoturvallisuuden taso oli korkeammalla kuin useimmilla tutkituilla yrityksillä ja jossa tietoturvallisuuteen oli panostettu huomattavasti. Tämän yrityksen toimiala vaati kuitenkin erityisten toimenpiteiden noudattamista, koska yrityksen toimialalla vaadittiin tiukkojen sääntöjen ja lakien noudattamista. Jos toimialalla ei ollut selkeitä tietoturvavaatimuksia lakien tai muiden asetusten kautta, ei toimiala vaikuttanut tietoturvallisuuden tasoon. Kaikilla aloilla oli keskimäärin hyvin yleiset vaatimukset tietoturvallisuudelle ja kaikki pyrkivät noudattamaan hyviä tietoturvallisuuden toimintatapoja.

Euroopan tietosuoja-asetuksella, joka astui vuoden 2018 toukokuussa voimaan, oli huomattava vaikutus yritysten tietoturvan kehitykseen ja tietoturvaan liittyvän kiinnostuksen kasvuun. Monet yritykset olivat uusineet tietosuojaan liittyvän työn yhteydessä tietoturvapolitiikkaansa ja -toimintojansa. Osassa yrityksistä tietosuoja-asiat ovat menneet tietoturvallisuuden edelle, mikä ei ole haluttua. Tietoturvallisuuden avulla voi toteuttaa tietosuojaa, joten tietosuojan onnistuminen vaatii, että tietoturvallisuus on yhtä lailla korostettuna. Lisäksi monet yritykset olivat päivittäneet tietoturvapolitiikkansa

parin viime vuoden aikana, sillä haastateltujen yritysten tietoturvapolitiikkojen keski-ikä oli noin 1,5 vuotta.

Moni tutkituista yrityksistä oli havainnut ihmisten merkityksen tietoturvan toteuttamisessa. Nähtiin, että “tietoturva lähtee henkilöstöstä” ja politiikkaa oli pyritty useassa tapauksessa yksinkertaistamaan, jotta se olisi helpommin ymmärrettävissä. Tiedetään, että ihmiset ovat syynä monille riskeille ja tähän on haluttu vaikuttaa. Ihmisten tärkeydestä puhuttiin luvussa 2.3 ja sen alaluvuissa. Henkilöstö on kuitenkin loppujen lopuksi se, joka toteuttaa tietoturvallisuutta käytännössä. Osa haastateltavista antoi kattavasti esimerkkejä, miten henkilöstöä kuultiin. Esimerkiksi yhdessä yrityksessä annettiin mahdollisuus kysyä johdolta kysymyksiä koko yhtiön henkilöstötapaamisissa. Osa haastateltavista tunnisti, että tässä on vielä kehitettävää ja tahtotila oli lisätä mahdollisuuksia henkilöstölle tulla kuulluksi.

4.2 Havainnot suunnitteluvaiheesta

Suunnitteluvaiheen kysymyksissä keskityttiin suunnitteluprosessiin ja erilaisiin sidosryhmiin, jotka vaikuttavat tietoturvapolitiikan toteutukseen. Vastauksissa tuli esiin erilaisia näkökulmia, miten tietoturvapolitiikkaa suunnitellaan ja millaisia sidosryhmiä otetaan mukaan. Jokaisella tutkitulla yrityksellä oli erilaiset tarpeet ja näiden takia myös erilaiset lähestymistavat sen suunnitteluun.

Yksi yleisimmistä yhtäläisyyksistä oli, että suunnittelussa käytettiin tukena ulkopuolista konsulttia. Kuusi kymmenestä haastateltavasta käytti ulkoista konsulttia, joka joko tuki suunnittelua tai teki jopa koko yrityksen nykytilan selvityksen, jonka pohjalta kehitettiin tietoturvapolitiikan toteutusprojektin vaiheet. Ulkopuolisen asiantuntijan avulla yrityksen osaamista voi laajentaa tehokkaasti muuttuvien tarpeiden mukaan. Ulkopuolinen taho tuo yritykseen myös mukanaan uudenlaisen näkökulman, joka voi auttaa yritystä tunnistamaan omat kuolleet kulmansa. Konsulttien käytöllä voi olla kuitenkin haasteensa. Heidän palvelunsa voivat olla lyhytaikaisia, minkä jälkeen heidän tuomastaan opista ja ymmärryksestä ei välttämättä jää yritykselle juuri mitään.

Puolella tutkituista yrityksistä tarve lähteä kehittämään tietoturvaa, ja määritellä tietoturvapolitiikka tämän yhteydessä, tuli ulkoisesta tarpeesta, kuten asiakasvaatimuksesta. Lopuilla tarve oli syntynyt sisäisesti, jolloin joko yrityksen tietohallinto oli huomannut tarpeen tietoturvan kehittämiselle tai yrityksen johto oli halunnut, että tietoturvaa kehitetään. Ulkoisesta tarpeesta syntynyt vaatimus voi olla haastava muuttaa yritykselle sopivaksi määritykseksi. Kun tarve ei synny sisäisesti, paine muuttaa ulkoisen toimijan, esimerkiksi asiakkaan, asettamat vaatimukset organisaatiolle sopiviksi tavoiksi voi törmätä organisaatioiden toimintatapojen kanssa. Tällöin tulee olla erittäin tarkka, kun vaatimuksia muutetaan yritykselle sopiviksi.

Yrityksen johdon tuki on yksi tärkeimmistä kriteereistä tietoturvapolitiikan onnistumisessa, kuten luvussa 2.3 mainittiin. Puolella tutkituista yrityksistä oli johdon suora tuki tai johdolta tullut pyyntö kehittää tietoturvaa. Kaikissa tapauksissa johto oli kuitenkin nähnyt luodut politiikat ja ohjeistukset ja hyväksyneet ne. Johdon hyväksymä politiikka on jo itsessään hyvä merkki johdon tuesta. Tukea voi osoittaa enemmän, kun politiikkaa ruvetaan jalkauttamaan. Tätä ei vastauksissa tullut juurikaan esille.

Muita sidosryhmiä, joita haastateltiin tai otettiin mukaan suunnitteluprojektiin, olivat IT tai tietohallinto, henkilöstöhallinto, lakiosasto, ulkoiset sidosryhmät, kuten konsultit ja asiakkaat, ja muut liiketoimintayksiköt. Taulukossa 3 on listattu huomioidut sidosryhmät ja kuinka monissa haastatteluissa mainittiin niiden huomioiminen.

Taulukko 3. *Huomioidut sidosryhmät tietoturvapolitiikan suunnittelussa*

Sidosryhmä	**Huomioitu suunnittelussa (lukumäärä)**
IT ja tietohallinto	6
Johto	3
Henkilöstöhallinto	2
Lakiosasto	2
Muut liiketoiminnot	5
Ulkoiset sidosryhmät (konsultit, asiakkaat)	4

Yleisin huomioitu sidosryhmä oli IT- tai tietohallinto-osasto, joka oli usein myös tietoturvapolitiikan luonnin tai päivittämisen toimeenpanija. Toiseksi yleisin sidosryhmä oli muut liiketoiminnot, kuten ydinliiketoiminnan yksiköt. Muut liiketoiminnot vaihtelivat paljon yritysten tarpeiden välillä ja siksi niitä ei ole listattu taulukkoon erikseen. Ulkoiset sidosryhmät olivat seuraavaksi tavallisin sidosryhmä, mutta kaikkia ulkoisia konsultteja ei koettu haastatteluissa ulkoisiksi sidosryhmiksi. Haastateltavilla oli hyvin erilaisia sidosryhmiä, mutta monet haastateltavat tuntuivat keränneen vain muutamilta mahdollisilta sidosryhmiltä tietoa. Keskimäärin haastateltiin kahta tai kolmea eri sidosryhmää, mutta muutamassa tapauksessa ei haastateltu ollenkaan sidosryhmiä. Tämä tekee työstä erittäin sulkeutunutta ja tukeutuu täysin politiikkaa toteuttavan ryhmän tai henkilön tietoon eri sidosryhmien tarpeista. Tällöin on suuri riski, että luotu politiikka ei vastaa organisaation tarpeisiin ja politiikasta tulee vain yksi dokumentti muiden joukossa, jolla on vain näennäinen merkitys.

Suunnittelun prosessit olivat kaikki hyvin erilaisia: osa prosesseista oli lähes pakon edessä tehtyjä “ponnistuksia” saada tietoturva dokumentoitua ja osa tarkasti suunniteltuja

prosesseja, joissa tietoturvalla on selkeä tavoite yrityksen liiketoiminnassa. Näissä heijastui yrityksen johdon tuki – jos tukea oli annettu, oli prosessin suunnitteluun käytetty enemmän aikaa. Tietoturvapolitiikan suunnitteluprosessia käytettiin myös puhdistusprosessina eli kerättiin kertyneitä ohjeistuksia ja määräyksiä, jotka käytiin läpi ja tarpeettomat määräykset poistettiin käytöstä. Osittain prosessin kuvaus kertoo, millainen tietoturvallisuuden tarve yrityksellä on. Osassa yrityksistä oli huomattu tietoturvallisuuden merkitys ja siksi sen suunnitteluun ja kehittämiseen oli paneuduttu syvällisemmin.

4.3 Havainnot toteutusvaiheesta

Toteutusvaiheessa tarkasteltiin, millaisia lähestymistapoja tietoturvapolitiikan toteutukselle oli ja erityisesti keskityttiin, miten toteutuksesta kommunikoitiin sidosryhmille. Kaksi suurinta havaintoa tästä oli, että tietoturvaa lähestyttiin lähes aina riskienhallinnan kautta (yhdeksän kymmenestä haastattelusta) ja tietoturvapolitiikasta tiedotettiin aina sähköisiä kanavia pitkin.

Riskienhallinta on yksi tärkeimmistä osista tietoturvapolitiikan ja tietoturvan suunnittelua yleisesti ja tämä näkyi hyvin myös tutkituissa yrityksissä. Kaksi tutkittua yritystä lähestyi tietoturvaa täysin riskienhallinnan kautta ja tietoturvapolitiikka nähtiin yhdessä yrityksessä osana riskienhallintapolitiikkaa. Tästä voi nähdä, että tietoturvaa on lähestytty hyvin taloudellisesta näkökulmasta ja tämä on teoriaosuuden perusteella tehokkain tapa lähestyä tietoturvan suunnittelua. Riskienhallinnan avulla tunnistetaan suojattavat kohteet ja luodaan niille sopivat suojausmekanismit. Yritysten riskienhallintaprosessiin ei paneuduttu syvällisemmin, mutta yleisintä oli, että yritykset käyttivät ulkoisia asiantuntijoita eri osa-alueiden riskien tunnistamiseen ja arviointiin.

Jokaista vaihtoehtoina ollutta rakennetta oli käytetty jossain tutkituista yrityksistä. Puolet käyttivät modulaarista rakennetta, eli politiikka oli yksi päädokumentti ja sillä oli tukevia dokumentteja. Neljällä kymmenestä oli kokonainen politiikka, eli politiikalla katettiin kaikki toiminnot. Yhdellä yrityksistä oli useilla eri toiminnoilla omat politiikkansa, eli politiikalla oli yksilöllinen rakenne, muttei kuitenkaan kaikilla, joten se voitaisiin laskea myös osaksi modulaarisesti rakennettuja politiikkoja. Kaikissa haastatteluissa ei annettu pääsyä tietoturvapolitiikkadokumentteihin, joten seikkaperäistä analyysia rakenteesta ei päästy tekemään ja työssä on luotettu haastateltujen antamiin arvioihin politiikan rakenteesta. Tämän perusteella voi kuitenkin sanoa, että moni on pyrkinyt rakenteeseen, jossa vain olennaisia dokumentteja tarvitsee päivittää, jos määräyksiin tulee muutoksia. Tämä on ylläpidon kannalta tehokkainta, kun läpikäyntiä ja hyväksyntää varten tarvitsee käydä vain spesifejä dokumentteja läpi eikä koko tietoturvapolitiikkaa.

Tietoturvapolitiikan toteutuksesta tiedotettiin suoraan henkilöstölle kahdeksassa yrityksessä, yhdessä tiedotettiin liiketoimintayksiköiden päälliköille ja yhdessä toteutuksesta ei tiedotettu lainkaan. Viimeiseksi mainitussa yrityksessä koettiin, että

tiedottamisesta ei ole hyötyä, koska informaatiota tulee jo niin paljon. Vaikka tiedottaminen projektin alkamisesta ja etenemisestä koetaan ylimääräiseksi tiedoksi, sen avulla voi osallistaa henkilöstöä mukaan prosessiin. Tiedottaminen mahdollistaa keskustelun tulevista muutoksista, jolloin organisaation toiminta koetaan läpinäkyvämmäksi. Tällöin henkilöstö kokee, että he ovat vaikuttaneet toimintaan ja ovat valmiimpia hyväksymään tulevat muutokset. Myös aikaisessa vaiheessa kommentointi voi estää mahdollisten ongelmien syntymisen myöhemmässä vaiheessa.

Politiikan valmistuessa tiedottaminen tapahtui jokaisessa yrityksessä sähköisesti joko sähköpostitse, intrassa tai molemmissa. Kahdessa yrityksessä järjestettiin sisäinen tiedotustilaisuus tai politiikasta kerrottiin henkilöstötapaamisissa. Koulutuksia järjestettiin kuudessa organisaatiossa, mutta yhdessä niistä koulutusta ei edellytetty. Yritysten toteutus koulutuksista vaihteli huomattavasti. Osa järjesti perinteisiä luentotilaisuuksia politiikasta, osa käytti verkkopohjaisia oppimisalustoja. Kahdessa yrityksessä GDPR-koulutukset olivat päärooolissa, sillä tietosuoja oli koettu tärkeämmäksi ymmärtää normaalissa päivätyössä. Kaikissa vastauksissa ei tullut selkeästi esille, kuinka usein koulutuksia järjestettiin. Osassa haastatteluista kuitenkin todettiin, että koulutus pidettiin vain kerran tietoturvapolitiikkaprojektin lopussa eikä myöhemmin pidetty minkäänlaisia kertauskoulutuksia.

4.4 Havainnot seurantavaiheesta

Seurantavaiheessa keskityttiin toimiin, joilla seurataan politiikan noudattamista organisaatioissa ja millaisia ja kuinka paljon erilaisia tapauksia oli havaittu. Myös jatkokehitykseen liittyviä toimia kysyttiin. Näin pyrittiin saamaan kuva, miten onnistuneita tietoturvapolitiikat olivat tietoturvakulttuurin synnyttämisessä ja miten ne tukivat tietoturvatoimintoja. Tietoturvapolitiikan kestävyyden kysymisellä pyrittiin selvittämään, onko tietoturvapolitiikan funktio tietoturvatoimintojen pohjana ymmärretty oikein eikä sitä käytetä pelkkänä ohjeena.

Politiikan toteutumista yrityksissä seurattiin neljässä yrityksessä koulutusten kautta. Seurattiin, kuinka moni oli käynyt koulutuksen verkossa tai käynyt koulutustilaisuudessa. Myös tietoturvapoikkeamia seurataan ja näillä pystytään näkemään, miten tietoturvaohjeet ovat sisäistetty. Pistemäinen seuranta ja auditoinnit olivat yleisin tapa tarkastaa tietoturvapolitiikan toimivuutta. Puolet haastatteluista käytti joko ulkoista tai sisäistä auditoijaa tarkastuksen tekemiseen. Jatkuva seuranta oli muutamassa tapauksessa täysin tietoturvallisuudesta valveutuneiden varassa, jotka pyrkivät muistuttamaan muita hyvistä käytännöistä, kuten laitteiden lukitsemista niiden ollessa käyttämättöminä.

Seitsemässä yrityksessä oli havaittu tahattomia rikkomuksia ja joitain tahattomia tietosuojarikkeitä. Tahallisia tapauksia oli tunnistettu vain yhdessä haastattelussa. Kahdessa yrityksessä todettiin suoraan seurannan olevan vähäistä, koska uskottiin, että

työntekijöihin voi luottaa ja näin ollen he noudattavat tietoturvapolitiikkaa. Kolmessa haastattelussa todettiin, että ei ollut tunnistettu tahattomia tai tahallisia tapauksia.

Kun organisaatioissa ei havaita rikkomuksia ja todetaan, että seuranta on pistemäistä, on hyvin mahdollista, että rikkomuksia on tapahtunut, mutta niistä ei ole jäänyt merkintöjä. Pienien rikkomusten merkitys voi olla mitätön, mutta tämä voi kieliä mahdollisuuksista, että suurempia rikkomuksia voi päästä tapahtumaan. Osaa rikkomuksista voi valvoa ja havaita teknisillä ratkaisuilla, kuten verkon ja laitteiden valvonnalla, mihin yhdessä yrityksessä oli panostettu huomattavasti resursseja. Tässä on hyvä peilata organisaation tarvittavia toimintoja organisaation riskienhallintaan, kun pohditaan, miten paljon resursseja valvontaan halutaan panostaa.

Kaikissa tutkituissa yrityksissä haluttiin tehdä mahdolliseksi tietoturvapolitiikkaan ja tietoturvatoimiin vaikuttaminen, joko antamalla ehdotuksia toimintatapojen muuttamisesta tai itsearvioita keräämällä ja niistä keskustelemalla. Myös vallitsevalla tietoturvakulttuurilla on ollut merkitystä tietoturvatoimintojen kehittämiseen. Tietoturvapolitiikkaan liittyvien muutosten jälkeen ainakin yhden tutkitun yrityksen henkilöstö on aktivoitunut uudella tavalla tietoturvaan ja he ovat alkaneet antamaan palautetta yrityksensä toiminnoista. Muutamissa haastatteluissa otettiin esiin, että tietoturvallisuus ei kiinnosta monia. Vaikka yrityksessä olisi avoin ja keskusteleva kulttuuri, on mahdollista, että tämä kiinnostuksen puute johtaa vähäiseen osallistumiseen ja täten kehitysideoita jää kuulematta.

Asioiden arkipäiväistäminen ja ohjeiden yksinkertaistaminen on ollut monessa yrityksessä hyväksi havaittu keino saada politiikka ymmärrettävämmäksi ja paremmin integroiduksi osaksi jokapäiväistä toimintaa. Vain tärkeimmät asiat ovat tuotu ohjeissa esiin, jotta ihmisiä ei kuormitettaisi liikaa. Itse politiikkadokumentti on voinut tällöin olla hyvin tekninen kieleltään, kun siitä johdetut ohjeet ovat olleet helposti ymmärrettäviä.

Politiikan päivittämiseen käytettiin vaihtelevasti aikaa. Seitsemän kymmenestä yrityksestä totesi päivittävänsä politiikkansa vuosittain, mutta työmääriin ei saatu kaikilta suoraa vastausta. Määrät vaihtelivat 1-20 henkilötyöpäivään, sillä tarve päivittää politiikkaa vaihteli vuosittain. Jalkauttamiseen käytettiin enemmän aikaa: ohjeita ja muita käytäntöönpanotehtäviä tehtiin kasvavissa määrin. Kahdessa yrityksessä tietoturvapolitiikan päivitys oli osa jatkuvaa kehitystä, eikä sitä päivitetty pistemäisesti kerran vuodessa. Käytetty aika peilasi vahvasti, miten politiikkaa käytettiin. Jos politiikka toimi vain pohjana muille ohjeille, sitä päivitettiin vähemmän. Jos politiikka sisälsi ohjeita ja sen tarkoitus oli olla ohjaamassa jokapäiväistä työtä, sen päivittämiseen käytettiin enemmän aikaa.

Politiikka nähtiin useimmiten hyvin aikaa kestävänä eikä sen ylläpitäminen vaatinut paljoa aikaa vuosittain. Jos politiikka ei ollut jo valmiiksi vanha, sen uskottiin kestävän useimmiten 3-5 vuotta. Tämä olettamus perustui politiikan rakenteeseen. Politiikan

uskottiin kestävän pidempään, kun sillä kuvataan yrityksen tietoturvan tavoitteet ja määritellään teknologiasta riippumattomia linjauksia eikä puututa käytännön toteutuksiin. Suurimpina uhkina politiikan kestämättömyydelle nähtiin suuret muutokset teknologiassa, yhteiskunnassa tai yrityksen toiminnassa. Jos jokin näistä muuttui odottamattomasti tai nopeasti, uskottiin politiikan tarvitsevan suuria korjaustoimenpiteitä.

4.5 Kehitystarpeet ja ratkaisuehdotukset

Suurimmat tunnistetut haasteet tietoturvapolitiikan ja sen tehokkuudessa tietoturvakulttuurin luonnissa liittyivät politiikan jalkauttamiseen. Haasteet vaikuttavat käytäntöjen muodostumiseen joko suorasti tai epäsuorasti. Vaikka monet yritykset pitivät koulutuksia ja laativat ohjeita, monissa yrityksissä oli parannettavaa politiikan muuntamisessa toiminnoiksi. Useassa haastattelussa vaikutti, että tietoturvapolitiikka nähtiin vain ohjeena, jota piti seurata eikä nähty sen täyttä potentiaalia johtamisen työkaluna.

Kehityskohteet ovat haastattelun mukaisessa järjestyksessä: ensiksi suunnittelusta nousseet kehityskohteet, sitten toteutuksesta nousseet ja lopuksi seurannasta nousseet. Kohteet perustuvat haastatteluhavainnoista löytyneisiin yleisiin kipukohtiin. Suunnittelu- ja toteutusvaiheen havainnot nousivat analyysista, mutta seurantavaiheen kehitystarpeen moni haastateltavista oli tunnistanut myös itse. Tämä ei tarkoita, että jokaisessa yrityksessä olisi tarvetta kehittää kaikkia löydettyjä kohteita, mutta niitä voi käyttää myös pohdinnan pohjana.

4.5.1 Suunnitteluvaiheen ratkaisuehdotukset

Suunnittelussa oli usein käytetty rajallisesti erilaisia sidosryhmiä. Monissa tapauksissa tietoturvapolitiikka oli tietohallinnon tai ICT-osaston yksinään toteuttama projekti, johon kuultiin vain pakollisia sidosryhmiä, kuten lakiosastoa tai henkilöstöhallintoa. Tämä rajoittaa paljon, miten kattavia tietoturvapolitiikasta ja siitä johdetuista tietoturvaohjeista tulee. Erityisen tärkeätä olisi ottaa eri liiketoimintayksiköiden edustajia mukaan politiikan suunnitteluun, koska he ovat loppujen lopuksi henkilöitä, jotka ovat vahvasti mukana jalkauttamassa politiikkaa.

Liiketoimintayksiköiden määrä ja tärkeys tietoturvapolitiikalle vaihtelee organisaatioittain. Parasta olisi, jos jokaista erilaista liiketoimintayksikköä saataisiin edustamaan edes yksi henkilö, joka tuntisi oman liiketoimintayksikkönsä ja liiketoimintayksikön tarpeet. Tämä auttaa monessakin tietoturvapolitiikkaan olennaisesti liittyvässä osassa. Ensinnäkin tämä tekee tietoturvapolitiikan suunnittelusta kattavampaa, kun ymmärretään kaikkia yrityksen prosesseja paremmin. Toiseksi se auttaa sitouttamaan

henkilöstöä paremmin politiikkaan, kun henkilöstö kokee tulleensa kuulluksi. Näin lopulta tietoturvapolitiikan jalkautuminen onnistuu myös paremmin, kun suunnitteluilla toiminnoilla ja määräyksillä on ymmärrettävät tavoitteet.

Teoriaosuudessa moni lähde tukee tätä ajattelua. Osallistaminen, josta puhuttiin luvussa 2.4.4, on tehokkaaksi todettu tapa saada tietoturvapolitiikan noudattamista parannettua. Yhteisymmärryksessä suunniteltu ja toteutettu politiikka on helpommin hyväksyttävä ja siten myös paremmin omaksuttava kokonaisuus. Mitä enemmän sidosryhmiä otetaan mukaan politiikan kehittämiseen, sitä paremmin saa erilaista kokemusta ja tietoa kerättyä ja näin politiikasta saadaan sisällöllisesti laadukkaampi. Haasteeksi voi osoittautua ryhmien tehokas kuuleminen ilman, että niiden välille syntyy konflikteja. Ryhmillä voi olla hyvin erilaiset tarpeet ja tämän takia ne voivat olla ristiriidassa keskenään, jolloin niiden yhteensovittaminen voi osoittautua vaikeaksi.

Toinen mahdollisesti huomionarvoinen sidosryhmä muodostuu ulkoisista edustajista. Moni yritys oli käyttänyt ulkoisia konsultteja politiikan toteutuksessa, mutta he eivät välttämättä ole suoraan liiketoimintaan vaikuttavia ulkoisia edustajia. Jos yrityksellä on esimerkiksi alihankkijoita, jotka ovat vahvasti mukana liiketoiminnassa, tulisi heidän edustajiaan myös kuulla, koska alihankkijat joutuvat usein myös noudattamaan tietoturvapolitiikkaa ja sen ohjeita. Huomioimalla ulkoisia edustajia voi välttää myöhemmin ongelmia yhteistyön kannalta.

Ulkoisten toimijoiden kuuleminen voi olla työlästä, koska sopivien henkilöiden löytäminen on haastavaa. Ulkoiset edustajat voivat joko vaihtua paljon tai heihin vaikuttaa vain pieni osa tietoturvapolitiikasta. Heiltä tulisi kuitenkin kuulla mielipide tietoturvapolitiikan tilasta tai tietoturvaohjeistuksista, jotka koskettavat heitä. Näin voi hyödyntää kaiken saatavilla olevan tiedon. Haastattelut ja kyselylomakkeet voivat olla tehokas tapa kerätä tietoa ulkoisilta sidosryhmiltä. Näin tiedonkeruu tehdään kerralla eikä kummankaan osapuolen aikaa käytetä tähän liikaa. Tiedonkeruun syvällisyys riippuu tietenkin ulkoisesta sidosryhmästä. Jos ryhmä on hyvin vahvasti liiketoiminnassa mukana, tulisi heidät osallistua tietoturvapolitiikan suunnitteluun yhtä lailla kuin sisäisetkin sidosryhmät.

4.5.2 Toteutusvaiheen ratkaisuehdotukset

Toteutus-osiosta nousi haasteena koulutusten järjestäminen. Vain kuusi kymmenestä tutkitusta yrityksestä järjesti koulutuksen. Yrityksissä, joissa koulutusta järjestettiin, vaikeinta oli koulutusten opetusmuoto. Koulutukset ovat helposti vain luentoja, joissa materiaali käydään läpi ja anti kuuntelijoille jää vähäiseksi, jolloin opetettu ei muutu tavoiksi [35]. Jos politiikka halutaan saada paremmin sisäistetyksi, tulee opetusmenetelmien olla aktivoivampia. Tämän lisäksi useassa tapauksessa seuranta perustui koulutusten käymiseen, joka oli usein vain yksi koulutustapahtuma.

Aktivointi voi tapahtua monella tavalla: testit ja kyselyt, joissa opiskelija voi mitata omaa taitotasoaan ja ymmärrystään ovat perinteisesti hyväksi havaittu keino aktivoida opiskelijaa. Erilaiset harjoitteet, jotka herättävät ajattelua ja antavat mahdollisuuden testata opiskelijaa ovat myös tehokkaita aktivointikeinoja [35]. Toimintatapojen muuttamiseen tarvitaan kuitenkin enemmän aikaa, koska ihmisillä on usein vakiintuneita tapoja ja niistä on vaikea luopua. Tämän takia muutoksen aikaansaaminen on pitkä prosessi eikä voi tapahtua yhdellä koulutuksella.

Karttunut kokemus vaikuttaa huomattavasti aikuisten oppimiseen. Osa organisaation henkilöstöstä voi olla kokeneempia tietoturvassa ja osa hyvinkin perustasolla. Tätä varten tulisi suunnitella eritasoisille oppijoille omat koulutussisällöt. Näin aiheen saa pidettyä mielenkiintoisena ja osallistujat motivoituneina, mikä parantaa oppimista. Tätä varten pitää kerätä tietoutta ihmisten taitotasosta ja antaa heille myös mahdollisuus vaikuttaa koulutusten sisältöön. Ihminen on paljon valmiimpi hyväksymään muutoksia, jos hän on päässyt vaikuttamaan siihen.

Näihin molempiin koulutuksellisiin haasteisiin ehdotetaan ratkaisuna verkkopohjaisia oppimisalustoja, jotka mahdollistavat erilaisten harjoitteiden, testien ja muiden aktiivisten oppimismenetelmien toteuttamisen. Moni haastateltu yritys oli jo ottanut tai oli ottamassa tällaisia alustoja käyttöönsä. Työkalujen lisäksi tulee keskittyä paljon koulutusten sisältöön ja kehittää niitä jatkuvasti eteenpäin, jotta ne pysyvät ajantasaisina ja mielenkiintoisina.

Verkkopohjaisten koulutusjärjestelmien etuna ovat niiden paikka- ja aikariippumattomuus, mahdollisuus tuottaa eritasoisille oppijoille omanlaiset koulutukset, mahdollisuus tuottaa virallisia koulutuksia, koulutuksista on mahdollista saada nopeasti palautetta ja opiskelija voi itse arvioida omaa suoritustaan [43]. Haasteina voivat olla motivaation ylläpito, vaikeus saada vastauksia kysymyksiin tehtäviin liittyen, vaikea olla vuorovaikutuksessa opettajan ja muiden opiskelijoiden kanssa ja vaikea keskittyä miettimiseen ja oppimiseen [43]. Yritysympäristössä aika- ja paikkariippumattomuus on suuri etu, sillä suuremmissa organisaatioissa voi olla todella vaikeata löytää kaikille sopivia aikoja yhteisille koulutuksille. Jos opiskelija itse voi valita ajan, milloin käydä koulutuksia läpi, on se parempi sekä oppijalle että organisaatiolle. Haasteisiin voi olla helpompi vastata yritysympäristössä, jos oletetaan, että koulutuksia tehdään työajalla. Tällöin on mahdollista saada helpommin apua ongelmiin ja opiskelijat voivat itse järjestää sopivia opintoryhmiä, jos he kokevat oppivansa näin paremmin. Alustan tuottama joustavuus voi vastata täten parhaiten kaikenlaisten oppijoiden tarpeisiin. Suurimmaksi haasteeksi jää koulutusten tuottaminen, niin että ne ovat sisällöltään hyödyllisiä, mielenkiintoisia ja ajantasaisia. Tämä vaatii paljon resursseja ja voi osoittautua pienemmissä organisaatioissa haastavaksi. Nykyään on paljon yrityksiä, jotka tarjoavat palveluna koulutusmateriaaleja ja niiden suunnittelua, joka voi olla toimiva ratkaisu, jos sisäisiä resursseja ei ole.

4.5.3 Seurantavaiheen ratkaisuehdotukset

Seuranta-osiosta suurimmaksi haasteeksi nousi politiikan noudattamisen seuranta ja yleisesti tietoturvatoiminnan seuranta. Moni yritys harrasti teknistä valvontaa, jotta laitteilla ja ohjelmistoilla tapahtuneet vahingot olisivat seurattavissa, mutta ihmisistä riippuvaisten toimintojen seuraaminen ja mittaaminen oli useassa tapauksessa puutteellista. Kolme haastateltavaa totesi, etteivät ole havainneet tahattomia tai tahallisia rikkomuksia. Myös moni muu haastateltu totesi, että seuraamisessa on kehitettävää. Toisaalta moni totesi myös, että mittaaminen on erittäin vaikeata, ellei jopa mahdotonta. Tästä syystä voisi olla hyvä miettiä toisenlaista lähestymiskulmaa.

Ongelmia tai virheitä ei pitäisi rangaistuksen pelossa ruveta piilottelemaan vaan niitä pitäisi voida tuoda rohkeasti esiin. Tätä varten ilmoittamisesta pitäisi tehdä mahdollisimman helppoa ja nopeaa, jotta ongelmista ilmoittaminen ei kompastuisi monimutkaisiin prosesseihin. Tämän lisäksi olisi hyvä ruveta “juhlistamaan” virheitä eli virheet nähtäisiin oppimistapahtumina ja tätä kautta saataisiin ne positiiviseen valoon. Näin ongelmia tuotaisiin enemmän esiin, koska niihin ei enää rinnastettaisi negatiivisia tunteita. Tämä ajatus nousi esiin asiantuntijahaastattelussa [44], joka toteutettiin tutkimuksen aikana. Asiantuntijahaastattelussa kysyttiin, miten tietoturvapolitiikkaa tulisi rakentaa ja millainen tietoturvapolitiikan rooli on yrityksessä. Noudattamisen seurannasta kysyttäessä nousi huomio, että rangaistuksen pelossa ihmiset rupeavat peittelemään virheitään ja siksi virheiden kautta esiin nousseet ongelmat ovat juhlimisen arvoisia, koska toiminta voi kehittyä tätä kautta.

Ongelmien tai virheiden käyttäminen oppimisessa ei ole juurikaan tutkittu tietoturvallisuuden kontekstissa, mutta esimerkiksi terveydenhuollossa, joka on erittäin haastava ympäristö ja sisältää suuria riskejä, tästä on keskusteltu. Bleich [45] kirjoittaa tästä artikkelissaan, miten tärkeää hyvän johtamisen kannalta on nähdä virheet oppimistilaisuuksina. Hän puhuu miten vakavistakin virheistä, kuten potilaan kuolemasta, tulisi pyrkiä löytämään juurisyy tapahtuneelle ja oppia tämän kautta muuttamaan toimintojaan. Vaikka tietoturvallisuudessa virheet eivät johda kuolemaan, tulisi tätä tapaa hyödyntää myös siellä. Virheiden kautta voi oppia suunnattomasti ja löytää tehottomia tai toiminnalle vaarallisia toimintatapoja. Jos henkilö kokee, että virheestä aiheutuu ainoastaan rangaistuksia ja haittaa yksilölle, on todennäköistä, että virhe jää piiloon ja nousee esiin vasta, kun siitä seuraa jotain haitallisempaa.

4.5.4 Tukevat ratkaisuehdotukset

Mihinkään ehdotetuista ratkaisuista – sidosryhmien määrään, koulutusten laajentamiseen ja seurannan kehittämiseen – ei ole olemassa mitään nopeaa ratkaisua vaan muutokset ovat suurempia organisaatiomuutoksia, jotka vaativat johdon tukea. Kuitenkin vain puolessa tutkituissa yrityksissä johto oli vahvasti mukana tietoturvapolitiikan

kehittämisessä. Osoittaakseen tukea toiminalle tulevaisuudessa, he voivat osallistua tietoturvapolitiikan jalkauttamiseen. Esimerkin näyttäminen ja kehittämiseen osallistuminen auttaa henkilöstöä näkemään muutosten tärkeyden, kehittäen yrityksen tietoturvakulttuuria.

5. MALLI TIETOTURVAPOLITIIKASTA

Tähän lukuun kootaan edellä kerättyyn materiaaliin perustuen malli tietoturvapolitiikasta ja paneudutaan syvemmin, miksi tietoturvapolitiikasta tulisi kukin kohta löytyä. Rakenne perustuu pääosin Ismailin ym:n [11] tunnistamiin politiikan kehittämisen vaiheisiin sekä Whitmanin [7] tunnistamiin korkean tason politiikan osiin. Mallissa, joka on listattu taulukkoon 4, pyritään tuomaan esiin, mitä kohdissa tulee huomioida eikä niinkään mitä niiden tulisi tarkasti sisältää.

Yleisiä vaatimuksia politiikalle ovat selkeäkielisyys, ytimekkyys, tarkoituksenmukaisuus. Selkeäkielisyys tekee lukijalle politiikasta helpommin luettavan ja kirjoittajan tulee tällöin miettiä, mitä asiat tarkoittavat pohjimmiltaan, jotta ne saadaan yksinkertaiseen muotoon. Ytimekkyys tarkoittaa tässä, että politiikka kiteyttää selkeästi tarkoitukset eikä pitkitä tai jaarittele turhaan. Näin politiikka pysyy nopeasti luettavana ja asettaa selkeästi ymmärrettävät tavoitteet. Tarkoituksenmukaisuudella tarkoitetaan, että politiikka tulee oikeaan tarpeeseen. Politiikkaa ei tule kirjoittaa vain politiikan kirjoittamisen takia vaan sen tulee olla hyödyllinen työkalu tietoturvan ohjaamisessa.

Taulukko 4. *Mallitietoturvapolitiikan rakenne*

Tietoturvapolitiikan osa	**Selite**
Tietoturvallisuuden ja sen osien määrittely	Mitä tietoturvallisuudella tarkoitetaan yrityskontekstissa ja millaisia osa-alueita se kattaa.
Tietoturvapolitiikan sisältö	Mitä tietoturvapolitiikka sisältää – millaisia dokumentteja siinä on, mitä ne sisältävät ja määrittelevät.
Vastuiden määrittely	Vastuiden määrittelyllä eri toiminnoille ja osa-alueille saadaan omistajat, jolloin politiikkaa on tehokkaampaa hallita.
Politiikan määräykset	Politiikan ydin eli määräykset, joista johdetaan muut tietoturvatoimet.
Valvonta	Miten tietoturvapolitikkaa valvotaan ja millaisia keinoja käytetään sen tehokkaaseen jalkauttamiseen
Tietoturvapolitiikan kehittäminen	Miten tietoturvapolitiikkaa kehitetään, kenen toimesta ja miten siihen voi vaikuttaa.

5.1 Tietoturvallisuus ja sen osien määrittely

Tietoturvapolitiikka tulee lähteä liikkeelle tietoturvan ja sen osien määrittämisestä organisaatiolle. Tämä tarkoittaa, millainen rooli tietoturvalla on koko organisaation toiminnassa ja mikä sen päätavoite on. Tämä auttaa sekä suunnittelijaa pysymään

tavoitteissaan että lukijaa myöhemmin ymmärtämään tietoturvallisuuden tärkeyden kyseisessä organisaatiossa. Lukijan tulisi tämän pohjalta ymmärtää, mitä toimintoja tietoturvallisuus kattaa ja miksi näitä halutaan suojata. Joskus tämä on itsestään selvää ja tällöin olisi hyvä tuoda esille organisaation erityistarpeita ja miten ne eroavat yleisistä tilanteista, jos tällaisia on. Monet tutkitut yritykset eivät tuoneet esille yritystensä toimialojen haasteita, mikä voisi olla tarpeen. Jo pelkän ensimmäisen osan jälkeen lukijan tulisi ymmärtää tietoturvallisuuden arvo ja olla motivoituneempi lukemaan ja sisäistämään loput tietoturvapolitiikasta. Motivaatiota voi vahvistaa myös koulutuksilla, jotka ovat usein pääsääntöinen tapa käydä tietoturvapolitiikka läpi. Koulutusten jälkeen lukija tuntee politiikan syyt paremmin ja hän on entistä vastaanottavaisempi tietoturvapolitiikan sisällölle.

5.2 Tietoturvapolitiikan sisältö

Määritelmän jälkeen tulisi päättää, mistä osista politiikka koostuu, sekä dokumentin sisältö että siihen liittyvät politiikat ja ohjeet. Tässä työssä suositellaan politiikan rakenteeksi modulaarista rakennetta, jonka Lopes ym. [2016] esittelivät työssään. Tämä rakenne sallii hallittavamman kokonaisuuden, koska ydinpolitiikka ei juuri muutu, mutta siihen liittyvien politiikkojen tai ohjeiden sisältö ja määrä voi muuttua, joten politiikan hallinnan kannalta tämä on tehokkain ratkaisu. Vaikka kyseessä olisi pieni organisaatio, modulaarista politiikka voi helposti laajentaa organisaation kasvaessa. Tutkituissa yrityksissä puolet olivat modulaarisia, joten tämä oli tunnistettu käytännössä myös toimivaksi rakenteeksi.

Liittyvissä politiikoissa tulee pitää mielessä samat seikat kuin itse tietoturvapolitiikan laadinnassa – erityisesti, että tulevatko politiikat oikeaan tarpeeseen. Rakenne on myös lukijalle selkeämpi. Hän löytää indeksin kaikista tukevista poliitikoista ja ohjeista, jotka hänen tulisi tuntea. Kun henkilö palaa politiikan pariin, on hänen helpompi löytää oleellinen tieto. Tämä tekee kokonaisuudesta selkeämmän eikä tietoturvapolitiikka tunnu niin pelottavalta. Myös kouluttamisen voi jakaa tätä kautta selkeämpiin kokonaisuuksiin ja opiskelijat voivat selkeästi yhdistää, mitä tietoturvapolitiikan osaa kyseisessä koulutuksessa käydään.

5.3 Vastuiden määrittely

Vastuiden jakaminen tulisi kuvata mahdollisimman aikaisin dokumentissa, heti perusmäärittelyjen jälkeen. Lukijan kannalta tämä helpottaa tarpeellisten henkilöiden tai ryhmien löytämisessä. Vastuiden määrittäminen auttaa politiikan jalkauttamisessa ja ylläpidossa. Kun yksi henkilö tai ryhmä on vastuussa yhdestä politiikan osasta, on tätä osa-aluetta helpompi ja tehokkaampi kehittää. Joissain tapauksissa yksi henkilö on vastuussa koko tietoturvapolitiikasta ja sen osa-alueista, jolloin hänen tukenaan olisi hyvä olla ryhmä muita ihmisiä, jotta politiikka ja sen kehittäminen heijastaisi koko

organisaation tilaa. Politiikkaa kehittäessä voi myös ottaa mukaan enemmän muita sidosryhmiä, joiden merkityksestä on jo puhuttu paljon, ja silloin kuulla heidän ajatuksiaan eri osa-alueista. Isommassa organisaatiossa eri tietoturvallisuuden osa-alueet on tehokkaampi jakaa politiikkaa ylläpitävän ryhmän kesken, koska osa-alueet voivat kattaa laajoja toimintoja, joita yksi henkilö ei voi hallita tehokkaasti.

Kun puhutaan tietoturvallisuuden osa-alueista, tarkoitetaan riskienhallinnan kautta tunnistettuja kokonaisuuksia. Tämä jako vaihtelee organisaatioiden välillä, mutta esimerkkejä voivat olla fyysinen turvallisuus, laiteturvallisuus, verkkoturvallisuus ja ohjelmistoturvallisuus. Nämä kaikki vaikuttavat tietoturvallisuuden kokonaisuuteen ja niiden hallinta voi organisaation koosta riippuen olla hyvinkin vaihtelevaa. Tietoturvan ja sitä ohjaavan tietoturvapolitiikan tulee olla sidoksissa organisaation toimintaan ja tämä sidos syntyy riskienhallinnan kautta. Riskianalyysin kautta tunnistetaan organisaatioon oikeasti vaikuttavia haasteita, joihin tietoturvallisuuden pitää vastata. Riskienhallinta on haastava kokonaisuus ja tähän voi olla järkevää hankkia ulkoista apua, jos organisaatioista ei löydy tarvittavaa osaamista.

5.4 Politiikan määräykset

Politiikan määräykset ovat koko politiikan ydin ja niiden sisältö vaihtelee eniten kaikista. Niiden tulee sisältää yritykselle olennaiset määräykset tietoturvalliseen toimintaan ja tätä varten tulee tietoturvallisuuden tarpeet olla selvitetty perinpohjaisesti. Kuten haastattelujen pohjalta tehdyn analyysin perusteella voi todeta, yrityksillä on usein haasteita kattavien sidosryhmien keräämisessä. Ilman tätä politiikan asettamat turvallisuusmenettelyt eivät sovi toimintaan ja niiden tehokkuus heikentyy.

Tässä osiossa on myös hyvä käydä läpi, millaisia vaatimuksia tietoturvapolitiikalla on taustalla, kuten lakeja ja asiakasvaatimuksia. Haastatteluissa yleisimpinä vaatimuksina tuotiin esiin standardit ja asiakasvaatimukset, mutta muita vaatimuksia tulisi joko nousta esiin tai niihin, erityisesti lakeihin, kannattaa tutustua, jos tavoitteena on toimia julkisten toimijoiden kanssa. Vaatimukset osittain auttavat lukijaa ymmärtämään, miksi tietyt määräykset ovat asetettu. Standardien avulla määräyksiä voi rajata hyväksi todettujen tapojen mukaisesti. Määräysten tulisi olla teknologia- ja ratkaisuriippumattomia, sillä nämä voivat muuttua nopeasti, mikä aiheuttaisi ylimääräistä työtä tietoturvapolitiikan ylläpidossa. Johdetut ohjeistukset voivat ottaa kantaa teknologioihin ja siihen, miten tietyt määräykset ratkaistaan käytännön tasolla.

5.5 Valvonta

Määräysten jälkeen tulisi ottaa kantaa siihen, miten tietoturvapolitiikkaa valvotaan ja millaisia toimia tehdään, että sen seuranta olisi mielekkäämpää. Tässä on hyvä ottaa huomioon valvonnan ja seurannan varmistamiseen liittyvät lähestymistavat: työntäminen

ja vetäminen. Rangaistuksilla uhkaaminen ja toimintaan pakottaminen voi joissain organisaatioissa olla toimiva tapa, jos yrityksen kulttuurissa on totuttu tiukkaan kuriin. Tutkimusten perusteella vetäminen eli palkitsemisen ja motivoinnin kautta vaikuttaminen on tehokkaampaa. Näin saadaan parempia tuloksia, kun henkilökunta on oikeasti halukas noudattamaan tietoturvapolitiikkaa ja sen ohjeita. Positiivisten keinojen hyödyntäminen noudattamisen tehostamisessa oli jäänyt vähälle huomiolle tutkituissa yrityksissä, vaikka positiivisia motivointikeinoja, kuten liiketoimintayksiköiden tulospalkkioita, käytetään usein muualla yrityksessä.

Tärkeää noudattamisen kannalta on, että noudattamisen ja noudattamattomuuden välillä on selkeä ero, joko rangaistusten tai palkintojen suhteen. Jos kummastakaan ei seuraa mitään, on motivaatio noudattaa politiikkaa olematon. Politiikan noudattamisen seuranta on tehokas tapa saada tilastoja, miten tehokas politiikka on tuottamaan tietoturvallisuutta yrityksessä. Jatkuvat rikkomukset tai piittaamattomuuden aiheuttamat tietoturvaongelmat kertovat huonosti toimivasta politiikasta, johon on tehtävä muutos.

5.6 Tietoturvapolitiikan kehittäminen

Lopuksi politiikkadokumentin tulisi ottaa kantaa, miten tietoturvapolitiikkaa päivitetään. Tässä pitäisi määritellä henkilö tai ryhmä, joka ylläpitää ja kehittää politiikkaa. Tämän avulla lukija voi löytää, kehen tulee ottaa yhteyttä, jos hänellä on kysymyksiä tai kehitysideoita politiikan suhteen. Myös päivitysprosessia voi kuvata tässä, kuten kuinka usein ja milloin politiikkaa yleensä päivitetään. Monet haastatellut yritykset käyttivät jatkuvan kehityksen mallia, jolloin tiettyjen toimenpiteiden suoraviivainen noudattaminen voi olla haastavaa. Kuitenkin kehittämisprosessin kuvauksella jatkuvankin kehittämisen saa toimimaan paremmin. Tämä toimii myös dokumentaationa, jos politiikasta vastaava henkilö vaihtuu.

6. PÄÄTELMÄT JA YHTEENVETO

Tässä diplomityössä tutkittiin, miten erilaisissa yrityksissä tietoturvapolitiikka on suunniteltu ja millaisia käytännönvaikutuksia sillä on. Tämän kautta haluttiin löytää haasteita tässä muutoksessa määräyksestä käytäntöön ja tuottaa opitun perusteella mallipolitiikka, joka on rakennettu tietoturvakulttuurin näkökulmasta.

6.1 Tutkimuksen yhteenveto

Tutkimuksessa haastateltiin kymmentä Suomessa eri toimialoilla toimivaa yritystä. Niiden koot vaihtelivat keskisuurista yrityksistä suuryrityksiin asti. Haastattelussa käytiin läpi kysymyksiä liittyen tietoturvapolitiikan suunnitteluun, toteuttamiseen ja seurantaan. Haastattelun muistiinpanot analysoitiin ja tuloksista kerättiin erilaisia havaintoja. Havainnoista kerättiin yleisiä sekä eri vaiheisiin liittyviä kehitysehdotuksia. Haastattelujen ja kirjallisuuden perusteella rakennettiin esimerkkirakenne tietoturvapolitiikan laadinnalle.

Kaikissa yrityksissä tietoturvapolitiikan taso oli hyvä suhteessa yrityksen kokoon. Yhdessäkään yrityksistä ei ollut täysin samanlaisia haasteita, mutta usein esiintyneitä haasteita tunnistettiin. Kullakin osa-alueella – suunnittelussa, toteuttamisessa ja seurannassa – tunnistettiin yksi selkeä kehitysalue. Kaikkia tukevana ratkaisuehdotuksena annettiin, että johdon tulisi osallistua enemmän tietoturvapolitiikan rakentamiseen. Erityisesti esimerkin näyttö on todettu tehokkaaksi tavaksi jalkauttaa tietoturvapolitiikkaa yritykseen.

Suunnittelun kehitysehdotuksena annettiin useampien sidosryhmien lisääminen prosessiin. Erityisesti ulkopuolisten sidosryhmien lisäämistä suositeltiin, sillä ne voivat tuoda erilaisia ajatuksia, miten tietoturvallisuus voisi toimia parhaiten. Erilaisten sidosryhmien etuna nähtiin niiden tuomien tarpeiden ja prosessien yksityiskohtainen tuntemus, joka helpottaa tietoturvapolitiikan jalkauttamista tulevaisuudessa. Haasteena voi kuitenkin olla organisaation koon aiheuttamat haasteet sidosryhmien osallistamisessa. Tämä vaatii tarkan suunnitelman, jotta oleellisen tiedon saa kerättyä ilman, että syntyy tilanne, jossa eri sidosryhmät rupeavat kinastelemaan tarpeistaan.

Toteuttamisen kehitysehdotuksessa tuotiin esiin koulutusten määrä ja laatu. Useissa yrityksissä tietoturvasta ja tietoturvapolitiikasta oli järjestetty vain yksi koulutus eikä noussut esiin, että tehtäisiin jatkuvasti töitä henkilöstön kouluttamisessa. Koulutusten järjestäminen ja kehittäminen on yksi tehokkaimmista tavoista saada vietyä tietoturvapolitiikka ja sitä tukevat ohjeet käytäntöön. Suunnittelussa tulee ottaa huomioon erilaiset oppijat ja heidän tarpeensa ja pyrkiä suunnittelemaan koulutukset ne mielessä pitäen. Verkkopohjaiset oppimisjärjestelmät ovat tehokas ratkaisu koulutusten

järjestämiseen, mutta ne vaativat paljon työtä suunnittelemisen ja rakentamisen muodossa. Suunnittelun tueksi on tarjolla paljon vapaasti saatavilla olevaa materiaalia, jonka pohjalta koulutuksia voi suunnitella. Koulutusten järjestämiseen voi käyttää myös ulkoisia konsultteja, mutta tällöin pitää varmistaa, että he perehtyvät yrityksen toimintatapoihin riittävän hyvin, jotta koulutuksista tulee oikealla tavalla kohdennettuja.

Seurannan kehitysehdotuksena esitettiin virheiden juhlimista. Tämän taustalla on ajatus, että ihmiset reagoivat paremmin positiiviseen lähestymiseen. Kun virhe tapahtuu, se nähdään oppimistapahtumana eikä virhettä tehnyttä aleta vain syyttämään ja rankaisemaan tapahtuneesta. Näin henkilöt tuovat ongelmia esille auliimmin ja tietoturvaa pystytään kehittämään ajoissa, ennen kuin ongelmat aiheuttavat jotain vakavampaa. Tämän haasteena on, miten henkilöstö saadaan luottamaan järjestelemään ja miten tietoturvallisuudesta vastuussa olevat henkilöt saadaan rakentavasti purkamaan ongelmat niin, että niistä voi oppia eikä ketään syyllistetä liikaa.

Lopuksi kaiken opitun pohjalta rakennettiin mallipolitiikka, jossa kuvattiin hyvän tietoturvapolitiikan keskeiset piirteet ja niiden merkitys tietoturvakulttuurin näkökulmasta. Rakenteessa pyrittiin ratkaisemaan työn aikana haastavimmiksi osiksi koetut tietoturvapolitiikan osat ja pitämään politiikka mahdollisimman yksinkertaisena. Politiikkaa ei kuitenkaan pidä rakentaa suoraan minkään ohjeen mukaisesti, sillä mikään valmis pohja ei välttämättä ole yritykselle sopiva vaan oman yrityksen tarpeet pitää tunnistaa ja rakentaa politiikka parhaita tapoja hyödyntäen, mutta silti soveltaa tätä tietoa omaan organisaatioon.

6.2 Merkitys käytännölle

Työn tuottamat tulokset tuovat vähän uutta tietoturvallisuuden tutkimukseen, mutta niillä saa katsauksen siitä, miten osassa Suomessa toimivista yrityksistä on toteutettu tietoturvapolitiikka ja sen jalkauttaminen tietoturvakulttuurin näkökulmasta. Tietoturvapolitiikkaa on tutkittu kattavasti viimeiset vuosikymmenet, koska sen merkitys on kasvanut merkittävästi. Tutkimuksissa on huomattu, tietoturvallisuuden johtamiseen pätevät samat menetelmät kuin muissakin yrityksen toiminnoissa. Tietoturvallisuuden hallinnossa käytetään samanlaisia strategioita, samanlaisia ihmisen käyttäytymiseen liittyviä tutkimuksia, määräyksiä ja ohjeita, joiden avulla pyritään ymmärtämään ja ohjaamaan kokonaisuutta. Tietoturvallisuus on yksi ala, jolla tätä kaikkea tietoa sovelletaan. Tästä tutkimuksesta voi huomata, että tietoturvallisuuden alalla on samanlaisia haasteita kuin muillakin aloilla ja perusteet ovat jo hyvin hallussa useimmilla yrityksillä.

6.3 Tutkimuksen kehittäminen

Työstä nousi kaksi aihetta, joita tulisi tutkia tietoturvallisuudessa enemmän. Ensimmäinen on virheiden juhliminen tietoturvaongelmien kontekstissa. Toisena on tietoturvapolitiikan mittaamisen kehittäminen ja hyvien mittareiden määrittäminen.

Virheiden juhlimista tietoturvallisuuden kontekstissa voisi tutkia kahdella yrityksellä, joissa toisessa tietoturvaongelmat koetaan negatiivisina ja toisessa niiden positiivisia puolia on korostettu. Näin nähtäisiin, vaikuttaako positiivinen suhtautuminen myönteisesti tietoturvaongelmista raportoimiseen. Tässä yrityksen tietoturvallisuuden kypsyystaso vaikuttaa paljon siihen, miten henkilöstö tunnistaa potentiaaliset ongelmat ja virheet.

Toisena potentiaalisena tutkimusalueena on tietoturvapolitiikkaan liittyvän mittaamisen kehittäminen. Erityisesti sopivien mittareiden tunnistamiseen tulisi löytää hyviä keinoja. Poikkeavan käytöksen huomaamiseen on jo teknisiä keinoja, jotka tarkkailevat tietoverkkoja ja laitteita ja miten ihmiset käyttävät niitä. Kuitenkin on paljon toimia, joihin ei ole vielä tunnistettu sopivia automaattisia mittareita. Moni tietoturvalliseen käyttäytymiseen liittyvä mittaaminen perustuu pistemäiseen auditointiin, joka ei välttämättä anna todellista kuvaa toiminnasta. Kehittynyt teknologia on tuonut uusia mahdollisuuksia saada parempaa kuvaa tietoturvatoiminnasta, muun muassa suurien data-aineistojen (*big data*) analysoinnin avulla voi löytää uusia tietoturvamittareita. Dataa voi kerätä verkkoon yhdistetyistä laitteista, kuten tietokoneista, pääsynhallintajärjestelmistä ja palomuureista. Verkkoliikenteestä voi nähdä, miten tietyt prosessit toimivat tai löytää poikkeamia normaalista toiminnasta.

LÄHTEET

[1] Gartner Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, web page. Saatavissa (viitattu 12.05.2019): https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019.

[2] J. Andress, M. Leary, Chapter 4 - Why Information Security Policies? in: J. Andress, , M. Leary (ed.), Building a Practical Information Security Program, Syngress, 2017, s. 63-75.

[3] Valtiovarainministeriö, Tietoturvallisuudella tuloksia: Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, Valtiovarainministeriö, 2007, 111 s.

[4] Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto, julkaisussa: SFS-EN ISO/IEC 27000:2017, Suomen Standardoimisliitto SFS, 2017.

[5] Valtiovarainministeriö Tietoturvallisuus - mitä se on? Saatavissa (viitattu: 11.04.2019) https://www.vahtiohje.fi/web/guest/691.

[6] I. Lopes, P. Oliveira, Architecture of information security policies: A content analysis, Advances in Intelligent Systems and Computing, s. 493-502.

[7] M.E. Whitman, Security Policy: From Design to Maintenance, in: R. Baskerville, D.W. Straub, S.E. Goodman (ed.), Information Security: Policy, Processes, and Practices, Routledge, Armonk, NY, 2008, s. 123-151.

[8] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, MIS Quarterly: Management Information Systems, Vol. 34, Iss. SPEC. ISSUE 3, 2010, s. 523-548.

[9] A.C. Johnston, M. Warkentin, M. Mcbride, L. Carter, Dispositional and situational factors: influences on information security policy violations, European Journal of Information Systems, Vol. 25, Iss. 3, 2016, s. 231-251.

[10] J.R. Vacca, Managing Information Security, Syngress, Waltham, MA, 2014, 347 s.

[11] W.B.W. Ismail, S. Widyarto, Ahmad, Raja Ahmad Tariqi Raja, K. Abd Ghani, A generic framework for information security policy development, 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), IEEE, s. 1-6.

[12] J.D. Nosworthy, Implementing information security in the 21st century - Do you have the balancing factors? Computers and Security, Vol. 19, Iss. 4, 2000, s. 337-347.

[13] E. Niemimaa, Crafting organizational information security policies, väitöskirja, Tampereen teknillinen yliopisto, 2017, Saatavissa: https://tutcris.tut.fi.

[14] K.J. Knapp, R. Franklin Morris, T.E. Marshall, T.A. Byrd, Information security policy: An organizational-level process model, Computers & Security, Vol. 28, Iss. 7, 2009, s. 493-508.

[15] R. Baskerville, M. Siponen, An information security meta-policy for emergent organizations, Logistics Information Management, Vol. 15, Iss. 5/6, 2002, s. 337-346.

[16] P. Puhakainen, M. Siponen, Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, MIS Quarterly, Vol. 34, Iss. 4, 2010, s. 757-778.

[17] S. Pahnila, M. Siponen, A. Mahmood, Employees' Behavior towards IS Security Policy Compliance, 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), IEEE, s. 156b.

[18] S. Pahnila, M. Siponen, A. Mahmood, Which factors explain employees' adherence to information security policies? An empirical study, PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises.

[19] E. Niemimaa, Legitimising Information Security Policy during Policy Crafting: Exploring Legitimising Strategies, 2016.

[20] E. Niemimaa, M. Niemimaa, Information systems security policy implementation in practice: From best practices to situated practices, European Journal of Information Systems, Vol. 26, Iss. 1, 2017, s. 1-20.

[21] E. Niemimaa, Crafting an Information Security Policy: Insights from an Ethnographic Study, 2016.

[22] S.V. Flowerday, T. Tuyikeze, Information security policy development and implementation: The what, how and who, Computers & Security, Vol. 61, 2016, s. 169-183.

[23] S.B. Maynard, A.B. Ruighaver, A. Ahmad, Stakeholders in security policy development, 9th Australian Information Security Management Conference, Edith Cowan University, s. 182-188.

[24] Ohje riskienhallintaan, in: Valtiovarainministeriön julkaisuja, Valtiovarainministeriö, 2017.

[25] Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet, in: SFS-EN ISO/IEC 27002, Suomen Standardoimisliitto SFS, 2017.

[26] Information Systems Audit and Control Association, COBIT 5: A business framework for the governance and management of enterprise IT, ISACA, Rolling Meadows, IL, 2012.

[27] B.L. Williams, Information Security Policy Development for Compliance: ISO/IEC 27001, NIST SP 800-53, HIPAA Standard, PCI DSS V2.0, and AUP V5.0, Auerbach Publications, Boca Raton, Fla, 2016.

[28] Laki kansainvälisistä tietoturvallisuusvelvoitteista, 2004. Saatavissa: https://www.finlex.fi/fi/laki/smur/2004/20040588.

[29] T. Schlienger, S. Teufel, Information security culture-from analysis to change, South African Computer Journal, Vol. 2003, Iss. 31, 2003, s. 46-52.

[30] ENISA, Cyber Security Culture in organisations, 2018, Saatavissa (viitattu 27.3.2019): https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[31] M. Tang, M. Li, T. Zhang, The impacts of organizational culture on information security culture: a case study, Information Technology and Management, Vol. 17, Iss. 2, 2016, s. 179-186.

[32] G. Hofstede, B. Neuijen, D.D. Ohayv, G. Sanders, Measuring Organizational Cultures: A Qualitative and Quantitative Study across Twenty Cases, Administrative Science Quarterly, Vol. 35, Iss. 3, 1990, s. 286-316.

[33] A. McIlwraith, Information Security and Employee Behaviour : How to Reduce Risk Through Employee Education, Training and Awareness, Routledge, Aldershot, England, 2006.

[34] Kyberturvallisuuskeskus, Tietoturvan vuosi 2018, 2019, Saatavissa (viitattu 07.04.2019): https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf.

[35] B. Gardner, V. Thomas, Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats, Syngress Media Incorporated, US, 2014, s. 214.

[36] P.N. Blanchard Training Delivery Methods, Saatavissa (viitattu 07.04.2019): https://www.referenceforbusiness.com/management/Tr-Z/Training-Delivery-Methods.html.

[37] Y. Chen, K. Ramamurthy, K. Wen, Organizations' Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems, Vol. 29, Iss. 3, 2012, s. 157-188.

[38] J.H. Schuessler, General Deterrence Theory: Assessing Information Systems Security Effectiveness in Large versus Small Businesses, väitöskirja, University of North Texas, 2009.

[39] M.J. Lahtinen, Henkilöstön osallistaminen palkkajärjestelmän uudistuksessa: case Finlayson Oy, pro gradu -työ, 2007, Saatavissa: https://tuni.finna.fi/Record/tamcat.463891.

[40] Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi, SFS-ISO/IEC 27004, Suomen Standardoimisliitto SFS, 2016.

[41] I. Salmela, Mittaaminen osana liiketoimintalähtöistä tietoturvallisuuden hallinnointia, Tampereen teknillinen yliopisto, 2013.

[42] G. Walsham, Interpretive case studies in IS research: nature and method, European Journal of Information Systems, Vol. 4, Iss. 2, 1995, s. 74-81.

[43] K. Nagata, Y. Kigawa, T. Aoki, Trial for E-learning system on information security incorporate with learning style and consciousness factors, International Journal of Engineering Pedagogy, Vol. 8, Iss. 3, 2018, s. 120-136.

[44] Kyberturvallisuuden asiantuntija, Helsinki. Haastattelu 23.10.2018.

[45] M.R. Bleich, Leadership and Brilliant Mistakes, The Journal of Continuing Education in Nursing, Vol. 46, Iss. 5, 2015, s. 203-204.

LIITE A: HAASTATTELUKYSYMYKSET

Suunnittelu

1. Perustuuko tietoturvapolitiikka johonkin olemassa olevaan pohjaan?
2. Millaisia sidosryhmiä suunnittelutyöhön otettiin mukaan?
3. Millainen johdon tuki oli, kun tietoturvapolitiikan luontiin?
4. Millainen prosessi tietoturvapolitiikan suunnittelussa oli?

Toteutus

5. Toteutettiinko riskianalyysia tietoturvariskien varalta?
6. Millainen politiikan rakenne on? Yksilöllinen (järjestelmillä yms. omat politiikkadokumenttinsa), kokonainen (yksi politiikka, joka kattaa kaikki järjestelmät ja antaa yleisiä ohjeita) vai modulaarinen (keskitetty dokumentti, joka antaa eri järjestelmille ja teknologioille ohjeita ja määräyksiä)?
7. Tiedotettiinko politiikan toteuttamisesta? Jos tiedotettiin, miten paljon ja mitä kautta?
8. Miten politiikka jaettiin kaikille sidosryhmille? Sähköisesti, paperilla? Oliko koulutusta?

Seuranta

9. Miten tietoturvapolitiikan noudattamista seurataan?
10. Onko tiedossa, että politiikkaa olisi rikottu? Jos on, miten kuvailisit rikkomusten vakavuutta ja määrää?
11. Mitä toimia tehdään, että yrityksen henkilö voi kokea politiikan omakseen?
12. Miten paljon aikaa politiikan ylläpitoon käytetään vuosittain (htp)?
13. Miten kauan nykyisen politiikan uskotaan kestävän?