Ulkoministeriön tietoturvakäsikirja esimiehille

Virtanen Matias

2018 Laurea

Laurea-ammattikorkeakoulu

Ulkoministeriön tietoturvakäsikirja esimiehille

Virtanen Matias
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Joulukuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Virtanen Matias

Ulkoministeriön tietoturvakäsikirja esimiehille

Vuosi 2018 Sivumäärä 60

Opinnäytetyö kokoaa ulkoministeriön esimiesten käyttöön tietoturvallisuutta käsittelevän ohjeistuksen tietoturvakäsikirjan muodossa. Käsikirja on osa organisaation tietoturvatiimin vuoden 2016 tavoitteita, ja sen tarkoitus on tarjota esimiesasemassa oleville organisaation työntekijöille tiivis ja ajantasainen tietopaketti. Ohjeistus on kohdennettu tukemaan heitä heidän tietoturvarooleissaan.

Turvallisuuskulttuuri rakentuu johdon sitoutumisen pohjalta, esimiesten osoittamalla esimerkillä, turvallisuusasiantuntijoiden koordinoimana. Esimerkillä johtaminen turvallisuustyössä edellyttää esimiehiltä tietotaitoa ja ymmärrystä toimintakentästä. Se vaatii myös motivaatiota turvallisuustyöhön sekä työtä tukevia työkaluja. Tämä on haastavaa koska kyberturvallisuuden toimintakenttään liittyvät riskit ovat jatkuvassa muutosliikkeessä.

Esimiesten ja ylimmän johdon on otettava turvallisuus ja riskienhallinta huomioon kaikissa päätöksissään. Koko organisaation kattavan turvallisuusajattelun kehittyminen edellyttää että esimiehet sisäistävät tietoturvavastuunsa sekä hyväksyvät oman roolinsa turvallisuuskulttuurin kehittäjinä. Opinnäytetyön teoreettinen viitekehys hyödyntää teoriaa turvallisuuskulttuuriin vaikuttamisesta, tietoturvaohjeistuksen luomisessa ja hakee vastauksia siihen mitkä asiat haastavat esimiehiä heidän tietoturvaan liittyvien vastuidensa toteuttamisessa ja millainen on hyvä esimiehen tietoturvaohje.

Opinnäytetyössä haastateltiin neljää kohdeorganisaation esimiestehtävissä toimivaa virkamiestä, sekä haastateltiin viittä eri turvallisuusalan ja tietoturvallisuuden asiantuntijaa ja analysoitiin heidän ajatuksiaan laadullisen tutkimuksen keinoin. Tietoturvallisuuskäsikirjan muotoa ja sisältöä haettiin haastattelun ja kirjallisuuskatsauksen analysoinnin perusteella. Opinnäyte käsittelee myös vaihtoehtoisia tietoturvallisuuden oppimismuotoja, koska kirjoitettu ohjeistus on vain yksi työkalu turvallisuuskulttuurin kehittämisessä.

Opinnäytetyön tuloksena syntynyt ohjeistus toimii toimintaa tukevana turvallisuusdokumenttina kohdeorganisaation käytössä. Saatavuuden ja päivitettävyyden takaamiseksi tietoturvakäsikirjasta luotiin sisäverkossa toimiva Wiki-aineisto. Ohjeistuksen formaatiksi muodostui lukijaansa puhutteleva ja tavanomaisesta tiukan asialinjaisesta turvallisuusohjeesta poikkeava konstruktio, joka tarjoaa case-esimerkkejä sekä tarkistuslistoja sekä haastaa esimiehiä keskustelemaan tietoturvallisuuden eri osa-alueista työyhteisössään. Toisena opinnäytetyön konstruktiona rakentui konsepti “Edustuston tietoturvapeli”, jossa interaktiivisen pelillistämisen keinoin kehitetään esimiesvetoisesti henkilöstön turvallisuustietoisuutta.

Asiasanat: Tietoturvapeli, Turvallisuusjohtaminen, Turvallisuuskulttuuri, Tietoturvakäsikirja, Turvallisuustietoisuus

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor's Thesis

Virtanen Matias

Information Security Handbook for Managers at the Ministry of Foreign Affairs of Finland

Year 20182018 Pages 60

This objective of this thesis was to summarize the Ministry of Foreign Affairs of Finland's information security guidelines and instructions for the managers in the form of an information security handbook. The handbook, as an up-to-date information manual, was one of the objectives set for the Ministry's information security team in 2016 to support the managers and leaders of the organization in their security responsibilities.

Commitment of the leadership is crucial in creating a successful security culture, with support of the managers and guidance of security specialists. Leading by example in security management requires knowhow, motivation and proper resources. In information security management this is especially challenging as cybersecurity risks are constantly evolving.

It is vital for managers to take a security and risk-management based approach in all of their decisions. Improvement of security awareness in the organization requires managers to grow into their information security roles and to acknowledge their responsibilities as promoters of security culture.

The theoretical framework of this thesis covers the concepts of the security culture and instructions for writing security instructions and it examines the challenges managers face in fulfilling their information security responsibilities. Four managers of the host organization as well as five information security specialists were interviewed in this thesis to answer the relevant research questions. The results of these interviews were analysed with qualitative analysis methods.

The format and content of the information security handbook were formed based on conclusions drawn from the interviews and literature review. Alternative forms of information security learning were also examined and recommended as the theory suggested that written instructions were only a part of the solution for developing a successful security culture.

The information security handbook as the main outcome of this thesis serves as a supportive information security document for the ministry's organization. To ensure availability and updatability, the handbook was developed as an intranet Wiki. The style of the document was a case-story and checklist driven narrative, instead of a regular policy-driven security document. As a side result of the thesis, a concept of an information security game for embassies was drawn, to improve employee security awareness through the use of gamification and interactivity under managers' supervision.

Keywords: Gamification, Security awareness, Security culture, Information security handbook

Sisällys

1 Johdanto 6
2 Työn tausta 6
2.1 Tavoite, tarkoitus ja tutkimuskysymykset 7
2.2 Työn rajaus 7
2.3 Keskeiset käsitteet 8
3 Opinnäytetyössä käytetyt menetelmät 8
3.1 Tietoperustan rakennus kirjallisuuskatsauksen ja havainnoinnin avulla 9
3.2 Teemahaastattelut 9
3.3 Haastatteluaineiston analysointi 10
4 Ulkoministeriö ja ulkoasianhallinto numeroina 10
4.1 Ulkoministeriön ja ulkoasianhallinnon toimintaympäristö 11
4.2 Ulkoministeriön tietoturvatoiminta 12
4.3 Ulkoministeriön ja edustustojen esimiesten rooli tietoturvallisuudessa 13
5 Johtamisen yhteys organisaatiokulttuuriin 15
6 Turvallisuuskulttuuri ja sen kehittäminen 16
6.1 Turvallisuustietoisuuden kehittymisen vaatimuksia 18
6.2 Mistä virheet tietoturvaohjeiden noudattamisessa johtuvat 20
6.3 Onnistuneen ohjeen ja koulutuksen piirteitä 22
7 Opinnäytetyöprosessi 23
7.1 Teemahaastatteluista uutta tietoa esimiesten turvallisuusohjeistukseen 26
8 Tulokset 26
8.1 Esimiehen rooli turvallisuuskulttuurin rakentajana 26
8.2 Tietoturvan toteutumisen haasteet esimiestyössä 28
8.3 Hyvän esimiesohjeen tunnusmerkkejä 29
9 Johtopäätökset ja pohdinta 31
9.1 Työn arviointi ja jatkotutkimuskysymykset 37

1 Johdanto

Osallistuin vuoden 2017 alussa asiantuntijaseminaariin, jonka alustajana toimi ulkoministeriön tietoturvapäällikkö Antti Savolainen. Seminaari käsitteli 2013 ulkoministeriössä tapahtunutta tietovuotoa (Helsingin Sanomat 2013). Olin hakenut jo vuoden ajan omaa ammattitaitoani kehittävää työharjoittelupaikkaa. Keskusteltuani Savolaisen kanssa havaitsimme, että ulkoministeriöllä olisi käyttöä turvallisuusalan opiskelijalle, joka käsittelisi opinnäytetyössään ulkoministeriön esimiesten tietoturvavastuita ja kokoisi ohjeasiakirjan heidän työnsä tueksi.

Ulkoministeriön halu kehittää tietoturvallisuuden osuutta viraston esimiestyössä on osaltaan mahdollistanut tämän opinnäytetyöprojektin aloituksen. Tietoturvallisuuden kehittäminen julkishallinnossa juontaa 1.12.2009 voimaan astuneeseen Valtioneuvoston periaatepäätökseen valtionhallinnon tietoturvallisuuden kehittämisestä. Periaatepäätös ohjaa julkishallintoa tietoturvallisuuden kehittämisessä osana riskienhallintaa, johtamista, resurssisuunnittelua, hallinnon kehittämistä sekä tarkastustoimintaa. (Valtiovarainministeriö 2009.)

Ulkoministeriölle suoritettuun tietoturvaharjoitteluun sisällytettiin esimiehille suunnatun ohjeistuskirjan laatiminen. Opinnäytetyön tarkoitukseksi määriteltiin koota jo olemassa oleva ulkoministeriön tietoturvan hallussa oleva tietoturvadokumentaatio ja rikastaa sitä lisämateriaalilla, joka peilaisi haastatteluista saatua tietoa ja omia havaintojani ulkoministeriössä suoritettavan harjoittelun aikana.

Opinnäytetyöprojektin kuluessa tarkastelussa on kohdeorganisaation tietoturvatoiminnan nykytila ja erityisesti esimiehille tarjottavat tietoturvakoulutukset ja –palvelut. Kehityspisteiden löytämiseksi olemassa olevia ohjeita ja työkaluja peilataan esimiesten käytännön mielikuviin tietoturvallisuudesta osana ulkoministeriön päivittäistä työskentelyä.

2 Työn tausta

Ulkoministeriön tietoturvatiimi on vuosisuunnitelmassaan katsonut, että esimiesten tietoturvallisuustietoisuutta on tuettava, jotta turvallisuusjohtamisen tasoa voidaan nostaa vastaamaan valtionhallinnon tietoturvatavoitteita ja nykyajan korostuvia tietoturvahaasteita (Ulkoministeriön tietoturvatiimi 2016). Asia on ajankohtainen etenkin ulkoasiainhallinnon edustustoverkossa. Edustustot ovat pitkälti autonomisia yksiköitä, joiden toiminnasta ja sen mukaan myös tietoturvallisuustyön toteutuksesta edustuston esimiehet ovat vastuussa (ulkoministeriö 2018; Peltonen 2017; Savolainen 2018.) Esimiehille muodostuu korostettu henkilöstön koulutus- ja ohjeistusvastuu johtuen ulkoministeriön tehtäväkierrosta: virkamiesuran ja yleisuran virkamiesten tehtävänkuvat vaihtuvat tasaisesti noin 2-5 vuoden välein. (Peltonen 2017).

2.1 Tavoite, tarkoitus ja tutkimuskysymykset

Opinnäytetyön tarkoituksena on etsiä tietoa ja kehittää työkaluja, joilla voidaan edistää kohdeorganisaation turvallisuuskulttuuria ja esimiesten turvallisuustietoisuutta. Ulkoministeriö kansallisten ja kansainvälisten tietoturvallisuusvelvoitteidensa vuoksi tähtää jatkuvasti kehittämään tietoturvallisuutensa tasoa, kattaakseen vaatimuksen mukaisuuden osalta kaikki sen tietoturvallisuuden tasoa koskevat vaatimukset (Tietoturvatiimi 2016).

Opinnäytetyöprojektin tavoitteeksi muodostui laatia ulkoministeriön ja etenkin sen edustustojen esimiehiä palveleva tietoturvaohjeistus. Tavoitteeseen pääseminen edellytti toimintaympäristön ja sen haasteiden ymmärtämistä katselmoimalla tietoturvan nykytilaa ja esimiesten roolia siinä. Tämän lisäksi tarkoituksenmukaista oli tarkastella esimiesasemassa olevien virkamiesten vaikutusta turvallisuuskulttuuriin kohdeorganisaatiossa ja pohtia keinoja heidän tukemiseensa tietoturvatehtävissään. Opinnäytetyössä tarkasteltavat tutkimuskysymykset ovat:

1. Mikä on esimiesten rooli turvallisuuskulttuurin rakentajina?

2. Mitkä asiat haastavat ulkoministeriön esimiehiä toteuttamasta heidän tietoturvaroolejaan?

3. Mitä ominaisuuksia on hyvällä esimiehen tietoturvaohjeistuksella?

Ensimmäinen kysymys esimiesten roolista turvallisuuskulttuurin rakentajina, kysyy myös kuinka tärkeä huomioitava ryhmä esimiehet ovat tietoturvallisuustyössä. Toinen kysymys hakee tietoa siitä mitä tietoturvallisuuteen liittyviä käytännön haasteita esimiehet kokevat omassa työssään ja alaistensa ohjauksessa. Kaksi aiempaa kysymystä toivottavasti tarjoavat näkökulmia hyvän tietoturvaohjeistukselle luotaviin vaatimuksiin.

2.2 Työn rajaus

Vaikka ulkoministeriö on laaja organisaatio, tietoturvakäsikirjan kohdelukijoiksi valikoituivat kaikki organisaation esimiesrooleissa toimivat. Kohdeorganisaatiolla on jo ohjeet ja prosessit uusien työntekijöiden tietoturvallisuuden kouluttamiseksi, joten kaikkia työntekijöitä koskevia aihealueita käsitellään vain sillä syvyydellä, jolla esimiesnäkökulma saa siitä tarvitsemaansa tarttumapintaa. Erityisen tärkeäksi kohderyhmäksi muodostuivat ulkohallinnon edustustoverkoston esimiehet: edustuston päällikkö ja hänen sijainen ovat vastuussa edustuston kokonaisturvallisuudesta osittain maantieteellisesti ja aikavyöhykkeellisesti kaukana ulkoministeriön tietoturvallisuuteen ja turvallisuuteen liittyvistä tukipalveluista.

Tietoturvakäsikirjan tuottamisessa työtä rajattiin yhdessä toimeksiantajan kanssa siten, että opinnäytetyön kirjoittajan vastuulla on tietoturvallisuuskäsikirjan kirjallisen sisällön suunnittelu. Työhön sisältyy olemassa olevien tietoturvaohjeiden kokoamista sekä uuden materiaalin laatimista siltä osin, kuin aiemmasta ohjeistuksesta löytyy puutteita. Tietoturvakäsikirjan

tuottamisen osalta kohdeorganisaation edustajan vastuulle jää muodostetun kirjoitetun materiaalin arviointi ja siitä soveltuvin osin käsikirjan tuottaminen joko verkko – tai painettuna käsikirjana, tai molempina.

2.3 Keskeiset käsitteet

Käsikirja on kielitoimiston (2018) määrityksen mukaan teos, joka selittää keskeiset käytännön tiedot joltain alalta. Merriam-Webster (2018) määrittää sen kirjaksi, jota on helppo kuljettaa mukanaan, ja joka toimii tiiviinä viitekirjana jostain tietystä aihealueesta. **Tietoturvakäsikirja** kokoaa ja tarjoaa joukon ohjeita, jotka liittyvät tietoturvallisuuden laajaan aihealueeseen.

Tietoturvallisuus on käsitteenä laaja. Se koostuu tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä. Käsitteistöä laajennetaan ajoittain etenkin viranomaisohjeistuksissa kiistämättömyydellä. Tietoturvallisuus on osa organisaation laadullista turvallisuustoimintaa. Riittävä tietoturvallisuuden taso on välttämätön edellytys minkä tahansa toiminnan uskottavuudelle ja jatkuvuudelle. (Valtiovarainministeriö 2004, 5.) Tietoturvallisuuden osa-alueita on kahdeksan ja ne ovat kaikki tärkeitä organisaation kokonaisturvallisuuden kannalta. Osa-alueet ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. (Vahti 2004, 5-6.)

Turvallisuustietoisuus tarkoittaa henkilön ymmärrystä turvallisuudesta sekä sen syistä ja seurauksista. Henkilön arvot ja asenteet vaikuttavat konkreettisesti turvallisuustietoisuuden kehittymiseen. Henkilön turvallisuustietoisuudella on vahva linkki koko organisaation turvallisuuskulttuuriin. (Puhakainen 2006; Puhakainen 2017; Heljaste ym. 2008.)

3 Opinnäytetyössä käytetyt menetelmät

Tietoturvallisuuden esimieskäsikirja on toiminnallinen ja työelämälähtöinen opinnäytetyö, jonka tarkoituksena on hakea toimeksiantajan organisaation tarvitsemia vastauksia ja ratkaista niiden avulla käytännön ongelmia. Tutkimukselliset menetelmät tukevat saatujen vastausten luotettavuutta, vaikka niiden käyttö toiminnallisessa opinnäytteessä onkin väljempää. Opinnäytetyössä tiedon keräämisen ja analysoinnin menetelminä käytetään laadullisia, eli kvalitatiivisia menetelmiä, jotka sopivat aiemmin vieraan aihealueen, kuten esimiesten turvallisuustietoisuuden kehittämiseen liittyvien kysymysten ymmärtämiseen.

Toiminnallinen opinnäytetyö on luonteva valinta menetelmäksi, kun laaditaan ohjetta tai kirjaa, joka on lukijavetoinen ja sen laadinnassa on tarkoitus osoittaa asiantuntevuutta. Toiminnalliselle opinnäytetyölle on ominaista tutkimuksen ja toiminnan samanaikaisuus. Kirjoitusprosessi ja tiedon hankinta vuorottelevat ja tukevat toisiaan. Toiminnallisen opinnäytetyöhön

liittyy olennaisesti tutkiva osuus, jossa kirjoitetaan opinnäytetyöraportti sekä toiminnallinen osuus, eli produkti tai konstruktio. (Vilkka & Airaksinen 2003.)

3.1 Tietoperustan rakennus kirjallisuuskatsauksen ja havainnoinnin avulla

Kirjallisuuskatsaus tiedonkeruumenetelmänä mahdollistaa jo kirjoitettujen ja työn kannalta olennaisten materiaalin läpikäynnin keräten niistä tietoa osaksi teoreettista viitekehystä ja luoden kirjoittajalle kuvan siitä, miten aihealuetta on tutkittu aiemmin ja ohjaten tutkimuksenteon seuraavia vaiheita (Hirsjärvi, Remes & Sajavaara 2013, 121.)

Kirjallisuuskatsauksen osalta tietoperustan kasvattamiseksi suoritettiin hakuja Finnasta ja Google Scholarista suomeksi ja englanniksi hakusanoilla ”information security awareness”, ”information security education”,”turvallisuustietoisuus”, ”tietoturvallisuus koulutus”, ”security culture” ja ”turvallisuuskulttuuri”.

Tutkimuksen alkutietojen keräämisessä käytetään myös osallistuvaa havainnointia. Havainnoinnin keinoin voidaan mm. tutkia, toimivatko henkilöt, kuten he kertovat toimivansa ja miten organisaation turvallisuuskulttuuri näkyy toimintaympäristössä. (Hirsjärvi, Remes & Sajavaara 2013, 212-213). Laadullisen tutkimuksen keinoin on tarkoitus löytää runsaasti tietoa opinnäytetyön aihealueesta, koska tietoturvakäsikirjan laatiminen vaatii lukijaryhmän ja kohdeorganisaation kokonaisvaltaista ymmärtämistä.

3.2 Teemahaastattelut

Hirsjärvi & Hurme (2011, 35) toteavat, että haastattelu on sopiva tutkimusmenetelmäksi, kun ei tiedetä, minkälaisia vastauksia tiedonhankintamenetelmällä tullaan saamaan, tai kun vastauksia haetaan perustuen haastateltavan omiin kokemuksiin. Teemahaastattelua voidaan käyttää sellaisten aihealueiden tutkimiseen, jotka ovat joko arkoja tai niistä tiedetään vähän (Metsämuuronen 2003, 187).

Teemoittelussa valittujen teema-alueiden täytyisi olla tarpeeksi väljiä, että aihealueen monipuolisuus pääsee esille. Yksityiskohtaista kysymysluetteloa ei käytetä, vaan tätä väljempää teema-alueluetteloa. (Hirsjärvi & Hurme 2011.) Yleisin tapa valita teemahaastattelun teemat on intuitiivinen. Jos teemojen valinta ei perustu teoreettisiin kytkentöihin, on saadun lähdeaineiston analysointi vaikeaa. Teemarungon rakentamisessa voidaan käyttää myös aiempaan tutkimukseen perustuvaa kysymysrunkoa tai johtaa teemat suoraan teoriasta (Eskola & Vastamäki 2001, 33.)

Teemahaastatteluita suoritettaessa katsottiin tärkeäksi käydä haastattelut kasvotusten aina kun se oli mahdollista. Toissijaisena keinona oli suorittaa haastatteluita puhelimitse. Haastattelujen tallentamiseen käytettiin nauhoitusta, jotta tarkkaavaisuutta ei tarvitse jakaa vastausten kirjaamiseen ja haastattelun suorittamisen välillä. Nauhoitus myös edistää tiedon

eheyttä, koska tallenteen voi kuunnella useampaan kertaan (Hirsjärvi & Hurme 2011, 184). Myös tietoturvallisuuden näkökannalta on tärkeää saada lupa nauhoitukseen etukäteen sekä kertoa haastateltaville, miten tietoa käsitellään, säilytetään ja kenelle sitä voidaan jakaa eteenpäin. Haastateltavilla on oltava myös mahdollisuus vaikuttaa nauhoitteiden säilyttämiseen aineiston litteroinnin jälkeen.

3.3 Haastatteluaineiston analysointi

Analyysin teko voi alkaa jo haastattelutilanteessa. Analysointimallin valinnassa on oleellista yhteys aineiston ja analysoitujen tulosten välillä. Päättely voi olla joko induktiivista tai abduktiivista. Induktiivisessa päättelyssä tärkeintä on aineistokeskeisyys ja siitä päätelmien muodostus, kun taas abduktiivisessa päättelyssä haastattelija pyrkii todentamaan jonkin olemassa olevan hypoteesin tai teorian. Oikea analysointitapa mahdollistaa tutkimuksen luotettavuuden. Haastattelujen teemoja selvitettiin induktiivisella (Hirsjärvi & Hurme 2011, 136.)

Haastattelujen analysointi suoritettiin ensimmäistä kertaa mahdollisimman nopeasti haastattelujen jälkeen. Tällöin itse haastattelutapahtuma oli vielä muistissa sekä siihen liittyvät sanattomat eleet ja korostukset (Hirsjärvi & Hurme 2011, 135). Haastattelut litteroitiin tietokoneelle, jotta niitä oli helpompi analysoida. Haastattelijalla ei pyrkinyt todentamaan olemassa olevaa hypoteesia, vaan analysointi oli luonteeltaan induktiivista. Jatkuva haastattelun analysointi helpotti myös aina seuraavaan haastatteluun valmistautumista ja valittuihin teemoihin liittyvien jatkokysymyksiin valmistautumista. Ensimmäiset haastattelut olivatkin tästä johtuen heikkotasoisempia kuin viimeiseksi suoritetut.

Haastattelujen vastaukset teemoiteltiin sen mukaan, miten ne tarjoavat tietoa haastateltavan käsityksistä tietoturvallisuudesta ja sen yhteydestä työnkuvaansa ja päivittäisiin rutiineihinsa. Teemat (liite 1) tuntuivat luonnollisilta, koska ne olivat syntyneet jo pitkälti haastattelukysymyksiä laadittaessa. Esimiehiltä kysyttiin myös, mitkä he katsoivat suurimmiksi haasteiksi tietoturvaan liittyvien esimiesvastuidensa toteutumiselle. Opinnäytetyössä tärkeänä teemana oli myös keskustelu tietoturvaohjeen hyvyysvaatimuksista ja minkälainen tietoturvaohje vastaisi esimiehen tarpeita. Aineistosta pyrittiin keräämään toistuvia teemoja, ajatuksia ja mielipiteitä. Ennen tutkimuskysymyksiin liittyviin teemoihin pyrkimistä haastateltavien kanssa keskusteltiin miten he ymmärsivät tietoturvallisuuden ja mikä sen merkitys oli hänelle hänen työssään.

4 Ulkoministeriö ja ulkoasianhallinto numeroina

Maamme kansainvälisistä suhteista vastaa ulkoasiainhallinto, jonka muodostaa pääkaupungissamme Helsingissä sijaitseva ulkoministeriö ja 89 ulkomaanedustustoa ympäri maailman (ulkoministeriö 2018.) Kuvion 1 mukaisesti vuonna 2016 ulkoministeriössä työskenteli 900-henkilöä Suomessa, 550 Suomesta edustustoihin lähetettyä työntekijää.

Kuvio 1 ulkoministeriö lukuina 2016 (ulkoministeriö 2016).

Tämän lisäksi ulkohallinnon palveluksessa on yhteensä 980 asemamaasta palkattua työntekijää. Asemamaasta palkatut työntekijät ovat joko asemamaassa asuvia Suomen kansalaisia tai asemamaansa kansalaisia.

4.1 Ulkoministeriön ja ulkoasianhallinnon toimintaympäristö

Ulkoministeriön toimialaan valtionhallinnossa kuuluvat ulko-, turvallisuus- ja kehityspolitiikka. Ulkoasianministeriön tehtävänä on myös avustaa muita hallinnonaloja kansainvälisten asioiden yhteensovittamisessa tehtävänkuvaansa. Ulkoministeriön tavoitteena on palvella hyvin suomalaisia, suomalaista talouselämää ja yhteiskuntaa, tasavallan johtoa ja eduskuntaa. Ulkoministeriö vastaa oman toimialansa puitteissa valtioneuvostolle kuuluvien asioiden valmistelusta ja oman hallinnonalansa toiminnasta. (Ulkoministeriö 2018.)

Edustustojen keskeiset tehtävät perustuvat ulkoasianhallintolakiin ja – asetukseen, Wienin yleissopimukseen ja vakiintuneisiin käytäntöihin. Ulkoministeriö edesauttaa Suomen ja suomalaisten etuja maailmalla. Toimenkuvaan kuuluu ulkopolitiikkaa, kauppapolitiikkaa, kehitysyhteistyötä, Suomen edustamista toisissa maissa ja kansainvälisissä järjestöissä, maakuvatyötä,

konsulipalveluita ja kansalaispalveluita. Ulkoministeriön edustustoilla on myös tärkeä rooli kriisitilanteissa valmiussuunnittelijana sekä kriisiviestijänä. (Ulkoministeriö 2018.)

Ulkoministeriön ulkosuhteiden hoitamisen väline on diplomatia, jolla on yhtä pitkä historia kuin valtioiden välisellä kaupalla tai sodilla. Diplomatia on Berridgen (2002, 1) mukaan olennaisesti poliittista vaikuttamista, joka taitavasti suoritettuna on merkittävän vallan väline. Diplomatian tarkoitus on mahdollistaa valtioiden ulkopoliittisten tavoitteiden saavuttaminen turvautumatta voimaan, propagandaan tai lainsäädäntöön. (Berridge 2002, 1.) Wienin yleissopimus (4/1970) kirjasi sopimuksen muotoon jo traditioksi muodostuneet diplomatian pelisäännöt muun muassa virallistamalla suurlähetystöjen aseman, sekä lähetettyjen diplomaattien erityisaseman paikallisen lainsäädännön silmissä (Berridge 2002, 112).

Tietoturva diplomatiassa liittyy keskustelujen ja erinäisten ulkopoliittisia suhteita käsittelevien asiakirjojen salassapitoon, johon tietotekniikan kehitys ja vakoiluun sopivien laitteiden kutistunut koko on luonut omat haasteensa (Aarnio 2017; Puhakainen 2017). Edustuston päälliköt ja poliitikot tarvitsevat aiempaa kehittyneempää turvallisuustietoisuutta etenkin tapaamisissa, joita järjestetään edustustojen ulkopuolella, kuten esimerkiksi Ranskan presidentti Macron sekä Saudi-Arabian kruununprinssi Mohammed bin Salmon havaitsivat G20-kokouksessa Buenos Airesissa (Helsingin Sanomat 2018.)

4.2 Ulkoministeriön tietoturvatoiminta

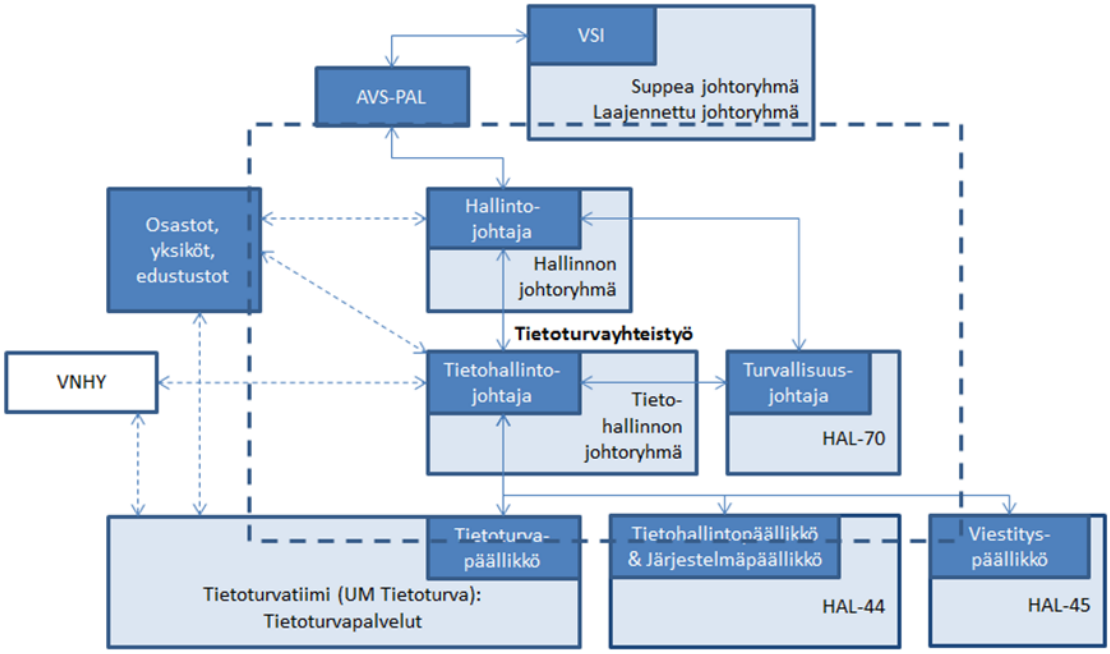
Ulkoasianministeriön työjärjestykseen (550/2008) sekä päätökseen tietoturvallisuudesta ulkoasianhallinnossa perustuva kuvaus tietoturvatoiminnan organisoinnista, vastuista ja tehtävistä määrittää jokaisen toiminnon vastuulliseksi huomioimaan tietoturvavaatimukset ja -tarpeet omalla vastuu- ja tehtäväalueellaan. Toimintojen on tunnistettava osa-aluekohtaiset tarpeensa, sekä suojattavat kohteensa. Turvallisuuteen liittyvät vastuuhenkilöt on nimettävä, toimintaan kohdistuvat uhkat tunnistettava ja niitä vastaan suoritettava riskiarviointi. Tämän lisäksi toiminnoilla on vastuu huolehtia tarvittavien kontrollien määrittelystä, suunnittelusta, toteuttamisesta, toimeenpanosta, tuesta ja ylläpitämisestä, seurannasta ja valvonnasta (Ulkoasianministeriön työjärjestys 550/2008).

Työjärjestyksen listaamat tehtävät ja vastuut perustuvat Valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010), jossa säädetään viranomaisia koskevista yleisistä tietoturvallisuusvaatimuksista, asiakirjojen turvallisuusluokituksen perusteista sekä luokiteltujen asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista. Tietoturva-asetus täydentää osaltaan vuodelta 1999 voimassa olevaa lainsäädäntöä viranomaisen toiminnan julkisuudesta (621/1999).

Asetus määrittää tietoturvallisuuden perustason ja antaa sille lukuisia vaatimuksia, joista useampi käsittelee tietoturvaosaamista ja tietoturvatietoisuutta: Viranomaisen käytössä on

oltava riittävä asiantuntemus tietoturvallisuuden varmistamiseksi, tietoturvallisuuden hoitamista koskevat tehtävät ja vastuut on määritelty, henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä. Annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti. (2010/681).

Kokonaisvastuu (kuvio 2) osoittaa tietoturvayhteistyötoiminnan ulkoministeriössä raportointisuhteineen. Vastuu ulkoministeriön tietoturvatyön toimintaedellytyksien luomisesta on valtiosihteerillä. Ulkoministeriön työjärjestyksen mukaan tietohallintojohtaja on vastuussa tietoturvallisuudesta yhdessä turvallisuusjohtajan kanssa. Tietoturvapäällikkö, tukenaan tietoturvatiimi, vastaa tietohallintojohtajan mandaatilla operatiivisesta tietoturvatoiminnasta. Kunkin osaston, yksikön, edustuston, hankkeen ja projektin ollessa velvollisia tunnistamaan oman vastuualueensa tarpeet ja huolehtimaan sen turvallisuudesta (Ulkoministeriön tietoturvapolitiikka 2011).



Kuvio 2 tietoturvatoiminnan organisointi ja raportointisuhteet (Ulkoministeriön tietoturvapolitiikka 2011)

4.3 Ulkoministeriön ja edustustojen esimiesten rooli tietoturvallisuudessa

Ulkoasiainministeriön työjärjestys (2008/550) ja sen pohjalta luotu tietoturvatoiminnan organisointi, vastuut ja tehtävät kuvaus linjaa, että jokainen työntekijä on vastuussa tietoturvallisuudesta omassa työtehtävässään. Jokaisen työntekijän tietoturvallisuuteen liittyvien vastuiden lisäksi esimiesroolissa toimiville on määrätty erinäisiä erityisvastuita. Näitä ovat mahdollistaa resursoimalla tarvittavat rahalliset ja ajalliset edellytykset alaisten tietoturvallisen työn

mahdollistamiseksi sekä koulutuksiin osallistumiseksi. Toiminnan ja ohjeiden noudattamisen valvonta ja tarvittaessa asioihin puuttuminen. Esimiehelle kuuluu myös havaitsemistaan tai hänelle raportoiduista tietoturvallisuutta vaarantavista seikoista ja epäilyistä ilmoittaminen tietoturvapäällikölle tai tietoturvapäivystäjälle. Tämän lisäksi esimiehen on noudatettava itse tietoturvaohjeita ja toimittava näin hyvänä esimerkkinä alaisilleen. Taulukossa 1 kuvataan eri roolien tietoturvaroolit ja -vastuut ulkoministeriössä. Taulukossa on erikseen huomioitu esimiesasemassa toimivan vastuualue, tietoturvatehtävät ja tarvittavat tietoturvapätevyydet. (Ulkoministeriön tietoturvapolitiikka 2011.)

Rooli / Toimija	**Vastuualue**	**Tietoturvatehtävät**
Esimiesasemassa toimiva henkilö	□ Oman vastuu- ja tehtäväalueen tietoturvallisuus	□ Tietoturvavaatimusten ja -tarpeiden huomioon ottaminen esimiestyössä □ Henkilöstön tietoturvatietoisuuden varmistaminen □ Toiminnan ja ohjeiden noudattamisen valvonta ja tarvittaessa asioihin puuttuminen □ Hyvänä esimerkkinä toimiminen
Jokainen ministeriön tai edustuston henkilöstöön kuuluva tai sen toimeksiannosta tai yhteistyökumppanina toimiva henkilö	□ Tietoturvallisuus omissa työtehtävissä	□ Tietoturvavaatimusten ja -tarpeiden huomioon ottaminen päivittäisissä työtehtävissä □ Perehtyminen itseään ja vastuualuettaan koskeviin tietoturvavaatimuksiin, kuten normeihin ja ohjeisiin □ Osallistuminen tarjottuun tietoturvakoulutukseen □ Toiminta tietoturvavaatimusten ja -tarpeiden mukaisesti □ Havaitsemistaan tietoturvallisuutta vaarantavista seikoista ja epäilyistä ilmoittaminen joko esimiehelleen, kohteen vastuuhenkilölle, tietoturvapäällikölle tai tietoturvapäivystyksestä vastaavalle taholle

Taulukko 1 Yleinen tietoturvarooli ja esimiehen tietoturvarooli

Ulkoasianministeriön työjärjestykseen (550/2008) sekä ulkoministeriön tietoturvapolitiikkaan eli Päätökseen tietoturvallisuudesta ulkoasianhallinnossa (2014) perustuva kuvaus tietoturvatoiminnan organisoinnista, vastuista ja tehtävistä määrittää tietoturvallisuuden jokaisen ministeriössä työskentelevän vastuulle. Jokaisen on perehdyttävä itseään ja vastuualuettaan koskeviin tietoturvavaatimuksiin, osallistuttava tarjottuihin koulutuksiin, otettava tietoturvavaatimukset- ja tarpeet huomioon päivittäisessä työssään sekä raportoitava tietoturvallisuutta

vaarantavista seikoista esimiehelleen, kohteen vastuuhenkilölle tai tietoturvasta vastaaville asiantuntijoille. Korotettu tietoturvarooli organisaatiossa kuuluu esimiesasemassa toimiville henkilöille. Heidän vastuullaan on henkilöstönsä tietoturvallisuuden varmistaminen, toiminnan ja ohjeiden noudattamisen valvonta sekä mahdollisesti tärkeimpänä kohtana hyvänä esimerkkinä toimiminen.

Ulkoministeriössä johto sitoutuu kiitettävästi tietoturvatyöhön ja sen toteutumiseen ja on määrittänyt vastuuroolit esimies- ja henkilöstötasolla. Organisaation osastoille, yksiköille ja toiminnoille löytyvät nimetyt vastuuhenkilöt ja tietoturvatoiminta kattaa kaikki keskeiset hallinnolliset toiminnat. Tietoturvallisuuden suunnittelu tietoturvatiimissä tapahtuu vuosisuunnitteluna, joka integroituu toiminnan- ja talouden suunnitteluun. Vuosisuunnittelussa ulkoministeriön johto huomioi tietoturvallisuuden tarvitsemat resurssit, kehittämistoimet ja budjetoi aiheutuneet kustannukset. Tietoturvallisuuden seurantaan ja raportointiin kiinnitetään huomiota. (Vahti 2/2011; Savolainen 2018).

5 Johtamisen yhteys organisaatiokulttuuriin

Virkamiesten toimintaan vaikuttavat ylhäältäpäin välitetyt ohjeet ja määräykset, joita katsotaan viraston tai organisaation kulttuurin lasien lävitse. Valtionhallinnon hallintokulttuurissa normit ja käytännöt välittyvät taas vahvasti vanhemmalta virkamiespolvelta nuoremmalle. (Savolainen 2015.) Kulttuuri tarkoittaa sivistystä, viljelyä, ihmisten perustarpeiden tyydyttämistä, ihmisen toimintaa ja sen tuotteita tieteissä, tekniikassa ja uskonnossa. Kulttuuri tarkoittaa myös ihmishengen jalostamista ja jonkin ryhmän tai kansan kokonaissuorituksia (Uusi sivistyssanakirja 1993, 365.) Kulttuuri luo ajatusrakennelmia, jotka pohjautuvat arvojärjestelmiin, jotka ilmenevät kulttuurin jäsenten sanojen ja tekojen kautta. Kollektiivisesti kulttuurissa sen jäsenet jakavat yhteisiä arvoja ja tulkintoja asioista, luoden ryhmälle yhteneväisen, ja muista eroavan identiteetin, pelisäännöt sekä ilmapiirin. Kulttuurin osia ovat sen jäsenten käyttäytymistä ohjaavat arvot ja käsitteet sekä organisaation jäsenten näkyvä toiminta. Toiminta voi olla käyttäytymistä tai yhtenevä puhetapa. (Schein 1984, 24).

Roerin (2015, 8-9) mukaan kulttuuri on pitkälti opittua käyttäytymistä. Yksinkertaisena esimerkkinä hän esittää sen, millä tavalla ihmiset kävelevät ja miten kävelytavat eroavat eri puolella maailmaa. Läntisessä maailmassa suurin osa meistä käyttää kenkiä, koska ne suojaavat jalkoja. Osa naisista käyttää korkokenkiä, joilla käveleminen ei ole kovinkaan luonnollista. Afrikasta taas löytyy heimoja, jotka katsovat kävelemisen olevan ajan tuhlausta ja pyrkivät juoksemaan. (Roer 2015, 8-9.)

Scheinin (1987) mukaan johtajat luovat johtamiskulttuuria muun muassa kiinnittämällä järjestelmällisesti huomiota tietyntyyppisiin asioihin. Schein katsoo kulttuurin luomisen, hallinnoimisen olevan johtajan tärkeimpiä velvollisuuksia. Toisaalta hän myös toteaa, että kulttuuri vaikuttaa vähintään yhtä paljon johtajaan kun johtaja vaikuttaa kulttuuriin.

Ulkoministeriössä esimiestehtävissä toimivia virkamiehiä on suhteellisesti huomattavan paljon vähemmän kuin ulkomaan edustuksessa. Ulkoministeriön erityispiirteenä on myös diplomaattiura, joka kestää 30-45 vuotta. Ulkoministeriössä suurin osa ylimmän johdon tehtävistä on osa diplomaattiuraa ja tiettyihin virkanimikkeisiin, kuten valtiosihteerin, alivaltiosihteerin sekä osastonpäällikön että ulkoasiainhallinnon tarkastajan tehtäviin voidaan ulkoasiainhallintoasetuksen (256/2000, 5 § ja 9 §) mukaan valita ainoastaan diplomaattiuralainen. Valtioneuvoston periaatepäätös sallii johtotehtävissä avoimen haun, ja sen perusteella diplomaattiuran ulkopuolelta on mahdollista valita myös ulkopuolinen henkilö ulkoministeriön johtotehtäviin. Tähän mennessä menettely on ollut poikkeuksellista, joten lähes kaikilla ulkoministeriön esimiehillä on usean kymmenen vuoden kokemus ministeriön virkakulttuurista ja toimintatavoista (Ulkoasiainministeriön esimieskäsikirja 2017.)

Ulkoasiainhallinnossa vallitsee tehtäväkohtainen urakierto, joka johtajapolitiikan linjauksen mukaan jäntevöittää johtamista sekä korostaa tulosvastuullisuutta. Diplomaattiuran tehtäväkierrossa toimikaudet ovat tyypillisesti muutaman vuoden mittaisia vaihteluvälin ollessa noin 2-7 vuotta. Siirtymävelvollisuus varmistaa sen, että johtotehtävät vaihtuvat säännöllisesti. Ulkoministeriöllä on esimieskunnalle tarkoitettu johtamisvalmennus. Ennen ensimmäistä esimiestehtävää virkamies käy lävitse ministeriön oman esimiehen peruskoulutuksen. Ministeriö järjestää myös ajoittain erillisiä esimiesfoorumeita, joissa käydään lävitse ajankohtaisia johtamiseen liittyviä kysymyksiä ja teemoja. Edustustojen päälliköt ovat muista ulkoministeriön johtajista erottuva esimiesryhmä. He toimivat hyvin heterogeenisen työntekijäjoukon esimiehinä. Heille järjestetään lisäksi tehtäväkohtaista esimieskoulutusta suurlähettiläspäivien yhteydessä (Ulkoasiainministeriön esimieskäsikirja).

Ulkoministeriön johtajuusvisio asettaa seuraavat vaatimukset toimeenpanevalle, tavoitteelliselle ja tulokselliselle johtajalle: Johtajan täytyy ymmärtää toimintayksikkönsä tehtävä, rooli ja merkitys suhteessa ministeriön tavoitteisiin sekä laajempiin kansallisiin tavoitteisiin ja asettaa yksikölleen kokonaisuuden pohjalta selkeät tavoitteet. Johtaja ohjaa toimintayksikköään asetettujen tavoitteiden saavuttamiseksi. Johtaja uskaltaa tehdä kokonaisuuden ja tavoitteiden kannalta toimivia päätöksiä ja pystyy osoittamaan tekemiensä päätösten perusteet. Johtaja ottaa kokonaisvastuun toimintayksikkönsä toiminnasta. (Ulkoministeriön Johtajuusvisio 2011.)

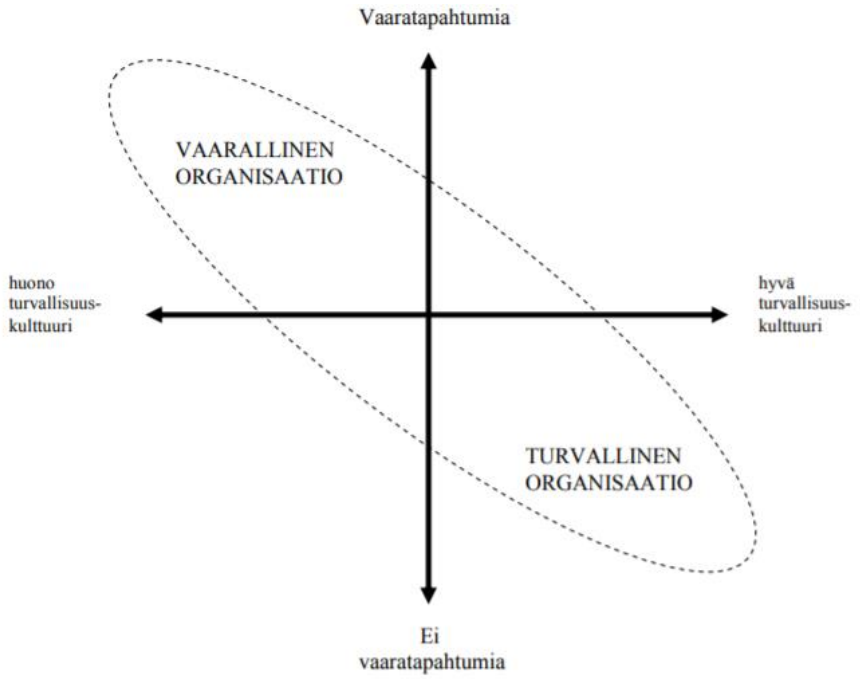
6 Turvallisuuskulttuuri ja sen kehittäminen

Meidät on sosiaalisina olentoina rakennettu luontaisesti ryhmittymään ja toimimaan muiden henkilöiden kanssa. Psykologien mukaan tarpeemme luoda ryhmiä on yksi perusvaistojamme. Ihmiset ovat syntymästään saakka useiden eri ryhmien jäseniä olipa kyse perheestämme, käymistämme kouluista tai työyhteisöistämme. Mitä laajempi ja monimutkaisempi työyhteisön organisaatio on, sitä enemmän sosiaalisia ryhmiä sen sisälle syntyy. Käyttäydymme luontaisesti epäilevästi ja jopa vihamielisesti ryhmämme ulkopuolisia kohtaan. Tämän vuoksi ne

organisaatiot, joilta puuttuu voimakas organisaationlaajuinen yhteenkuuluvuuden tunne, altistuvat helposti sisäiseen lokeroitumiseen ja jakautumiseen pienempiin sosiaalisiin ryhmiin. Tässä asetelmassa epäluuloisuus, vihamielisyys ja muutosvastarinta korostuvat, myös turvallisuuteen liittyvissä asioissa. Kyky luoda organisaation kattavaa turvallisuuskulttuuria tai jalkauttaa turvallisuusohjeistuksia on suoraan verrannollinen siihen katsotaanko turvallisuusorganisaatio osaksi työyhteisöä vai ei. (Roier 2015, 55-60.)

Roierin mukaan turvallisuuskulttuurin kehittäminen vaatii erillistä kehittämisohjelmaa. Kehittämisohjelman markkinointi vaatii vahvaa yhteistyötä henkilöstöosaston ja viestintäosaston kanssa, sekä uuden organisaation ristiin kattavan uuden sisäisen turvallisuuskulttuuria levittävän sosiaalisen ryhmän luontia. Tässä asetelmassa voimme hyväksikäyttää ihmisen luontaista ryhmittymisen halua ja kattaa vaikutuksemme alle ne sidosryhmät, joiden edustajat kutsumme turvallisuuskulttuuria kasvattavan ryhmän jäseniksi. (Roier 2015, 60-61).

Organisaatio, jolla on terve turvallisuuskulttuuri, on luontaisesti vähemmän altis vaaratapahtumille. Reimanin (2008) mukaan turvallisuuskulttuurilla ja vaaratapahtumilla, joita ovat tapahtuneet onnettomuudet sekä niitä usein edeltävät läheltä-piti-tilanteet omaavat selkeän korrelaation. Kuvio 3 osoittaa, että hyvän turvallisuuskulttuurin seurauksena on vähäinen määrä vaaratapahtumia.



Kuvio 3: Turvallisuuskulttuurin ja vaaratapahtumien suhde (Reiman 2008, 85)

Läheltä piti tapahtumat eivät liity ainoastaan työturvallisuuteen. Tietoturvallisuudessa läheltä piti tapauksia voivat olla esimerkiksi salassa pidettävää tietoa sisältävä asiakirja, joka arkistoidaan turvaluokittelemattomaan säilytystilaan tai toimiston monitoimilaite, jota on kutsuttu huoltamaan taustaselvittämätön huoltomies. Tulostavoitteena turvallisuusohjelmalla voi olla esimerkiksi onnistuneiden phishing-hyökkäysten vähentäminen 50%:lla. Jotta tavoitteita voidaan mitata, on ensin selvitettävä organisaation nykytila sekä tavoiteltava tila. Kun tulostavoite on selvillä, on ymmärrettävä mitä oppimistavoitteita vaaditaan tulostavoitteen saavuttamiseksi. Minkälaista koulutusta ja ohjeistusta ohjelman piirissä oleva henkilöstö vaatii, jotta he voivat saavuttaa tavoitellun tulostavoitteen. (Roier 2015, 82-84).

Ohjelmassa on tärkeätä analysoida kohderyhmä. Eri osastojen ja etenkin ulkomaisten toimintojen osalta niissä työskentelevät voivat katsoa kuuluvansa omaan erityiseen sisäryhmäänsä. Phishing-esimerkissä on järkevää analysoida hyökkäystyypille kaikkein haavoittuvimmat kohderyhmät. Roer esittää kahden kohderyhmän luontia: liikefokusryhmän (ylempi johto sekä keskijohto) ja insinöörifokus (patenttilakimiehet, insinöörit ja suunnittelijat ja heidän avustajansa). Vaikka molemmat ryhmät ovat selkeästi kohde spear-phishingille eroavat heidän tietotaitonsa ja kiinnostuksen kohteensa toisistaan. Vaikka turvallisuustietoisuusohjelman tavoitteet pysyvät samoina, on tärkeätä löytää molemmille kohderyhmille oikea kommunikointitapa ja lähestymiskulma. Mitä paremmin kohderyhmän kiinnostuksenkohteet, fokus ja nykyiset tietotaidot tunnetaan sitä paremmat mahdollisuudet ohjelmalla on onnistua. Roer suosittelee konsultoimaan kohderyhmien edustajia ja pyytämään heitä avustamaan turvallisuustietoisuusohjelman toteuttamisessa. Dialogissa turvallisuusosasto voi oppia paljon uutta ja luomaan lämpimämmät suhteet kyseisiin kohderyhmän edustajiin. (Roier 2015, 88-89). Avain hyvän turvallisuuskulttuurin luomiseen ja ylläpitämiseen on ymmärtää, että ihmiset ovat yksilöitä ja turvallisuutta kehittävät toiminnat on muokattava heidän tarpeidensa, taustansa ja tietämyksensä ympärille. (Roier 2015, 55.)

6.1 Turvallisuustietoisuuden kehittymisen vaatimuksia

Siponen (2000) luettelee logiikan, moraalin ja eettisyyden, rationaalisuuden, tunteellisuuden, painostuksen ja rangaistukset, turvallisuuden tunteen sekä hyvinvoinnin käytännön käyttäytymistiedeteorioiden esittämiksi lähestymistavoiksi, joita voidaan soveltaa myös tietoturvallisuustietoisuuden ja ohjeiden noudattamisen saralla. Siponen (2000) väittää, että käyttäytymiseen vaikuttavat lähestymistapojen täytyy täyttää käyttäytymistieteiden vaatimukset, ja vastata loppukäyttäjille miksi heidän tulisi noudattaa tietoturvallisuusohjeita.

Puhakaisen (2006 ; 2017) mukaan testattu hypoteesi on, että tietoturvallisuuden kehittämiseen tähtäävä koulutus parantaa työntekijöiden tietoturvallisuusohjeiden noudattamista. Esimiesten asenteisiin vaikuttaa taas luonnollisesti eniten näiden esimiesten asenne tietoturvallisuusohjeiden noudattamiseen. Muita vaikuttavia seikkoja ovat ympäristö, työkalut, ohjeiden laatu, koulutukseen panostaminen. Turvallisuusajattelun kehittämiseen toimivia keinoja on

empiirisesti todennettu ainoastaan rangaistustoimenpiteiden vaikutuksesta organisaatioissa. On olemassa kahdenlaisia organisaatioita: A-tyypin organisaatioita, joissa esimies kaitsee lapsiaan ja B-tyypin organisaatioita, joissa esimies tukee alaisiaan ja työtä tehdään tasavertaisina. Sanktioita on tutkittu kohtuullisen paljon ja niillä on taipumus muuttaa B-tyypin organisaatio A-tyypin organisaatioksi. Etenkin virkamiehet, jotka toimivat virkavastuulla tekevät asioita vain, jos on täysi varmuus, ettei niitä tehdä väärin. Sanktioilla on paljon negatiivisia sivuvaikutuksia, joista yksi on opittu avuttomuus. (Puhakainen 2017).

Räty (2018) alleviivaa sitä, että esimiesten puolelleen voittaminen vaatii heidän asemansa ymmärtämistä. Heillä on enemmän vastuuta, joten he tarvitsevat myös syvempää ymmärrystä turvallisuustilanteesta. Räty myös kehottaa vahvistamaan oman asiantuntijaorganisaation viestiä, kutsumalla vierailevilla puhujia, jotka edustavat esimerkiksi suojelupoliisin ja viestintäviraston kaltaisia auktoriteetteja.

”Koska virkamiehet toimivat virkavastuulla heille on tyypillistä että asioita ei tehdä jos on vaara tehdä asioita väärin. Sanktioiden esiin tuominen vain pahentaa sitä ja vie asioita aina vaan pahempaan suuntaan. Rankaisun uhkailulla ja rankaisulla on paljon sivuvaikutuksia, vaikka se toimisikin. Yksi niistä on opittu avuttomuus. Eli älä tee mitään, jottei tule rangaistusta.” (Puhakainen 2017.)

Empiiristä todistusaineistoa käytännön koulutuksien, kampanjoiden ja palkitsemisen toimivuudesta löytyy kuitenkin muilta aloilta kuin tietoturvallisuuden alalta. Koulutusta on käytetty onnistuneesti mm. AIDS-tietoisuuden kehittämiseksi, ja turvallisuuskampanjoita käytöksen muutoksessa maantieturvallisuuteen liittyen. (Puhakainen 2006, 69.)

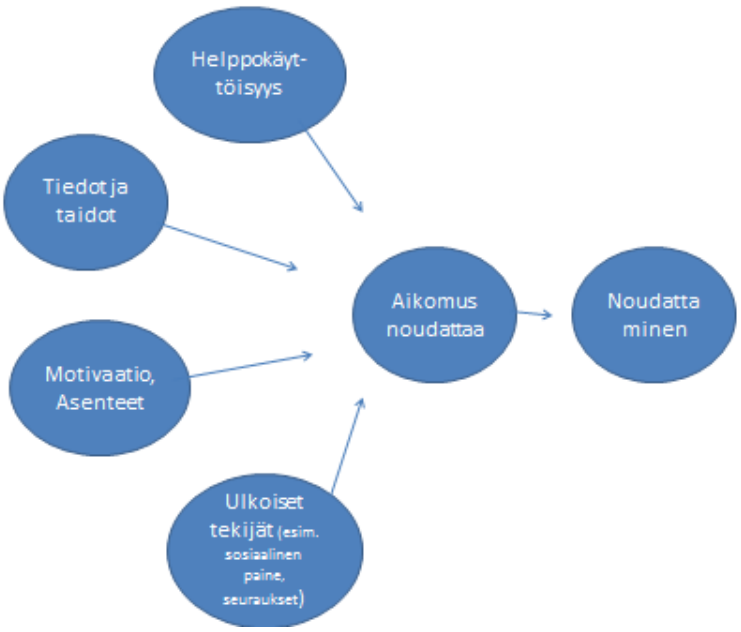
Puhakainen (2006, 71-73) tuo esille turvallisuustietoisuuden kehittymiseen liittyen tietoturvallisuuden suunnitteluteorian (Design theory features for Information security awareness training). Teoriaan liittyy prosessoinnin todennäköisyysmalli (elaboration likelihood model), joka tunnistaa kaksi tiedon sisäistämistapaa: kognitiivisen prosessoinnin (cognitive processing) sekä oikopolut (cues). Näistä kognitiivinen prosessi vaatii tiedon vastaanottajalta syvempää ajattelua sekä ymmärtämistä. Vihjeiden sisäistämisessä tiedon vastaanottaja, joka voi olla esimerkiksi tietoturvallisuuskoulutusta kuunteleva työntekijä, taas vastaanottaa passiivisesti tietoa ja esityksen ulkoiset tekijät, kuten tiedon esittäjän vakuuttavuus, tietoa tukemaan esitetyt tilastot ja käyrät, riittävät kuuntelijan vakuuttamiseksi. Kuuntelija ei tällöin henkilökohtaisesti käsittele, eikä arvioi vastaanottamaansa tietoa mielessään vaan hyväksyy sen pinnallisesti. Kognitiivisessa prosessissa tiedon vastaanottaja käsittelee ja omaksuu tarjotun tiedon ja sen perustelun ytimen, pyrkien käsittelemään ja ymmärtämään sitä aiempien tietojensa pohjalta. Prosessoinnin jälkeen henkilölle hyväksyy tarjotun tiedon ja hylkää sen. Puhakaisen mukaan toisin kuin kognitiivisessa prosessissa, tiedon sisäistäminen oikopolkujen pohjalta ei johda luotettavaan tottumusten ja tapojen muuttumiseen. Puhakaisen mukaan Kognitiivinen

prosessi vaatii tiedon vastaanottajalta tarpeellista henkilökohtaisia kykyjä sekä motivaatiota aihealueen sisäistämistä kohtaan. (Puhakainen 2006, 71-73.)

Halibozek & Kovavichin mukaan työntekijöiden täytyy ymmärtää velvollisuutensa organisaation tiedon ja omaisuuden suojelemiseksi. Heidän mukaansa turvallisuustietoisuuden kehittäminen on kuin mikä tahansa tuote, joka on kaupattava asiakkaille käyttämällä myynnistä ja markkinoinnista tuttuja tekniikoita (2017, 273). Petty ja Cacioppo (1986) tunnistavat kolme tekijää, jotka vaikuttavat oppijan motivaatioon: Tiedon henkilökohtainen merkitys oppijalle, perustelun laaja tietopohja, kuten tiedon pohjautuminen useisiin lähteisiin, sekä sisäinen pyrkimys harjoittaa kriittistä ajattelua. Henkilön motivaatiot voivat toisaalta olla myös vahvoja, mutta suorassa konfliktissa keskenään. Alasuutari (2016) toteaa että tietoturvallisuudessa nämä motiivit voivat olla halu toimia turvallisesti ja turvallisuusohjeistojen mukaan, sekä toimia mahdollisimman nopeasti ja tehokkaasti.

6.2 Mistä virheet tietoturvaohjeiden noudattamisessa johtuvat

Tutkijat ovat havainneet kolme eri vaikutusvoimaa, jotka vaikuttavat työntekijän työsuoritukseen. Eri vaikutuksia on satoja, mutta ne voidaan kaikki sijoittaa kategorioihin: ympäristö ja työkalut, taidot ja tietämys sekä motivaatio, asenteet ja kannustimet. (Roper & Grau 2006, 29.) Ympäristö-vaikuttimista yleisin on aika, tai kuviteltu ajan puute. Tietoturvallisuuskontrollit hidastavat työntekoa ja lisäävät siihen välivaiheita. Tästä esimerkkejä ovat esimerkiksi tietojärjestelmät pääsynhallinnan, esim. salasanan, takana ja tiedon pääsyn rajoittaminen tietoa luokittelemalla. Vuorinen (2014) kuvaa väitöskirjassaan kuvaavasti tietoturvallisuuden olevan kitkaa aiheuttava energiaa syövä parasiitti. Jos työn suorittaminen turvallisesti hidastaa työn tekoa liiaksi, työntekijä luo oikopolun suorittaakseen työnsä tehokkaasti. Muita ympäristövaikutteita voivat olla puutteelliset työkalut tai yksinkertaisesti se, ettei työympäristö sovellu työsuoritteeseen. (Roper & Grau 2006, 31-36.)



Kuvio 4: Ohjeistuksen noudattamisen edellytyksiä (Puhakainen 2006; Roper & Grau 2006).

Taidoissa ja tietämyksessä olevat puutteet saa korjattua koulutuksella. Oleellisia asioita ovat: mitä pitää tehdä, kuka tekee, missä tilanteessa tehdään ja lopulta, kuinka asiat tehdään oikeaoppisesti? Tiedon puute liittyen yhteenkin oheisista kysymyksistä voi saattaa työsuoritteen epäonnistumiseen (Roper & Grau 2006,32.) Siposen motivaatio on luonteeltaan dynaaminen ja lyhytaikainen. Motivaation kesto voi vaihdella minuuteista viikkoihin, kun taas henkilön asenteet ovat tätä pysyvämpiä. Asenne liittyy toiminnan laadukkuuteen ja motivaatio toiminaan aktiivisuuteen (Siponen 2000,33.) Turvallisuuspuutteet, jotka liittyvät motivaatio ja asenneongelmaan ja jotka saavat työntekijän epäonnistumaan työtehtävässään eivät Roperin & Graun mukaan korjaannu koulutuksen avulla. Motivaation korottaminen vaatii joko uusia kannustimia tai vastakkaisesti henkisten ärsykkeiden ja esteiden poistamista.

Dinev & Hu (2007) ovat puolestaan hyödyntäneet kyselyssään Theory of planned behavior -teoriaa tarkoituksenaan selvittää, mitkä seikat vaikuttavat tietokoneenkäyttäjän aikomukseen käyttää suojaavia teknologioita esimerkiksi vakoiluohjelmia vastaan. Tutkimuksessa tehdyn kyselyn tulokset osoittivat, että aikomukseen käyttää suojaavia teknologioita vaikuttaa tietoisuus niistä uhkista, joita negatiiviset teknologiat, kuten vakoiluohjelmat tuovat mukanaan. Pyrkimyksenään selvittää tekijöitä jotka edistävät tietoturvakäyttäytymistä organisaatioissa Herath & Rao (2009) ovat hyödyntäneet principal agent-teoriaa, sekä socio-ekonomista teoriaa vaatimustenmukaisuudesta ja yleisestä ehkäisevästä vaikutuksesta (socio-economic theory of compliance ja general deterrence). Tuloksena oli, että tietoturvakäyttäytymiseen vaikuttavat sekä sisäiset ja ulkoiset motivaatiotekijät. Sisäisiä tekijöitä ovat työntekijän tietoisuus heidän toimintansa vaikutusmahdollisuuksista tietoturva loukkauksia vastaan kuten

kyky havaita tietoturvauhkia sekä toimia hyödyllisesti uhkaavassa tilanteessa. Ulkoisia käyttäytymiseen vaikuttavia motivaattoreita havaittiin olevan sosiaalinen paine ja työtovereiden käytös turvallisuusasioissa.

Siponen (2000, 36) puhuu ennaltaehkäisevän tietoisuuden merkityksestä tietoturvallisuudessa. Tietoturvallisuustyössä loppukäyttäjien, halutaan sisäistävän tietoturvallisuusohjeistukset, ja katsovan niiden täytäntöönpanon olevan osa työnantajaltaan saamaansa työroolia ja täten jopa moraalinen velvollisuus. Siposen mukaan tämän sisäistämisen edellytyksenä on se, että työntekijä katsoo turvallisuusohjeet moraalisesti hyväksyttäviksi ja niiden tavoitteet toivottaviksi.

Tietoturvallisuuden huomiointi joka päiväisessä työssä vaatii muutosta aiempiin tottumuksiin ja työtapoihin. Ulkoministeriön ohje esimiehille käsittelee muutosvastarintaa seuraavasti: Muutos-vastarinta estää yleensä uuden oppimista. Se on lähtökohta ja haaste esimiehelle. Muutosvastarinnan käsittelyssä tulisi välttää suoraviivaista ja automaattista reagointia. Muutoksen hyväksyminen lähtee eri käsitysten yhdistymisestä. Muutosvastarinnan murtaminen edellyttää vastarinnan syiden ymmärtämistä (Ulkoministeriön esimieskäsikirja 2017.) Viestintä muutosvastarinnan murtamisessa esittää keinoiksi monipuolisen, ajankohtaisen, oikein kohdistetun tiedon jakamisen, henkilöstön kuulemisen ja avoimuuden. Luottamus katsotaan tärkeäksi, jotta muutokselle annetaan mahdollisuus.

Gaunt (2000, 152) esittää että suurin uhka organisaation tietoturvalle on sen henkilökunta. Tämän vuoksi henkilökunnan asenteet ovat pääroolissa tietoturvatoiminnan onnistuneessa toteuttamisessa. Tämän vuoksi kaikkien henkilökunnan jäsenten pitäisi olla tietoisia, hyväksyä ja ymmärtää ne syyt, jotka johtavat tiedon turvaamisen tarpeeseen. Gaunt (2000, 154) myös esittää, että tärkein yksittäinen keino vaikuttaa henkilökunnan asenteisiin on saada päämielipiteen vaikuttajat demonstroimaan tukeaan tietoturvatoiminnalle.

Puhakainen (2017) muistuttaa, että valtionhallinto on hyvin hierarkkinen organisaatio. Organisaation johto katsoo helposti, että jos on ohjeita ja määräyksiä niin niitä noudatetaan kyselemättä. Tästä vastavoimana on henkilöstöä, jotka ovat tehneet samaa työtä 20 vuotta ja katsovat tietävänsä paremmin miten kyseistä työtä tehdään. Koska ohjeita on liikaa ei niitä kaikkia voi noudattaa.

6.3 Onnistuneen ohjeen ja koulutuksen piirteitä

Siposen mukaan turvallisuusohjeistuksissa on tärkeätä todistaa työntekijöille ohjeistuksen tarkoitus ja tarpeellisuus. Perusteluina voidaan käyttää selkeitä, kuuntelijalle tarpeellisia esimerkkejä (2000). Luoduille ohjeille ja sovelluksille, kuten turvallisuusohjeelle ja verkkokoulutukselle on asetettavat onnistumisvaatimukset. Produktin on sovittava käyttötarkoitukseen ja tarkoitetulle käyttäjäryhmälle, oltava helppokäyttöinen ja käytön on oltava miellyttävää.

Ulkoasun on oltava yhtenevä ja looginen. Kuvia, miellekarttoja ja graafisia mallinnuksia käytetään toistamaan ja korostamaan haluttuja asioita. (Sinkkonen & Kump 2006, 9.)

Sinkkonen & Kump (2006) korostaa miellyttävää käyttökokemusta. Käyttökokemuksen esteenä voi olla myös joukko yksittäin vähäisiä esteitä, kuten huono fontin valinta, kirjoituksen sekä kuvien huono kontrasti taustaan. Sinkkonen & kump (2006) mainitsee, että tutkimusten mukaan Ariel on kyselyiden perusteella käyttäjien mukaan yksi helpoiten luettavista fonteista. Fontti on myös Ulkoasiainhallinnon brändin mukainen. Lukijan näkösäde on korkeintaan 5 astetta, jonka perusteella hän kykenee kerralla lukemaan korkeintaan 15-16 kirjainta liikuttamatta päätään. (2006, 58). Oppikirjan osalta tietoa käytetään tekstin sijoittelussa.

Sinkkosen & kumpp (2006) mukaan tuotoksen prototyyppiä on järkevä testata käyttäjäryhmällä. Tämän osalta tietoturvakäsikirja lähetetään lausuntokierrokselle ulkoministeriön sisällä, ja sisältöä ja ulkoasua muokataan palautteen perusteella.

7 Opinnäytetyöprosessi

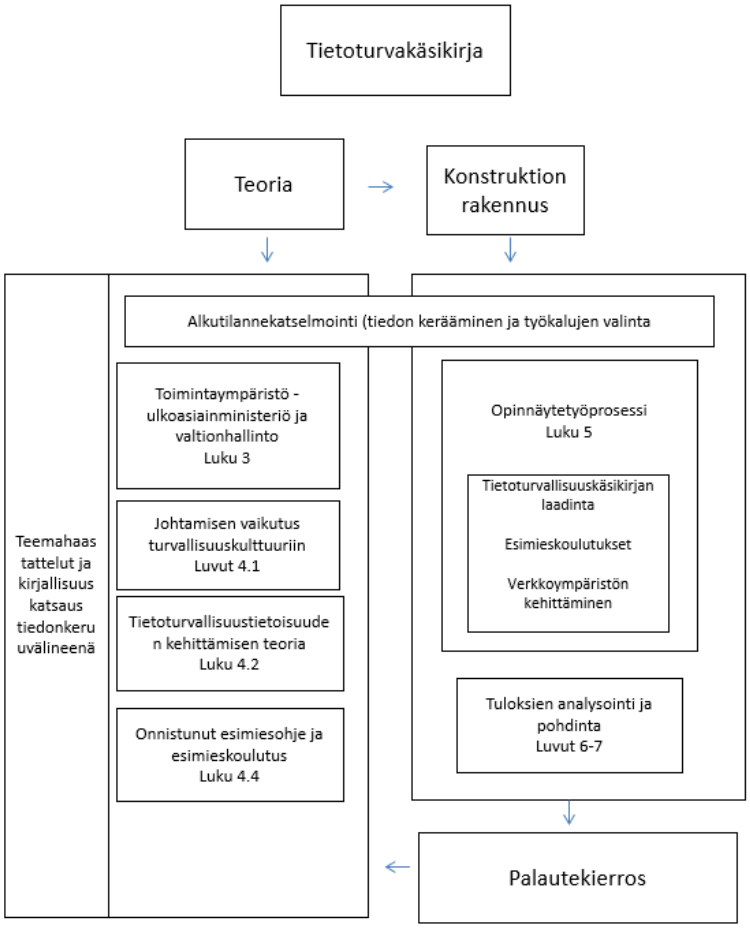
Opinnäytetyö-prosessin tarkastelu tapahtui konsultin näkökulmasta, siten että tutustuin ulkoministeriön työtapoihin, osana tietoturvatiimiä, perehtyen kahdeksan kuukauden ajan esimiesten ja muun henkilöstön työnkuviin, osallistuen viraston arkeen. Pyrin hakemaan oman käsitykseni arjen toimennasta ja peilaamaan sitä tietoturvan ja turvallisuusyksikön asiantuntijoiden näkökulmiin. Koska opinnäytetyö on julkinen asiakirjasta, sisältöä on rajattu, siten ettei se sisällä kohdeorganisaation luokiteltua tietoa. Myös joitain haastatteluista ja tapauksiin liittyviä tietoja on rajattu pois tästä dokumentista.

Opinnäytetyö (kuvio 3; Kuvio 4) suunniteltiin jakaantuvan seuraaviin prosessivaiheisiin: Orientaatio-, suunnittelu-, toteutus- ja julkaisuvaiheeseen. Orientaatiovaihe tapahtui toukokuussa 2017, jolloin kävin ensimmäiset keskustelut ulkoministeriön tietoturvapäällikkö Savolaisen kanssa harjoittelupaikasta tietoturvatiimissä ja valitsin opinnäytetyölle aiheen. Opinnäytetyö yhdistetään näin Laurean toisen työharjoittelun suorittamisen yhteyteen. Työskentelin viraston konsulttien kanssa avustaen heitä heidän työssään. Harjoittelun aikana aloitin opinnäytetyöprosessin suunnittelu, eli tiedonkeruuvaiheen.

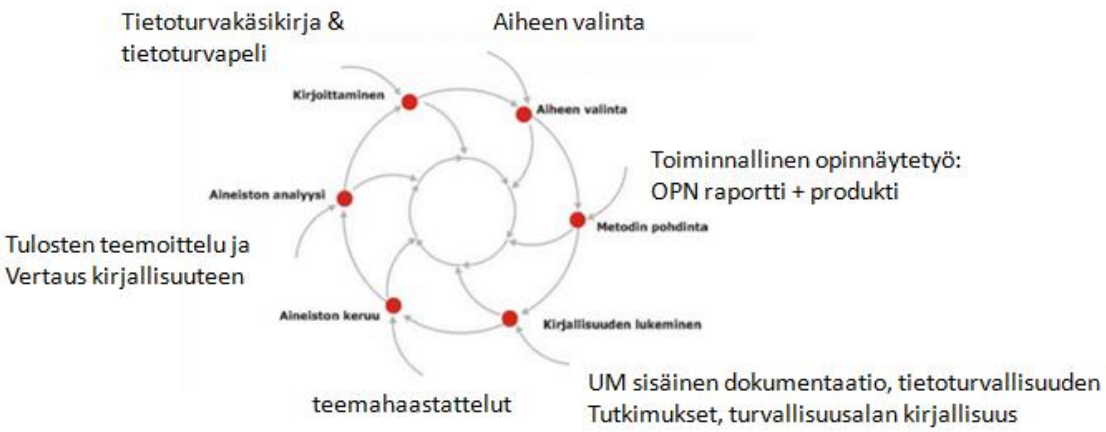
Suunnitteluvaihe alkoi alkutilannekatselmoinnilla. Alkukatselmoinnissa haettiin perusymmärtämystä toimintakentästä, sekä etsittiin relevantteja tietolähteitä. Lähteet voivat olla kirjallisuuslähteitä tai haastateltavia asiantuntijoita. Alkukatselmointivaiheessa laaditaan alustava aikataulutus projektin loppuun saakka. Osaltani projektin päättyminen merkittiin joulukuulle 2017, jolloin ohjeistus luovutettaisiin sen tilanneelle organisaatiolle.

Suunnitteluvaihetta seurasi tiedonkeruuvaihe. Tiedonkeruuvaiheessa haettiin potentiaalisia kirjallisia lähteitä ja etsittiin tietoturvakäsikirjan kokoamisen kannalta hyödyllisiä haastateltavia. Yhdessä tietoturvapäällikön kanssa haastateltaviksi katselmoitiin neljä ulkoministeriön

ja ulkohallinnon esimiestä sekä ulkoministeriön turvallisuusjohtaja ja turvallisuusneuvonantaja. Näin vastauksia tutkimuskysymyksiin saatiin sekä esimiehiltä, jotka ovat turvallisuusohjeistuksen asiakkailta, että turvallisuusasiantuntijoilta, jotka laativat turvallisuusohjeistuksia työkseen.



Kuvio 3: opinnäytetyöprosessi



Kuvio 4 Tutkimusspiraali, jota opinnäytetyö seurasi (Hirsjärvi, Remes ja Sajavaara 2001, 15).

Haastattelut suoritettiin sekä Helsingissä ministeriössä, että eräässä Suomen edustustossa. Jo haastattelujen suorittamisen aikana aloitin toteutusvaiheen, laatimalla tietoturvakäsikirjasta ensimmäisiä versioita. Ensimmäisten versioiden kautta selvisi, että ulkoministeriö oli avoin ohjeistukselle, joka ei olisi aiemmin laadittujen tietoturvaohjeiden kaltainen. Uudeksi tavoitteiksi ohjeelle määriteltiin saatavuus ja päivitettävyys.

Suunnitteluvaiheen lopussa esimieshaastatteluiden innoittamana Savolainen pyysi minua tarkastamaan olemassa olevat tietoturvan kotisivut ja suunnittelemaan ajankohtaisportaali Sharepoint-ympäristöön. Savolaisella on suunnitelma tuoda ajantasaista tietoa RSR-feedien muodossa. Samaan aikaan tietoturvapelin suunnittelu sai alkunsa, olemassa olevien pöytä – ja korttipelien, läpikäynnillä. Tarkasteluun valiutui niin sanottuna vakavia tietoturvapelejä, joiden pelaamisella voisi olla vaikutusta pelaajan turvallisuustietoisuuden kehittämiseen.

Toteutusvaihe, seurasi suunnitteluvaihetta ja jatkui elokuusta 2017 joulukuuhun 2017. Suunnitteluvaiheessa kun esimieshaastattelut oli jo litteroitu ja niiden tuloksia oli sovellettu kirjoitusprosessissa, ymmärsin, että kirjallisuuskatsaus ja suoritetut haastattelut eivät olleet tuottaneet omasta mielestäni tarpeeksi tuloksia opinnäytetyöraporttia varten. Sovin elo- ja syyskuulle lisähaastatteluja ulkoministeriön ulkopuolisilta tietoturvaasiantuntijoilta. Joulukuussa ulkoministeriön sisäverkkoon luotiin tietoturvatiimin sivuston yhteyteen Wiki-sivusto, johon koottu tietoturvakäsikirja-materiaali siirrettiin Sharepoint-ympäristöön. Tietoturvapäällikön kanssa sovittiin, että harjoitteluni päätyttyä hän jatkaisi Wiki-sivuston muokkausta ja tuottaisi myöhemmin osasta materiaalista painetun version.

7.1 Teemahaastatteluista uutta tietoa esimiesten turvallisuusohjeistukseen

Opinnäytetyön teemahaastatteluissa (liite 1) haastateltiin ulkoministeriön ja edustustojen päälliköitä ja muita esimiehiä, jotka ovat potentiaalisia tietoturvakäsikirjan kohdelukijoita. Teemahaastatteluissa haastateltiin erään lähetystön päällikköä, lähetystön päällikön sijaista sekä tietohallintovastaavaa. Tämän lisäksi haastatteluihin valikoitui ulkoministeriön henkilöstöpäällikkö, sisäisen tarkastuksen päällikkö, turvallisuusjohtaja ja turvallisuusneuvonantaja. Kunkin haastattelujen kesto oli noin tunti. Haastattelujen kulkuun vaikutti haastateltavan oma johdattelu, joka mahdollisti tähdentävät lisäkysymykset, sekä tiettyjen kysymysten pois jättämisen. Osa haastateltavista esiintyy työssä haastattelukoodeilla ja osa omilla nimillään luvan kanssa. Taulukko 2 esittää haastattelukoodit, joita käytetään myöhemmässä vaiheessa haastattelujen tuloksia käsiteltäessä.

Haastattelu	Tehtävä
H1	Edustuston esimies
H2	Edustuston esimies
H3	Edustuston hallintovirkamies
H4	Ulkoministeriön esimies
H5	Ulkoministeriön esimies

Taulukko 2 Esimiesten haastattelut

Koska tietoturvallisuuden esimiehille kohdennettua ohjeistusta on käsitelty hyvin vähän turvallisuusalan kirjallisuudessa, haastattelun kohteiksi valikoitui joukko julkishallinnon turvallisuuden- ja tietoturvallisuuden asiantuntijatehtävissä toimivia henkilöitä, sekä yksityisen puolen tietoturvallisuusasiantuntijoita. Haastateltaviksi valikoitui ulkoministeriön turvallisuusjohtaja, valtioneuvoston tietoturvapäällikkö, viestintäviraston kyberturvallisuuskeskuksen varapäällikkö, ulkoministeriön turvallisuusneuvonantaja, F-Securen tutkimuspäällikkö ja Aditron tietoturvajohtaja.

8 Tulokset

Tässä luvussa käsitellään teemahaastattelujen tuloksia. Teemahaastattelun tuloksia kerääntyi litteroituna 5-10 sivua per haastateltava, eli yhteensä 70-sivua. Haastattelumateriaalista poimittiin tutkimuskysymysten perusteella valitut teemat. Teemojen ulkopuolelle jääneet keskustelut rajataan pois tästä raportista, mutta ne vaikuttivat ainakin alitajuisesti produktin sisältöön.

8.1 Esimiehen rooli turvallisuuskulttuurin rakentajana

H1 ja H3 muistuttavat, että tietoturvallisuuden näkyminen ja koulutuksista huolehtiminen kuuluvat edustustoissa edustuston päällikölle. Puhakainen (2017) katsoo esimiehen johtamat turvallisuuttakin koskettavat esimies-alaiskeskustelut toimiviksi koulutuskeinoiksi, mutta

niiden vaatimuksena on se että asiantuntijat toimittavat esimiehelle koulutusmateriaalin ja käyvät sen etukäteen lävitse hänen kanssaan. (2017.)

H3:n mukaan tietoturva-ajattelussa vaikutusta on myös päällikön roolilla. Onko henkilö enemmän johtaja vai asiantuntijaroolissa. Asiantuntijat lähtevät siitä, että kaikki muutkin tekevät asiantuntijatyötä omilla tonteillaan ja vastaavat omista työtehtävistään. H3:n mukaan tämä on organisaatiokysymys ja pitkä prosessi: miten päälliköt mieltävät vastuunsa johtajina ja yhdistävät sen asiantuntijuuteen. (2017).

H2 kertoo, että hän on työskennellyt viidessä edustustossa pitkän työuransa aikana ja hänen mukaansa tietoturvaa ei ole menneisyydessä pidetty kovinkaan suurena uhkana tai riskinä. H2 katsoo, että tietoturvallisuus ei ole ollut paljon esillä. Erääksi syyksi hän katsoo sen, että suurin osa päivittäin käsitellystä tiedosta sisältää hyvin vähän käytännön riskejä. Hänen mukaansa vasta aivan lähivuosina tietoturvallisuudesta on alettu käymään vakavia keskusteluja ja niiden pohjalta esimerkiksi jättämään puhelimia pois virkamiesten strategisista keskusteluista. Tietoturva on tiedostettu, mutta siihen reagoidaan aika hitaasti. (2017.)

H3:n mukaan delegointi on johtamisessa välttämätöntä. Sen voi kuitenkin korvata dialogin kautta tapahtuvana, luottamukseen perustuva tonttien jakaminen. H3 kertoo, että työtä tehdään paljon aluksi, jotta työntekijöitä ei tarvitse enää tietyn ajan jälkeen käsiohjata. Onnistunut lopputulos saavutetaan, kun määritellään tavoitteet, työkalut, joilla tavoitteet saavutetaan, mekanismit, joilla tavoitteita seurataan ja tuloksia mitataan.

Ulkoministeriössä diplomaattisen viestinnän salassapito kuuluu olennaisesti edustustojen tietoturvaan. H2 (2017) kertoo, että monesti salassapito liittyy diplomatian tapakulttuuriin, että toisten asioista ei ole tapana puhua, eikä aina niinkään substanssiin. Salassapito korostuu etenkin kriisitilanteissa ja silloin tietoturvallisuus on tärkeätä. Paananen (2018) sivuaa samaa asiaa kysymällä osaavatko esimiehet edustustoissa ottaa täyden hyödyn edustustojen puolustus – ja poliisiasiamiesten ammattitaidosta tiedustelukoulutuksen saaneina virkamiehinä, omien alaistensa koulutuksessa. Paananen (2018) muistuttaa, että henkilökohtaisesti suoritettu, osaava koulutus on täysin eri asia kuin asioiden läpikäynti papereilla ja verkkokoulutuksessa.

Hyppönen (2017), Puhakainen (2017) ja Räty (2018) näkevät että organisaation turvallisuuskulttuuri lähtee johdosta ja esimiehistä. Esimiehen esimerkki kertoo henkilökunnalle, että sääntöjä seurataan ja sama esimieshän sääntöjen noudattamistakin vaati. Hyppösen mukaan on hurja ero, miten henkilökunta käyttäytyy tietoturva-asioiden suhteen, jos he aistivat tai konkreettisesti näkevät, että esimies ei välitä ja asioita ei seurata. Räty (2018) ei näe että yksikään organisaatio jossa johto ottaa vapauksia tietoturvan suhteen, voisi säilyä pitkällä juoksulla turvallisena.

8.2 Tietoturvan toteutumisen haasteet esimiestyössä

Haastatteluissa esiintyneet tietoturvan toteutumisen haasteet noudattivat pitkälti Roperin & Graun (2006) listausta työympäristöstä ja työkaluista, taidoista ja tietämyksestä sekä motivaatiosta ja asenteista. Näistä työkaluihin ja ajankäyttöön liittyvät haasteet olivat selkeästi korostettuina. Aarnion (2017) mukaan erityistehtäviä kuten esimiestyötä suorittaville täytyy olla oma räätälöity koulutus, jossa käydään lävitse syitä ja seurauksia. Aarnion mielestä positiivista on se, että usein henkilö on jo kiinnostunut aiheesta. Tietoturvallisuus lähtee perehdytyskoulutuksista ja uusien esimiesten perehdyttämisestä.

H3:n kokemuksen mukaan merkittävä esimiehen tietoturvallisuusvelvoitteisiin liittyvä haaste on se, että esimies ei kykene valvomaan kaikkea toimintaa: ”Meitä on 22 töissä ja harjoittelijat päälle. Tämä on kuin rakennustyömaa. Ei kukaan pysty kulkemaan täällä työmaapäällikkönä ja varmistamaan, että kaikilla on koko ajan kypärät päässä ja turvalasit.” H3 katsoo, että ratkaisu on tietoturvallisuuden valtavirtaistuminen. Sen täytyy tulla integroiduksi osaksi toimintakulttuuria ja vaatii jatkuvaa tietoturvatietoisuuden ylläpitoa. Kyse on kuin kirjoitus- ja lukutaidosta.”

H2 (2017) haluaisi, että tietoturvan näkyvyyttä nostettaisiin vielä näkyvämmäksi arjen rutiineissa. Tietotaitoa monissa edustustoissa löytyy myös poliisi- ja puolustusvoimien puolelta, mutta kulttuuri voi olla sisäänpäin kääntynyttä ja tietotaidon jakoa voisi kehittää pidemmälle. Paananen (2018) Viestintävirastosta nostaa saman asian esille ja toivoisi laajempaa yhteistyötä tiedon jaossa viranomaisten kesken.

H3 (2017) jatkaa vertaustaan tietoturvallisuudesta kansallistaitona. Tietoturvallinen työskentely ulkoministeriössä vaatii samoja varotoimia kuin henkilökohtaisen sähköpostin ja kotikoneen tietosuojan ylläpitäminenkin. ”Sun henkilökohtaiset postit ovat aivan yhtä haavoittuvaisia kaikille häiriötiloille kuin se sun työpostisikin.”

Aarnion mukaan henkilöstön rotaatio luo oman haasteensa. Rotaatiossa noin 20 % henkilöstöstä vaihtaa asemapaikkaa ja työtehtävää. H5 mukaan edeltäjän täytyisi huolehtia seuraajan perehdyttämisestä ja varmistaa, että kulkuoikeudet ja työhön liittyvät työkalut kulkeutuvat seuraajalle. Testamentti olisi saatava pakolliseksi jopa niin, ettei sinua signeerata uuteen kohteeseen, jollei testamenttia ole hyvin tehty. Aarnion mukaan hyvä työmalli voitaisiin kopioida YK:sta, josta saat lopputulin vasta kun koko lähtöprosessi on suoritettuna ja kaikki siihen liittyvä omaisuus palautettuna. Huonosti suoritettu rotaatio tuhlaa myös työaikaa kaikilta (Aarnio 2017; H5.)

Aarnion mukaan työkalut eivät vastaa vielä ulkoministeriön korkeita tietoturvatarpeita. Luokiteltujen asiakirjojen (ST III ja korkeampi) luominen on hyvin hankalaa. Aarnion mukaan paljon helpompi on rikkoa sääntöjä ja kirjoittaa dokumentti työkoneella kuin varata aika

sanomakeskukseen ja mennä sinne kirjoittamaan. ”Voit esimerkiksi huomata takaisin palatessasi, että asiakirjassa on kirjoitusvirheitä. Joudut palaamaan takaisin korjaamaan ne. Ei asioiden pitäisi olla näin vaikeita nykypäivänä”. Aarnion mukaan tietojärjestelmien keskittäminen olisi tehokas työkalu. Tällä hetkellä tietoa käsitellään liikaa manuaalisesti (Aarnio 2017.)

H3 muistuttaa, että usein työntekijät tuntevat itsensä kauhean avuttomaksi tietoturvauhkia kohtaan. Miten voin vaikuttaa siihen, että joku hämäräperäinen taho hakkeroi pankkitilisi? ”Siinä tuntee itsensä vain uhriksi. On tärkeätä, että tämä muuttuu ja ymmärrät, ettet ole aina objekti, vaan voit olla myös subjekti. Voit puolustaa itseäsi tarvittavien työkalujen avulla.” (H3 2017.)

Puhakainen (2017) ymmärtää hyvin organisaation johtoa, joka saa usein syyn niskaansa, kun jokin menee tietoturvassa vikaan. Puhakaisen mukaan sekään ei ole oikein, koska he ovat monesti tiukassa paikassa asian kanssa. ”Tämä on edelleen tukifunktio ja heillä on aivan omat päivittäiset murheensa, kuten organisaation johtaminen.”

H4 (2017) katsoo, että tietoturvallisuudessa ympäristö ja työkalut ovat tietotaidon lisäksi myös tärkeitä. Luokiteltuja dokumentteja käsiteltäessä niiden hyväksytyn säilytyspaikan, holvin tai kassakaapin, on oltava lähellä. Työkoneiden täytyy olla sijoitettuna työympäristöön niin, että ne ovat jatkuvasti työntekijän hallinnassa. Keskustelussa tuli ilmi, että H4:llä oli kokemuksia aiemmista työpiste järjestelyistä, joissa laitteita oli sijoitettu kahteen eri kiinteistön kerrokseen ja houkutus jättää koneet auki koko päiväksi oli suuri.

Peltosen (2017) tarkastelee palkitsemisen ja sanktioinnin suhdetta siten, että vaikka palkitseminen turvallisuuskulttuurin rakentamisessa on tärkeätä, täytyy löytyä myös toimiva sanktiointimenettely palkitsemisen epäonnistuessa. Peltonen muistuttaa, että se syö motivaatiota kaikilta toimia turvallisesti, jos organisaatiossa on henkilöitä, joiden käytös osoittaa, että turvallisuudesta ei tarvitse välittää.

8.3 Hyvän esimiesohjeen tunnusmerkkejä

Kaikki haastateltavat mainitsivat ajanpuutteen syynä siihen, että tietoturvaohjeita ei lueta. Ohjeiden pitäisi olla hyvin lyhyitä. Vastaukset vaihtelivat 1 sivun huoneen taulusta, korkeintaan 5 sivun pituuteen. Hieman paradoksaalisesti tästä huolimatta useampi henkilö halusi ohjeisiin tarkistuslistoja, joista voisi tarkistaa juuri sillä hetkellä ajankohtaisia asioita, kuten luokitellun asiakirjan sallitun lähetystavan. H3 (2017) kertoo, että ihmiset omaksuvat tietoa hyvin eri tavoilla. Osalle pitkäkin teksti sopii hyvin, mutta toiset saavat siitä kohtauksen. Kolme sivua on hänen omasta mielestään maksimimäärä, jonka hän hyväksyy, jos mukana asiaa avaavia kuvia ja muuta grafiikkaa.

Hyppönen (2017) ja H3 (2017) ehdottavat molemmat tarinoiden kertomista. Hyppönen kertoo case-tyylisten esimerkkien olevan tehokkaita työvälineitä, etenkin jos kerrotut tarinat

voisivat selkeästi tapahtua myös lukijalle. H3 korostaa abstraktiuden häviämisen tärkeyttä. Paananen sekä Puhakainen mainitsevat haastatteluissa, että esimiehet kuuntelevat parhaiten samassa asemassa olevia kollegoitaan ja esimiehiään. Paananen ehdottaakin case-luonteisten tietoturvatapausten esilletuomista vuosittaisilla suurlähettiläspäivillä, edustuston esimiesten kertomana muille edustuston esimiehille.

Haastatteluista löytyi runsaasti mielipiteitä huonoista ohjeista: Olemassa olevat ohjeet ovat liian pitkiä tai ohjeita ei löydy helposti sisäverkosta. Tiedonvälitys ei vastaa tiedon saannin tarvetta. Ohjeet ovat hautautuneena sisäverkkoon. Puhakainen muistuttaa myös, että maailma on myös täynnä huonoja tietoturvaohjeita, joita noudattamaan ei saa kukaan. (Aarnio 2017; H4 2017; Puhakainen 2017)

H2:n (2017) mukaan tietoturvakäsikirjasta olisi hyvä löytää ohjeita nopeasti tuleviin tilanteisiin, joihin ei ole rutiinia. Hän korostaa keskusteluja ja kokouksia, joissa voidaan keskustella potentiaalisesti luokitellusta tiedosta. Osa teemoista on hyvin selkeitä ja tiedämme, ettei niistä puhuta, mutta aina on sellainen harmaa osa-alue. Esimerkiksi jos ulkomaalainen kollega haluaa kutsua lounaalle ravintolaan, mistä asioista voit keskustella? H2 mainitsee, että esimerkiksi omaan työhön ja persoonaan liittyvissä kysymyksissä täytyy olla skarppina. Aina täytyy muistaa, kenen kanssa käydään dialogia.

Puhakainen (2017) mukaan syy siihen, miksi esimiehen ohjeistuksesta ei löydy suoraan tietoa on se, ettei se eroa paljoakaan normaalista kouluttamisesta ja ohjeistamisesta. Hän on myös hienoisen pessimistinen keinoista, joilla etenkään ylempää johtoa saataisiin helposti lukemaan turvallisuusohjeistusta. Hänen mukaansa kasvokkain tapahtuva kouluttaminen tuottaa parempia tuloksia. Peltonen ja H3 (2017) mainitsevat molemmat henkilökohtaisen koulutuksen olevan tehokkaampaa muun kaltaiseen ohjeistamiseen verrattuna. Aarnion (2017) mielestä hyvä tietoturvakäsikirja sisältää runsaasti konkretiaa jokapäiväisistä työtehtävistä. Tietojen käsittelyä on jo ohjeistettu hyvin, mutta silti siitä johdetut asiat unohtuvat helposti.

Moni päällikkö hyötyisi strategisesta johdannosta, eli miksi tätä työtä tehdään? Miksi tietoturva on tärkeä, miltä osin se on tekninen kysymys ja ei ole tekninen kysymys? Mitkä asiat ovat kontrollissasi ja mitkä eivät (H3 2017.) H3 (2017) taas kertoo pitävänsä turvallisuusasiat esillä ja nostavansa niitä viikkopalavereissa esille. Hän toivoisi käsikirjaan käytännön asioita, kuten tarkistuslistoja, joita voisi nostaa esille juuri tiimipalavereissa.

Peltonen (2017) varoittaa turvallisuustermien ja niin sanotun konsulttikielen käytöstä ohjeissa, koska ne vieraannuttavat lukijakunnan esitettävästä asiasta. Hän katsoo myös, että ainoa tehokas keino saada henkilöstö lukemaan tietoturvaohje, on tehdä siitä tuote, joka on syystä tai toisesta haluttava. Paananen (2017) ja Peltonen (2017) molemmat katsovat, että käsikirja vaatii näkyvän ylimmän virkamiesjohdon sponsoroinnin. Paananen ehdottaa, että

tehokas osoitus johdon sponsoroinnista tietoturvaohjeelle olisi heidän esiintymisensä valokuvin teoksen sivuilla.

H5 sekä Räty (2018) katsovat, että vaihtoehtoisilla esitystavoilla on myös paikkansa. Näitä voisivat olla esimerkiksi lyhyet tietoturvallisuusasiaa sisältävät koulutusvideot, joita lähetettäisiin työntekijöiden sähköposteihin. Paananen (2018) korostaa tietoturvan tiukempaa synteesiä muun esimiesohjeistuksen kanssa ja täten liittämistä olemassa oleviin ohjeistuksiin.

Räty (2018) katsoo, että hyvä tietoturvaohje ei ole koskaan virastotekstiä vaan on muodoltaan vapaamuotoisempi. Ohjeen kaava on seuraava: ohjeistettavaa asiaa koskevat lait ja vaatimukset, ohjeen selitys ja lopulta käytännön esimerkki ja käyttötapaus. Räty (2018) varoittaa, että vaikka interaktiiviset koulutustavat kuten pelillistäminen ovat yleisesti toimivia, niin monesti ne työntekijät, jotka kaipaisivat eniten lisätukea kieltäytyvät osallistumasta epäonnistumisen pelosta.

Teemahaastattelut hakivat vastauksia siihen minkälaisia ominaisuuksia esimiehet ja tietoturvallisuus asiantuntijat näkivät onnistuneessa tietoturvaohjeessa. Suurin osa katsoi käytännöllisesti, että ohjeiden on oltava lyhyitä, koska muuten niitä ei lue kukaan. Toisaalta ulkoministeriön kaltaisessa organisaatiossa tarvittavan tiedon määrä on huomattava. Useat haastateltavat myös mainitsivat erityisesti tarvitsevansa ohjeita esimerkiksi asiakirjaturvallisuuteen ja keskustelujen salassapitoon liittyvissä poikkeuksellisemmissa tapauksissa.

Peltonen (2017) katsoi pitkällä kokemuksellaan, että kasvokkain suoritettu koulutus antaa pitkäkestoisimman vaikutuksen positiiviseen turvalliseen käytökseen ja on ainoa keino vaikuttaa asenteisiin. Peltonen (2017) katsoo, että esimiehille voidaan pitää omia turvallisuuskatsauksia, mutta vaikuttamisen täytyy tapahtua monella tavalla yhtä aikaa ja suuntautua esimiehiin ja heidän alaisiinsa. ”kun alaistaso tulee tietoiseksi minkälaisia asioita edellytetään esimieheltä, tällöin esimiehen on myös helppo hoitaa asioita, kun ei tarvitse perustella tehtävän oikeutusta.”

9 Johtopäätökset ja pohdinta

Esimiehen voidaan ajatella olevan käsikirjan ensisijainen asiakas. Tekstin täytyy siten puhutella esimiestä ja pitää yllä hänen mielenkiintonsa. Tekstin on oltava tyyliltään helppolukuista ja välttää erikoissanastoa ja turvallisuusalalle rantautunutta englanninkielestä lainaavaa termistöä. Onnistunut tietoturvakäsikirja palvelee mahdollisimman monia lukijansa turvallisuuteen liittyviä tarpeita ja sopii myös muiden organisaatioiden käyttöön pienellä muokkauksella.

Gauntia (2000) mukaillen voidaan katsoa, että ministeriön esimiesasemassa olevat työntekijät ovat alaisilleen huomattavia mielipidevaikuttajia. Ulkoministeriön osalta ylimmän johdon edustaja, voisi olla valtiosihteeri tai ulkopolitiikasta vastaava ministeri. Johdon viesti

tietoturvallisuustyön merkityksestä ministeriön toiminnalle, voisi nostaa tietoturvallisuuden profiilia esimiesten silmissä, ja avustaa heitä osaltaan mielipidevaikuttajina.

Haastattelujen tulokset osoittavat, että ulkoministeriön esimiehet katsovat puutteellisten työkalujen olevan yksi merkittävistä haasteista tietoturvallisuuden toteutumisen tiellä. Työkalut voivat olla kömpelöitä, tai ne eivät sovellu työtehtävään. Tässä vertailu nykyaikaisiin älylaitteisiin ja viihdeteknologiaan ei imartele viraston laitteita, jotka tietoturvavaatimusten vuoksi ovat vähemmän käyttäjäystävällisiä. Haastattelut myös osoittivat, että lähes kaikki haastateltavat mainitsivat ohjeistuksien vaikeatajuisuuden. Jos hyviä ohjeita on kirjoitettu, ne ovat hajallaan sisäverkon syövereissä.

Haastattelut eivät kykene pureutumaan haastateltavien motivaatioon ja asenteisiin: haastattelutilanteessa kukaan ei myönnä kasvokkain suoritettavissa haastatteluissa välinpitämättömyyttään tietoturvallisuutta tai siihen liittyviä ohjeistuksia kohtaan ja tämän kaltaiset asianseikat voidaan havaita vain pitkällisen havainnoinnin seurauksena. Muutama haastattelu antoi kuitenkin vihjeitä siitä, että tietoturvallisuus ei ole menneisyydessä ollut paljoakaan esillä. Tietoturvan kuten muunkin turvallisuuden merkitys nähdään yleensä vasta kun vakava vaaratapaus tulee julki. Tämän kaltaisia, herättäviä, vaaratapauksia ovat varmasti olleet Saksan liittokanslerin Angela Merkelin paljastunut puhelinkuuntelu (Kauppalehti 2013) sekä omaa ulkoministeriötämme kohdannut tietomurto (Helsingin Sanomat 2013.)

Haastattelut jakaantuivat asiantuntijahaastatteluihin, sekä esimieshaastatteluihin. Näiden ryhmien mielipiteitä toisiinsa verratessa, käsitykset esimiehen roolista tietoturvallisuusvaikuttajina alaisilleen vastasivat pitkälti toisiaan. Vastaukset syistä esimiesten tietoturvaroolien haasteisiin eivät taas olleet täysin yhteneväiset asiantuntijoiden ja itse esimiesten kesken. Asiantuntijoista useampi ymmärsi esimiesten ajankäytön haasteet: hyvin moni tärkeä asia kilpailee esimiehen huomiosta heidän työssään ulkoministeriössä ja tietoturvallisuus sijoittautuu siinä vertailussa vähemmälle huomiolle. Asiantuntijat korostavat kuitenkin turvallisuuskulttuurin ja asenteiden merkitystä haasteina kun taas esimiehet mainitsevat suurimmiksi haasteiksi ajankäytön ja resurssi sekä työkaluihin liittyvät haasteet.

Tietoturvallisuuteen liittyvä tietotaito kehittyy haastattelujen tulosten perusteella parhaiten kasvokkain suoritettavien koulutusten kautta. Vaikka Helsingissä suoritetaankin erinäisiä koulutuksia, etenkin virkamiehen saapuessa viraston palvelukseen on paikallinen perehdyttäminen ja koulutus olennainen osa työtehtävien oppimista. Haastattelut korostavat urakiertoon liittyviä esimiesten perehdytyshaasteita ja niihin liittyviä aikarajoituksia. Virkamiehen siirtyessä asemapaikasta toiseen on seuraajan perehdytys pahimmassa tapauksessa ainoastaan ”testamentiksi” kutsun perehdyttämisasiakirjan varassa. Muutostila on aina altis virheille ja väärinkäytöksen uhriksi joutumiselle ennen toimintaympäristön omaksumista.

Ulkoministeriö organisaationa voidaan katsoa varsin byrokraattiseksi, mikä on virkamiesorganisaatiolle tavanomaista. Työtehtäviä suoritetaan virkavastuulla, työurat ovat varsin pitkiä ja organisaation virkamiesjohto on aloittanut työuransa virastossa aikana, jolloin tietotekniikka ja sen tuomat haasteet eivät olleet vielä ajankohtaisia. Tietoturvallisuuteen liittyvä turvallisuuskulttuuri ei ole vielä täten saavuttanut huippuaan. Haastattelujen perusteella vasta viime vuosina puhelimia on alettu jättää pois tärkeistä keskusteluista ja tietoturvallisuusriskit ovat nousseet yleisestikin huomioitaviksi asioiksi. Etenkin edustustoissa, jotka toimivat varsin autonomisesti suurlähettilään johdolla on edustuston keskeinen turvallisuuskulttuuri sen esimiesten vastuulla.

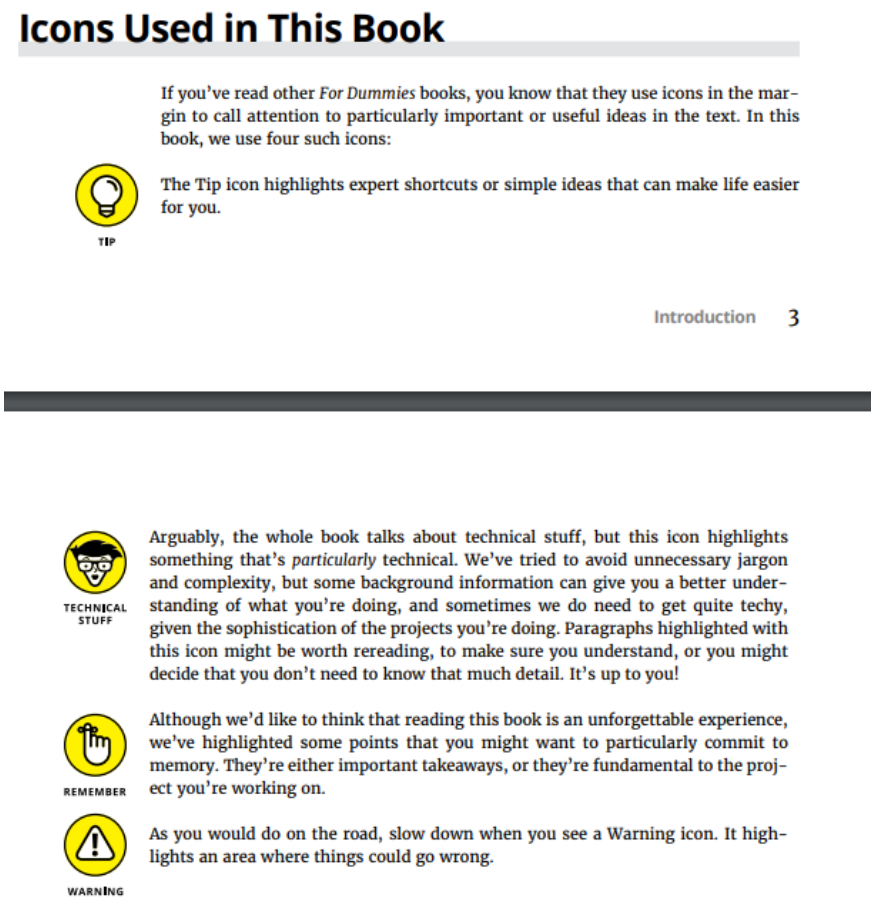
Tietoturvallisuus usein käsitetään kapeammaksi aihealueeksi kuin se onkaan. Sen fyysiseen turvallisuuteen, henkilöturvallisuuteen ja paloturvallisuuteen liittyvät osa-alueet jäävät haittaohjelmien ja salasanojen hallinnan varjoon. Voidaankin katsoa, että tämän vuoksi riski tietoturvalle on korostettu virheiden johdosta, jotka liittyvät tietoturvallisuuden osa-alueisiin, joiden ei mielletä perinteisesti kuuluvan tietoturvan piiriin: kulkuoikeuksien hallinta, hälytysjärjestelmien huolto, kokouksien tietoturva, työkeskustelut julkisilla paikalla…muutamia mainitakseni.

Haastattelujen perusteella tarve pukea olemassa olevat ohjeistukset helpommin lähestyttävään ulkoasuun ja -muotoon oli ilmeinen. Produktia kirjoittaessani organisaatiolta puuttui kokonaan kaikkien saatavilla sisäverkosta löytyvä normaalimuotoinen tietoturvaohje, vaikka merkityksellinen tietoturva-asia olikin upotettu lukuisiin henkilöstölle tutuiksi tulleisiin ohjeisiin, kuten salassa pidettävän luokitellun tiedon käsittely, salaviestijärjestelmät, edustuston turvallisuusohje jne. Tämän lisäksi pakollisen tietoturvallisuuden verkkokoulutuksen sisältö läpikäy tietoturvallisuuden keskeiset osa-alueet.

Tietoturvakäsikirja ei ole viimeistelty dokumentti vaan jatkuvasti päivitettävä ja muodoltaan vaihtuva. Tietoturvakäsikirja on formaatiltaan tavanomaisesta poikkeava. Se ei ole kuiva yhteenveto faktoista, vaan toivottavasti haastaa esimerkkiensä ja pohtimista vaativien kysymysten kautta esimiehen ja hänen työyhteisönsä käsittelemään pintaa syvemmältä tietoturvallisuutta: miksi tietoturvakontrollit ovat tarpeellisia, mitä tietoturvaan liittyviä uhkakuvia omaan työhön liittyy ja miten voin hallinta siihen liittyviä riskejä? Mitä esimiehen tietoturvavastuisiin oikeasti kuuluu ja mitkä osa-alueet jäävät esimerkiksi teknisinä asiantuntijoiden harteille? Pohdinnan kautta lukija käsittelee lukemaansa ja yhdistää siitä saadun tiedon aiempiin kokemuksiinsa ja peilaa sitä ennakkokäsityksiään vastaan tietoturvallisuuden suunnitteluteorian mukaisesti (Puhakainen 2006.)

Tietoturvakäsikirjan visuaalinen alkuperäinen muoto sai inspiraationsa suositusta For Dummies -kirjasarjasta (kuvio 5) jota on myyty kansainvälisesti yli 300 miljoonaa kappaletta (Wiley 2018.) For Dummies -kirjan tärkeä ominaisuus on normaalia kevyempi, keskusteleva ote ja

tapa syventää lukukokemusta selkeästi merkityillä tapauskertomuksilla, tekstiä selvittävillä kuvilla sekä tarkistuslistoilla. Kirjasarja pyrkii myös käsittelemään vaikeitakin asioita helposti ymmärrettävästi.



Icons Used in This Book

If you've read other *For Dummies* books, you know that they use icons in the margin to call attention to particularly important or useful ideas in the text. In this book, we use four such icons:

TIP

The Tip icon highlights expert shortcuts or simple ideas that can make life easier for you.

TECHNICAL STUFF

Arguably, the whole book talks about technical stuff, but this icon highlights something that's *particularly* technical. We've tried to avoid unnecessary jargon and complexity, but some background information can give you a better understanding of what you're doing, and sometimes we do need to get quite techy, given the sophistication of the projects you're doing. Paragraphs highlighted with this icon might be worth rereading, to make sure you understand, or you might decide that you don't need to know that much detail. It's up to you!

REMEMBER

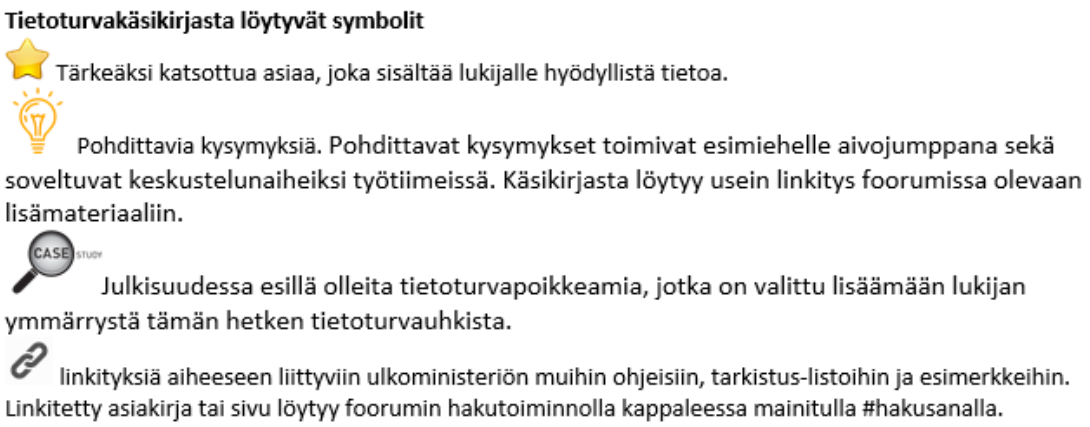
Although we'd like to think that reading this book is an unforgettable experience, we've highlighted some points that you might want to particularly commit to memory. They're either important takeaways, or they're fundamental to the project you're working on.

WARNING

As you would do on the road, slow down when you see a Warning icon. It highlights an area where things could go wrong.

Kuvio 5 A Wiley kirjojen lukua helpottavat ikonit (a Wiley 2018).

joka on ministeriön työntekijöiden helposti saavutettavissa. Käsikirjan kielen täytyy olla selväkielistä ja helppolukuista myös tietotekniikkaan ja sen sanastoon perehtymättömän käyttöön. Käsikirjan kieleksi valikoitui asiantuntijahaastatteluiden kautta puhutteleva. Koska Ulkoministeriön arvot määrittelevät ohjeelle laadullisia vaatimuksia, jokaisen käsikirjan luvun perään liitetään myös listaus lähteistä, joita kappaleessa käsitellään.



Kuvio 5 tietoturvakäsikirjassa käytetyt ikonit

Tiedon eheyden osalta tietoturvakäsikirjan on tärkeätä varmistaa myös tiedon oikeellisuus ja ajantasaisuus. Oikeellisuuden osalta sisältö tarkistetaan tietoturvapäällikön kanssa, ja sille haetaan palautetta lausuntokierroksella. Tiedon ajantasaisuuden osalta haaste on tietoturvallisuuden niin sanotun kyberturvallisuuden osa-alueen uhkakuvien nopea kehitys ja ohjeen päivitystarve kun uusia työkaluja ja toimintatapoja otetaan käyttöön. Tiedon ajantasaisuus turvataan verkkoversiolla, jota tullaan tarkistamaan vuosittain tietoturvatiimin toimesta. Ajantasaisuus säilyttää myös asiakirjan kiinnostavuuden esimiehille. Asiakirjan käytettävyys turvataan verkkoversiolla, johon on lukuoikeus kaikilla ulkoasiainhallinnon työntekijöillä, joilla on pääsyoikeus sisäverkkoon.

Opinnäytetyöprojektin sivutuotteena, haastatteluaineiston innoittaman, syntyi konsepti edustuston tietoturvapelistä (liite 5). Henrix, Al-Sherbaz & Bloom (2016) mukaan vakavat tietoturvapelit on tarkoitettu tietoturvatietämyksen kasvattamiseen ja pitkäkestoiseen käyttäytymisen muutokseen. Tietoturvallisuutta ja kyberturvallisuutta koskettavaa tutkimusta on suoritettu tähän mennessä vain pienissä tutkimusryhmissä. Tutkimustulokset ovat varovaisen positiivisia, mutta kysymykseen, ovatko vakavat tietoturvapelit tehokkaita tietoturvallisuuden opetuksessa, on vaikeata vielä vastata myöntävästi. Idea Edustuston tietoturvapelistä pohjautui haastatteluista saatuun palautteeseen liittyen esimiesten henkilöstökokouksissa pitämiin turvallisuuskatsauksiin. Turvallisuus katsottiin tärkeäksi muistutettavaksi aihealueeksi, mutta lähdemateriaalia kaivattiin lisää. Edustuston tietoturvapelissä henkilöstö kokoontui keskenään pohtimaan omaan työympäristöönsä liittyviä ulkoisia riskejä. Tietoturvapelissä leikkimielisesti haetaan henkilöstön hiljaisesta tiedosta työkaluja tietoturva ja turvallisuuspuutteiden havaitsemiseen, turvallisuustoiminnan kehittämiseksi. Tietoturvapeliä on hyvä peluuttaa aluksi ulkoministeriön tietoturvatiimin asiantuntijan vetämänä, mutta myöhemmin pelin pelaamisesta voi olla apua esimiehille uusien työntekijöiden kouluttamisessa tai tietoturvallisuuden merkityksen muistuttamiseksi.

Osa edustustoista sijaitsee infrastruktuuriltaan kehittymättömissä maissa. Näissä maissa toistuvat sähkökatkot rajoittavat huomattavasti teknisten järjestelmien ja tietoverkkojen käyttämistä. Tiedon saatavuusongelma on näissä edustustoissa todellinen ja vain verkosta erillään oleva ohjeistus ratkaisisi sen. Painettu versio voisi tarjota ratkaisun asiakirjan tiedon saatavuushaasteisiin. Paananen (2018) esitti haastattelussa myös vaihtoehtoisen ratkaisun kännykkään asennettavan sovelluksen, joka kulkisi virkamiehen mukana ja tarjoaisi tarkastustietoa, myös ilman verkkoyhteyttä.

Haasteen ratkaisemiseksi tietoturvallisuuskäsikirjasta suunniteltiin laadittavaksi kaksi eri versiota: sähköinen wiki, joka sijaitsisi ulkoministeriön sisäverkossa ja olisi kaikkien työntekijöiden saatavilla ja tietoturvatiimin helposti päivitettävissä ja linkitettävissä sekä myöhemmin wikin materiaalista kasattu maksimissaan 15-sivuinen painettu paperiversio. Sähköisen tietoturvakäsikirjan ehdottomia hyötyjä on sen päivitettävyys ja mahdollisuus luoda tekstiin asiaa rikastuttavia linkkejä muihin tietolähteisiin. Tietoturvapäällikön kanssa sovittiin, että tietoturvayksikkö tarkistaa ja päivittää tietoturvakäsikirjaa soveltuvin osin vuosittain osana dokumentin elinkaarta

Tutkimusmateriaalin keräyksen aikana teoriapohja alkoi osoittamaan, että esimiestason virkamiesten tietoturvatietoisuus ei korotu ainoastaan yksittäisen tietoturvallisuusteoksen, tietoturvallisuuskäsikirjan, myötä vaan valistukseen tarvitaan useampia erillisiä viestintävälineitä. Olemassa olevien suunnitelmien, haastattelujen sekä kirjallisuuskatsauksen perusteella päädyimme keskustelemaan seuraavista asioista:

1. Esimiehille suunnattu (pakollinen) verkkokoulutus.

2. Tietoturvan voimakkaampi esiintuonti olemassa olevissa esimieskoulutuksissa. Tämä vahvistaa viestiä siitä, että tietoturva ei ole erillinen osa-alue, vaan integroituu kaikkeen toimintaan.

3. Tietoturvan sisäisten kotisivujen ajantasaistaminen.

4. Tietoturvan esilletuonti ministeriössä auktoriteettien toimesta (valtiosihteeri ja lähetystöissä edustustojen päälliköt).

5. TTS-mittarit, jotka kiinnitetään vuosiraportointiin ja tulosohjaukseen ja täten turvallisuudesta tulee konkreettinen lisä johtamisjärjestelmää.

6. Edustuston tietoturvapeli, interaktiiviseksi työkaluksi henkilöstön turvallisuustietoisuuden kehittämiseksi, joko esimies tai asiantuntijavetoisesti.

Keskustelussa tietoturvapäällikön kanssa selvisi, että näistä tietoturvasivun kehittäminen ajankohtaista tietoturvatietoa muun muassa RSR-feedeistä tarjoavaksi portaaliksi oli jo

suunnitelmana ja kykenin avustamaan sen toteutuksessa harjoitteluni aikana. Myös tietoturvaan liittyvät TTS-mittarit olivat olleet jo pitkään suunnitteilla ulkoministeriössä.

Teoria, havainnointi ja haastattelut antoivat viitteitä siitä, että organisaation esimiesten turvallisuustietoisuuteen vaikuttaminen on potentiaalisesti jopa tärkeämpää organisaation kokonaisturvallisuudelle, kuin perinteisesti harjoitettu uuden työntekijän perinteinen tietoturvakoulutus (Hyppönen 2017; Aarnio 2017; tietoturvatiimi 2016).

9.1 Työn arviointi ja jatkotutkimuskysymykset

Opinnäytetyön toiseksi eniten aikaa vievä osa-alue olivat teemahaastattelut ja niiden litterointi ja analysointi. Haastattelut olivat myös itselleni opettavaisia ja olen varsin tyytyväinen niiden toteutukseen ja tuloksiin. Kaikki haastateltavat olivat yhtä lukuun ottamatta haastattelijalle tuntemattomia mikä antoi arvoa saatujen vastausten luotettavuudelle eli validiteetille. Tutut haastateltavat olisivat saattaneet tarjota haastattelijalle tämän haluamia vastauksia. Keskusteltavissa aiheissa voitiin kuitenkin havaita, että osa kysymyksistä oli varsin vaikeita ja vaativat paljon selittämistä, minkä vuosi keskustelu saattoi ajautua haastattelijan mainitsemien asioiden myötäilyyn. Voidaan nähdä, että esimiesten kanssa käydyt teemahaastattelut toivat tarvittavaa syvyyttä opinnäytetyöprosessille, vaikka haastattelujen määrä olikin kohtuullisen vaatimaton, ainakin osa sen tuloksista on toistettavissa, mikä antaa työlle reliabiliteettia.

Laadullisen aineiston analyysissä puhutaan aineiston saamasta saturaatiopisteestä, kun haastatteluista saatu aineisto alkaa toistaa itseään. Haastatteluissa saturaatiopiste saavutettiin asiantuntijahaastatteluiden osalta, vastaukset eivät järin poikenneet toisistaan muutamia poikkeuksia lukuun ottamatta. Esimieshaastatteluissa saturaatiota ei valitettavasti saavutettu, haastattelujen vähäisen määrän vuoksi sekä luultavasti siitä syystä, että aihealueet olivat laajoja ja osa kysymyksistä käsitteli haastateltaville varsin haasteellisia aihealueita.

Kirjallisuuskatsaus sisälsi hyvin niukasti mainintoja esimiesten tietoturvakouluttamisesta. Tämän vuoksi kirjallisuuskatsauksen teoriaa rikastutettiin joukolla asiantuntijahaastatteluja. Ne muun muassa vastasivat mahdollisesti esimiehiä objektiivisemmin kysymykseen esimiesten merkityksestä turvallisuuskulttuurille. Tämä antoi viitteitä esimiehille suunnatun koulutuksen ja ohjeistuksen merkityksestä asiakasorganisaatiolle.

Tietoturvakäsikirjan kaltaisen konstruktion laatiminen opinnäytetyöksi on hyvin vaativaa. Kirjoitettavaa materiaalia syntyy kaksinkertaisesti useimpiin opinnäytetöihin verrattuna. Kirjoittajalle opinnäytetyön laatiminen oli kuitenkin loistava mahdollisuus nähdä ja oppia tietoturvasta ja siihen liittyvästä riskienhallinnasta julkihallinnon tietoturvallisuuden edelläkävijäorganisaatiolta. Opinnäytetyöprosessi herätti kiinnostuksen ja arvostuksen turvallisuustyön

varmasti monihaaraisimmalle osa-alueelle, jonka parissa uuden oppiminen ja innovaation tarve ei koskaan pääty.

Prosessin pitkäkestoisin vaihe muodostui käsikirjan eli produktin laatimisesta josta mainittakoon, että produktin ja siihen liittyvän raportoinnin viimeistelyn väliseksi ajaksi muodostui kokonainen vuosi. Opinnäytetyön kirjoittaminen on ollut jatkuvaa uuden oppimista ja ollut hyvin haastava prosessi. Voidaan varmasti arvioida kriittisesti, onko kirjoittajan asiantuntemus ollut riittävää parhaan lopputuloksen tuottamiseksi kirjoitusprosessissa. Hyödyksi voidaan kuitenkin mainita, että monia asiakokonaisuuksia tarkasteltiin uusin silmin ja mitään ei katsottu itsestäänselvyydeksi. Kirjoittamisen tukena toimi myös ulkoministeriön tietoturvatiimin asiantuntijat, joiden vastuulle jäi koostaa toimitetusta materiaalista viimeinen versio tekstistä saadun palautteen perusteella sekä muokata ja päivittää aineistoa ajan saatossa organisaation tarpeiden mukaisesti. Tietoturvakäsikirjan malli sopinee myös muille organisaatioille, ei niinkään korvaamaan hallinnollisia korkean tason turvallisuusohjeita tai operatiivisen työn tukemiseen tarkoitettuja prosessiohjeita, vaan täydentämään niitä ja kehittämään tietoturvasta kiinnostuneen esimiehen turvallisuustietoisuutta.

Opinnäytetyö sai kiitosta sekä ulkoministeriön tietoturvapäällikkö Savolaiselta, että turvallisuusjohtaja Aarniolta. Valitettavasti esimiesten palaute ei ollut vielä saatavilla harjoittelun päätyttyä. Tietoturvakäsikirjakonsepti katsottiin käyttökelpoiseksi ja opinnäytetyöprojektin aikana kerätyt tiedot katsottiin hyödyllisiksi tulevia innovaatioita ajatellen. Jo opinnäytetyöprosessin aikana tutkimusaineiston perusteella suoritettiin muutoksia muun muassa tietoturvan kotisivuille, järjestämällä ohjeita helpommin löydettäviksi, sekä tarjoamalla sivuille ajantasaista tietoa tietoturvan nykytilasta kyberturvallisuuskeskuksen tiedotteiden avulla. Edustuston tietoturvapeli sai erityiskiitosta Savolaiselta, joka on kiinnostunut ottamaan siihen pohjautuvan koulutuskonseptin demokäyttöön lähitulevaisuudessa.

Esimiesten tietoturvaohjeistus- ja koulutus ovat kohtuullisen vähän tutkittuja aihealueita eikä niistä löydy mainintoja myöskään turvallisuutta tai tietoturvallisuutta käsittelevässä lähdekirjallisuudessa. Myöskään pelillistämisen pysyviä hyötyjä turvallisuustietoisuuden kasvattajana ei ole vielä todennettu luotettavasti, laajemman tutkimuksen keinoin. Useita jatkokysymyksiä löytyy täten opinnäytetyön aihealueesta: kuinka esimiehille kohdistettu tietoturvakoulutus vaikuttaa turvallisuuskulttuuriin ja Kuinka pelillistäminen ja interaktiivinen tietoturvakoulutus vaikuttavat henkilöstön asenteisiin tietoturvallisuutta kohtaan?

Lähteet

Lait ja asetukset:

Asetus diplomaattisia suhteita koskevan Wienin yleissopimuksen ja siihen liittyvien valinnaisten pöytäkirjojen voimaansaattamisesta (4/1970). Lainattu 21.8.2017.
http://www.finlex.fi/fi/sopimukset/sopsteksti/1970/19700004#idp450147552

Laki viranomaisen toiminnan julkisuudesta (199/621). Viitattu 31.5.2018.
https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Ulkoasianministeriön työjärjestys (550/2008). Viitattu 31.5.2018.
http://www.finlex.fi/fi/laki/ajantasa/2008/20080550

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (2010/681). Viitattu 31.5.2018.
https://www.finlex.fi/fi/laki/ajantasa/2010/20100681

Valtiovarainministeriö 2011. Johdon tietoturvaopas (Vahti 2/2011). Lainattu 21.8.2017.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=6068ca18-6214-4244-8ce6-dffe952e3e8e&groupId=10229

Valtiovarainministeriö 2002. Tietoaineistojen käsittely valtionhallinnossa (VAHTI 2/2002). Lainattu 30.5.2017.
https://www.vahtiohje.fi/web/guest/yleiset-suositukset-viitekehykset-ja-standardit

Valtiovarainministeriö 2009. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (7/2009). Lainattu 30.5.2017.
http://vm.fi/documents/10623/307681/VAHTI+periaatep%C3%A4%C3%A4t%C3%B6s+2009/24355a33-4042-42fb-9dba-981e6398ee7a

Painetut lähteet

Berridge, G.R. 2002. Diplomacy: Theory and Practice. Second Edition. London: Palgrave Macmillan.

Eskola, J. & Vastamäki, J. 2001. Teemahaastattelu: Opit ja opetukset. Teoksessa J. Aaltola & R. Valli (toim.) Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineiston keruu: virikkeitä aloittelevalle tutkijalle. Jyväskylä: PS-kustannus.

Lindström J. 2009. Models, Methodology and Challenges within Strategic Information Security for Senior Managements. Universitetstryckeriet Luleå.

Heljaste, J-M., Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J. & Vesterinen, P. 2008. Yrityksen turvallisuusopas. Helsinki: Helsingin seudun kauppakamari.

Hirsjärvi, S & Hurme, H. 2011. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki. Gaudeamus

Metsämuuroinen. 2003. Tutkimuksen tekemisen perusteet ihmistieteissä. 2. painos. Gummerus kirjapaino: Helsinki

Ojasalo K., Moilanen T. & Ritalahti J. 2009. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Roier, K. 2015. Build a security culture. United Kingdoms: IT Governance publishing.

Schein, E. 1984. Organisaatiokulttuuri ja johtaminen. Espoo: Weilin+Göös.

Sinkkonen, I. Kuoppala, H. Parkkinen, J. & Vastamäki, R. 2006. Käytettävyyden psykologia. Helsinki: Edita, IT Press.

Vilkka, H. & Airaksinen, t. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Sähköiset lähteet

Albrechtsen E. 2008. Friend or foe? Information security management of employees. Norwegian University of Science and Technology Trondheim. lainattu 30.9.2017.

https://pdfs.semanticscholar.org/40cf/125b1bb89e3d8f566708ebaa3f119e84beed.pdf

Beckers & Pape. 2016. A Serious Game on Social Engineering. Lainattu 2.12.2018.

https://mediatum.ub.tum.de/doc/1328974/1328974.pdf

Dinev & Hu. 2007. The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. Lainattu 22.8.2017.

https://www.researchgate.net/publication/255599686_The_Centrality_of_Awareness_in_the_Formation_of_User_Behavioral_Intention_Toward_Preventive_Technologies_in_the_Context_of_Voluntary_Use

Eduskunta. 2017. Valtiosopimukset. Lainattu 21.8.2017.

https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kv-jarjestot/kansainvalisen-oikeuden-tietopaketti/Sivut/Valtiosopimukset.aspx

Gaunt N. 2000. Practical approaches to creating a security culture. International Journal of Medi-cal Informatics 60, 151-157. Lainattu 21.8.2017.

https://www.sciencedirect.com/science/article/pii/S1386505600001155?via%3Dihub

Helsingin Sanomat 2013. Ulkoministeriön verkko oli täysin ulkopuolisten hallussa. Lainattu 13.10.2017.

https://www.hs.fi/kotimaa/art-2000002685298.html

Helsingin Sanomat 2018. Ranskan MAcronin ja saudiprinssi Salmanin keskustelu tallentui G20-kokouksessa. Viitattu 2.12.2018.

https://www.hs.fi/ulkomaat/art-2000005918153.html

Hendrix, M, Al-Sherbaz, A & Bloom V. Game Based Cyber Security Training: are Serious Games suitable for cyber security training? Lainattu 2.12.2018.

https://www.researchgate.net/publication/296686185_Game_Based_Cyber_Security_Training_are_Serious_Games_suitable_for_cyber_security_training

Herath & Rao. 2009. Protection motivation and deterrence: A framework for security policy compliance in organizations. Viitattu 21.8.2017.

https://www.researchgate.net/publication/220393154_Protection_motivation_and_deterrence_A_framework_for_security_policy_compliance_in_organisations

Karjalainen, M. 2011. Improving employees' information systems (IS) security behavior. Toward a meta-theory of IS security training and a new framework for understanding employees' IS security behaviour. University of Oulu. Lainattu 21.8.2017.
http://jultika.oulu.fi/files/isbn9789514295676.pdf

Kauppalehti 2013. Merkelin puhelinta kuunneltu kymmenen vuotta. Lainattu 3.12.2018.

https://www.kauppalehti.fi/uutiset/merkelin-puhelinta-kuunneltu-kymmenen-vuotta/2f00f635-cf1e-3f86-b405-cf3afcd94aa2

Kielitoimiston sanakirja. 2018. viitattu 25.11.2018.

https://www.kielitoimistonsanakirja.fi/netmot.exe?ListWord=k%C3%A4sikirja&SearchWord=k%C3%A4sikirja&page=results

Lindström J. 2009. Models, Methodology and Challenges within Strategic Information Security for Senior Managements. Universitetstryckeriet Luleå.

http://www.diva-portal.org/smash/get/diva2:990002/FULLTEXT01.pdf

Mirriam-Webster. verkkosanakirja. Viitattu 25.11.2018.

https://www.merriam-webster.com/dictionary/handbook

Puhakainen, P. 2006. A design theory for information security awareness. Lainattu 21.8.2017.

http://jultika.oulu.fi/files/isbn9514281144.pdf

Reiman,T, Pietikäinen E & Oedewald P. 2008. Turvallisuuskulttuuri, teoria ja arviointi. Espoo: VTT Publications. Lainattu 1.10.2018.

https://www.vtt.fi/inf/pdf/publications/2008/P700.pdf

Savolainen, A. 2015. Asiakirjan salassapidon tarpeet ulkoasiainhallinnossa. Viitattu 14.8.2017.

https://www.theseus.fi/bitstream/handle/10024/94926/Antti_Savolainen.pdf?sequence=1

Siponen, M. 2000. A conceptual foundation for organizational information security awareness. Lainattu 8.8.2017.

https://www.researchgate.net/publication/220208245_Siponen_M_A_conceptual_foundation_for_organizati-onal_information_security_awareness_Information_Management_Computer_Security_81_31-41

Ulkoministeriö. 2017a. Suomen edustustot ulkomailla. Lainattu 30.5.2017.

http://formin.finland.fi/Public/default.aspx?nodeid=49529

Ulkoministeriö 2018. Edustustot. Lainattu 20.11.2018.

https://um.fi/edustustot

Vuorinen, J. 2014. Parasitic Order Machine. A Sociology and Ontology of Information Securing. Lainattu 7.6.2017.

http://www.utupub.fi/bitstream/handle/10024/99059/AnnalesB392Vuorinen.pdf?sequence=2

Wiley 2018.Dummies-A Wiley Brand. Lainattu 1.12.2018.

https://www.dummies.com/

Julkaisemattomat lähteet

Ulkoministeriö 2014. Edustustojen turvallisuusohje. Ulkoministeriön sisäverkko.

Ulkoministeriön tietoturvatiimi 2016. Tietoturvallisuuden vuosisuunnitelma.

Ulkoasiainhallinnon johtajapolitiikka 2015. Ulkoministeriön sisäverkko.

Ulkoasiainministeriön johtajuusvisio 2011. Ulkoministeriön sisäverkko

Ulkoministeriön esimieskäsikirja. Ulkoministeriön sisäverkko.

Ulkoministeriön tietoturvapolitiikka 2011. Päätös tietoturvallisuudesta ulkoasianhallinnossa. Kuvaus tietoturvatoiminnan organisoinnista, vastuista ja tehtävistä.

Aarnio,J. Henkilökohtainen tiedonanto 19.06.2017. Ulkoministeriön turvallisuusjohtaja.

H5. Henkilökohtainen tiedonanto 06.7.2017. Ulkoministeriön esimies.

H1, Henkilökohtainen tiedonanto 16.6.2017. Edustuston hallintovastaava.

H2. Henkilökohtainen tiedonanto 16.6.2017. Edustuston esimies.

H3. Henkilökohtainen tiedonanto 16.6.2017. Edustuston esimies

H4. Henkilökohtainen tiedonanto 28.6.2017. Ulkoministeriön esimies

Hyppönen,M. Henkilökohtainen tiedonanto 21.9.2017. F-Securen tutkimusjohtaja.

Paananen, R. Henkilökohtainen tiedonanto 11.10.2018. Kyberturvallisuuskeskuksen varajohtaja.

Peltonen,J. Henkilökohtainen tiedonanto 25.8.2017. Ulkoministeriön turvallisuusneuvonantaja.

Puhakainen,P. Henkilökohtainen tiedonanto 15.8.2017. Valtioneuvoston kanslian tietoturvapäällikkö.

Räty, J. Henkilökohtainen tiedonanto 7.9.2018. Adecon tietoturvajohtaja.

Savolainen, A. Henkilökohtainen tiedonanto 3.12.2018. Ulkoministeriön tietotuvapäällikkö.

Kuviot

Kuvio 1 ulkoministeriö lukuina 2016 (ulkoministeriö 2016). 11

Kuvio 2 tietoturvatoiminnan organisointi ja raportointisuhteet (Ulkoministeriön tietoturvapolitiikka 2011) 13

Kuvio 3: Turvallisuuskulttuurin ja vaaratapahtumien suhde (Reiman 2008, 85)..... 17

Kuvio 4: Ohjeistuksen noudattamisen edellytyksiä (Puhakainen 2006; Roper & Grau 2006). .. 21

Kuvio 5 tietoturvakäsikirjassa käytetyt ikonit..... 35

Taulukot

Taulukko 1 Yleinen tietoturvarooli ja esimiehen tietoturvarooli 14

Taulukko 2 Esimiesten haastattelut..... 26

Liitteet

Liite 1: Teemahaastattelupohja. 46
Liite 2: Tietoturvakäsikirja sisäverkon Wikipediaan 47
Liite 3: Tietoturvakäsikirjan sisällysluettelo 48
Liite 4: Poimintoja tietoturvakäsikirjasta 49
Liite 5: Edustuston tietoturvapeli 54

Liite 1: Teemahaastattelupohja.

Teemahaastattelun teemat

1. Tietoturvallisuuden/turvallisuuskulttuurin näkyminen arjessa työpaikalla.
2. Suurimmat haasteet/vahvuudet esimiehen tietoturvavastuiden toteutumiselle
3. Ajankäyttö tietoturvallisuuden hallinnassa ja johtamisessa
4. Työkalut ja apuvälineet, jotka tukisivat esimiehen tietoturvajohtamista
5. Esimies roolimallina alaisilleen
6. Tietoturvallisuuden kytkeminen johtamisjärjestelmään ja hallinnon vuosikelloon.
7. Tietoturvallisuuden käsikirjan hyvyysvaatimukset.
8. Tietoturvatiimi yhteiskumppanina ja sen palveluiden tunnettavuus.

Liite 2: Tietoturvakäsikirja sisäverkon Wikipediaan

Sisällysluettelo

Esipuhe ulkoministeriön esimiehille
Terminologia ja sanasto
Miksi tietoa suojataan ulkoministeriössä
Luokiteltu tieto tietoturvan näkökulmasta
Henkilötiedot ja tietosuoja - tärkeämpiä kuin koskaan
Tietoturvatoiminnan organisointi

Tietoturvakäsikirjasta löytyvät symbolit

Tärkeäksi katsottua asiaa, joka sisältää lukijalle hyödyllistä tietoa.

Pohdittavia kysymyksiä.

Pohdittavat kysymykset toimivat esimiehelle aivojumppana sekä soveltuvat keskustelunaiheiksi työtiimeissä. Käsikirjasta löytyy usein linkitys foorumissa olevaan lisämateriaaliin.

Julkisuudessa esillä olleita tietoturvapoikkeamia, jotka on valittu lisäämään lukijan ymmärrystä tämän hetken tietoturvauhkista.

linkityksiä aiheeseen liittyviin ulkoministeriön muihin ohjeisiin, tarkistuslistoihin ja esimerkkeihin.

Liite 3: Tietoturvakäsikirjan sisällysluettelo

Sisällys

Esipuhe ulkoministeriön esimiehille 1
Terminologia ja sanasto 5
Miksi tietoa suojataan ulkoministeriössä? 7
Luokiteltu tieto tietoturvan näkökulmasta 11
Henkilötiedot ja tietosuoja – tärkeämpää kuin koskaan ennen 13
Tietoturvatoiminnan organisointi 15
Esimies osana tietoturvallisuusorganisaatiota 16
Tietoturvallisuuden huomioiminen vuosisuunnittelussa 19
Esimiehen johtama turvallisuustuokio 20
Kuinka vaikuttaa ja puuttua 21
Riskienhallinta 22
Hankintojen ja projektien tietoturvallisuus 24
Henkilöstöjohtaminen 26
Uusi työntekijä 26
Uuden työntekijän luotettavuuden arviointi 26
Uuden työntekijän perehdyttäminen 27
Tietoturvallisuuskoulutukset 28
Käyttöoikeuksien hallinta 28
Siirrot ja työn päättyminen 29
Tietojenkäsittelyn turvallisuus käytännön tilanteissa 30
Tiedon elinkaariajattelu eli tiedon luokittelu, säilyttäminen ja hävittäminen 31
Työvälineet 33
Työtilat 34
Etätyöskentely 35
Kokousturvallisuus 36
Matkaturvallisuus ja siirto ulkomaille 37
Kuinka havaita tietoturvapuutteita ja tapahtumia 39
Tietoturvarikkomuksen seuraamusmenettely 40
Tietoturvapoikkeaman raportointi 41

Tietoturvakäsikirjasta löytyvät symbolit:

 Tärkeäksi katsottua asiaa, joka sisältää lukijalle hyödyllistä tietoa.

 Pohdittavia kysymyksiä. Pohdittavat kysymykset toimivat esimiehelle aivojumppana, sekä soveltuvat keskustelunaiheiksi työtiimeissä. Käsikirjasta löytyy usein linkitys foorumissa olevaan lisämateriaaliin.

Julkisuudessa esillä olleita tietoturvapoikkeamia, jotka on valittu lisäämään lukijan ymmärrystä tämän hetken tietoturvauhkista.

 linkityksiä aiheeseen liittyviin ulkoministeriön muihin ohjeisiin, tarkistuslistoihin ja esimerkkeihin. Linkitetty asiakirja tai sivu löytyy foorumin hakutoiminnolla kappaleessa mainitulla #hakusanalla.

Liite 4: Poimintoja tietoturvakäsikirjasta

Esimiehen johtama turvallisuustuokio

Esimiehen tehtäviin kuuluu olennaisesti myös uusista ohjeista ja määräyksistä tiedottaminen. Käytännössä toimivaksi havaittu menetelmä on, että esimies selvittää työntekijöille toistuvasti tietoturvaohjeiden merkityksen ja sisällön.

Esimiehen johtama turvallisuustuokio on hyvä työkalu keskustella tietoturvallisuudesta työyhteisössä, sekä ylläpitää keskustelukanavaa jo ohjeistetuista tietoturvallisuuteen liittyvistä asioista. Esimies voi halutessaan lisätä koulutushetken teemana jo olemassa olevaan kokoukseen. Koulutushetken voi brändätä esimerkiksi turvallisuustuokioksi viikkopalaverin tai kuukausipalaverin kylkeen.

Esimiehen johtamissa koulutushetkissä on se etu, että hän tuntee alaisensa persoonina ja ymmärtää mitä heidän työrooleihinsa sisältyy. Ulkopuolisen tietoturvallisuusasiantuntijan johtama koulutus ei välttämättä pureudu yhtä syvälle yksikkönne tehtävänkuvan tarjoamiin erityispiirteisiin.

Esimiehen ei tarvitse olla tietoturvallisuuden asiantuntija. Hän varaa aikaa yhteiseen keskusteluun, ja tarvittaessa toimii puheenjohtajana ja sparraajana. Jos keskustelun aikana nousee esiin kysymyksiä, joihin ei löydetä vastauksia, ne kirjataan ylös ja niihin palataan seuraavassa turvallisuustuokiossa.

Esiin tulevat kysymykset voi lähettää sähköpostitse: <osoite>@formin.fi. Vastaamme niihin mielellämme.

Tiedustele tietoturvatiimiltä koulutusmateriaalia turvallisuustuokioihin. Tarjolla on myös erillinen tietoturvapeli.

Tarkistuslista turvallisuustuokion järjestämiseen:

Turvallisuustuokioon varataan noin 45 minuuttia ja se ajoitetaan ajankohtaan, jolloin mahdollisimman moni työntekijöistä kykenee siihen osallistumaan.

- Tapaamisessa osallistujia on motivoitava ja saatava heidät näkemään tietoturvallisuudesta koituvat hyödyt - ei vain työnantajan kannalta, vaan myös oman työnsä varmistamisen kannalta. Esimiehen kannattaa peilata keskustelua alaistensa konkreettisiin työtehtäviin.
- Asiat on esitettävä yksinkertaisesti ja selkeästi. Keskustelussa voi käyttää avoimia kysymyksiä: "Miten tämä asia voitaisiin ratkaista?" tai suoria kysymyksiä "Liisa, miten tämä näkyy sinun työnkuvassasi? Jaakko, milloin olet viimeksi törmännyt tähän asiaan?".
- Koulutuksessa on hyvä korostaa, mitä ovat kunkin vastuut liittyen aihealueeseen. Mitä haasteita käsiteltävään asiaan liittyy ja mitkä ovat edellytykset haasteiden selättämiselle?
- Koulutuksen sisältö on hyvä pitää ajankohtaisena. Aiheita löytyy mm. UM tietoturvan aihesivulta, sekä seuraamalla ajankohtaisia uutisia.
- Koulutushetken jälkeen esimiehen on hyvä tarkkailla toimintaa, josta on juuri keskusteltu. Oikeasta toiminnasta palkitaan positiivisella palautteella. Virheelliseen toimintaan tartutaan välittömästi ja selvitetään tapahtuman syy-yhteydet, jotta se ei toistuisi tulevaisuudessa.

Kuinka vaikuttaa ja puuttua

Tietoturvallisuuteen liittyy valitettavan paljon asennekysymyksiä. Se on aihealueena myös abstraktimpi kuin muut turvallisuuden osa-alueet. Syy tähän on yksinkertainen: tietoon kohdistuvat uhat ovat yleisesti ottaen moninaisia ja haastavia ymmärtää.

Esimiehen yhtenä tehtävänä on kaikesta huolimatta luoda puitteet tietoturvalliselle työskentelylle, myös normaalitilanteissa. Havaittuihin tietoturvallisuuspoikkeamiin on puututtava välittömästi, kuten mihin tahansa muuhunkin työssä havaittuun virheeseen. Palaute on tehokkainta, jos se välitetään välittömästi. Jos esimiehen palaute välittyy vasta seuraavassa kehityskeskusteluissa, se on se menettänyt jo suuren osan merkityksestään.

Esimiehen on tärkeätä ymmärtää ne seikat, jotka ovat johtaneet virheeseen tai puutteeseen. Oliko virhe tahaton vai tahallinen? Syntyikö virhe puutteellisesta ymmärryksestä, kiireestä? Vaikuttiko virheeseen osaltaan työympäristöön ja työkaluihin liittyvät haasteet? Voidaanko kyseinen virhe välttää tulevaisuudessa vaikuttamalla ongelman juurisyihin?

Turvallisuuskulttuuria ajatellen avoin ja oppiva työilmapiiri on parempi kuin rangaistuksen pelosta kärsivä virheitään peittelevä työyhteisö. On luonnollista, että virheitä tapahtuu. Se on luonnollista. Organisaatiolle parempi vaihtoehto on, että tapahtuneista virheistä uskalletaan raportoida, jotta korjausliikkeet saadaan käynnistettyä välittömästi. Tapahtuneet virheet ja haasteet ovat itse asiassa esimiehelle arvokasta tietoa lisäkoulutuksen suuntaamiseksi ja resurssoinnin keskittämiseksi.

Tutkimuksen mukaan sosiaalinen paine kollegoilta ja esimieheltä on voimakkaasti vaikuttava tekijä, joka vaikuttaa työntekijän asenteisiin noudattaa turvallisuusohjeita. Jos esimies korostaa tietyn tietoturvaohjeen merkitystä (otetaan esimerkiksi puhtaan pöydän politiikka) ja saa pääosan työtiimistä noudattaa omaa esimerkkiään vaatii oman työpöydän paperiarkistoksi jättäminen erityistä määrätietoisuutta.

Erityisesti uusiin työntekijöihin on helpointa vaikuttaa positiivisesti, tartuttamalla heihin aikaisin siemen turvallisuuskulttuurista. Vastakkaisesti, jos esimies välittää sanattoman viestin, ettei arvosta turvallisuusohjeita eikä noudata niitä omassa työssään, ei hän voi olettaa ohjeiden noudattamista myöskään työntekijöiltään.

Hankintojen ja projektien tietoturvallisuus

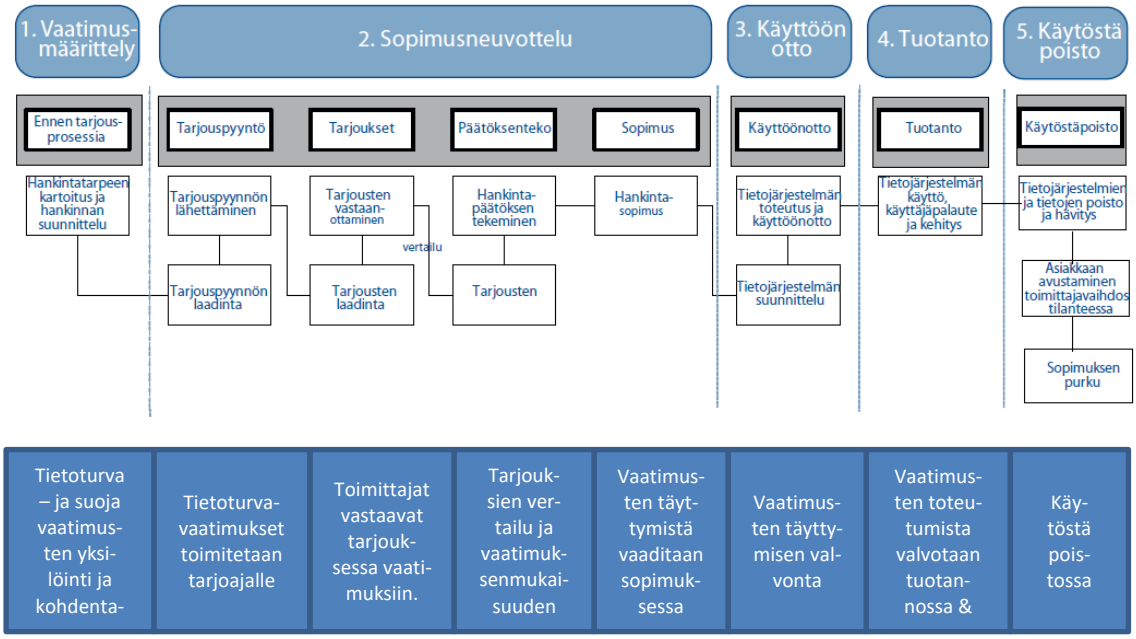
Tietoturva- ja tietosuoja-asiat liittyvät lähes kaikkiin hankintoihin. Joko kyse on laite– tai järjestelmähankinnasta, jossa on tietojärjestelmäkomponentteja tai palveluhankinnasta, joka vaatii ulkopuolisen yrityksen henkilökunnan palvelu- tai huoltotoimenpiteitä toimitiloissa tai pääsyä ulkoministeriön tietoon.

Ulkoministeriössä hanketta hallinnoimaan perustetaan erillinen hankeorganisaatio, joka eroaa normaalista linjaorganisaatiosta ja on vastuussa hankkeen kaikista osa-alueista (mukaan luettuna tietoturvallisuus), kunnes hankeen tuotos on valmis luovutettavaksi linjaorganisaation ja tulevan omistajan käyttöön. Jotta hanke kykenee hallitsemaan siihen liittyvät tietoturvavaatimukset, on sen nimitettävä tietoturvasta vastaava projektitiimin jäsen.

Tietoturvakysymysten huomioiminen ICT-hankintaprosessissa vaatii tietoturvallisuuden erityisosaamista. Hankintaa ajavan esimiehen onkin tärkeätä kytkeä tietoturvatiimi mukaan tietoturvatarpeita sisältävään hankintaan mahdollisimman nopeasti. Etupainotteinen tietoturvallisuuden huomioiminen maksaa pitkällä aikavälillä moninkertaisesti itsensä takaisin.

Hankinnoissa tietoriski on aina tilaajalla. Valtionhallinnon hankinnoissa on huomioitava tietoturvataso, joka on käytännössä vähintään tietoturvallisuuden perustaso. Erityistä harkintaa on harjoitettava hankinnoissa, joissa tietoa tallennetaan pilvipalveluihin.

Onnistunutta hanketta edeltää aina vaatimusmäärittely ja siihen liittyvä riskianalyysi. Vaatimusmäärittelyssä tarkastellaan hankintaan liittyviä toiminnallisia ja ei-toiminnallisia vaatimuksia, ml. tietoturvavaatimuksia. Riskianalyysissä tarkastellaan kriittisesti hankkeen onnistumisedellytyksiä.



Tietosuoja ja tietoturvallisuus hankinnan ja tietoturvatiimin näkökulmasta

Vaatimusmäärittely

Vaatimusmäärittely on onnistuneen tietojärjestelmän kilpailutuksen ja hankinnan perusedellytys – se määrittelee mitä vaatimuksia projektin täytyy täyttää ja miksi. Riittämätön vaatimusten määrittely on yleisimpiä yksittäisiä syitä ohjelmistoprojektien epäonnistumiseen.

Vaatimusmäärittelyn vähimmäisvaatimukset – tarkistuslista, sekä *#Sovellusten hankinnan, kehityksen ja ylläpidon tietoturva – ja tietosuojaohje*.

Ulkoministeriön rotaatio luo esimiesrooleissa toimiville järjestelmien omistajille erityisiä haasteita. Voi syntyä tilanne, joissa uuteen rooliinsa siirtyvä päällikkö ei ole tietoinen roolin mukana siirtyvistä järjestelmän omistajarooleista.

Turvallisuussopimus
Hankinnoissa on kirjattava sopimuksiin hankkija ja toimittajaosapuolen vastuut ja velvollisuudet. Tieto- ja viestintäteknologian hankinnoissa, joihin liittyy luokitellun tai arkaluontoisen tiedon käsittelyä, on laadittava erillinen turvallisuussopimus. Turvallisuussopimuksen laajuus ja tarkkuus muotoutuu järjestelmässä käsiteltävän tiedon kriittisyydestä. Myös hankinnoissa, joihin ei liity arkaluontoisen tai luokitellun tiedon käsittelyä, on hyvä huomioida turvallisuusriskejä pääsopimuksen yhteydessä.

Jos hankintaan liittyy henkilötietojen käsittelyn ulkoistamista, on sopimuksellisesti huomioitava ulkoministeriön velvollisuudet rekisterinpitäjänä sekä määritellyn henkilötietojen käsittelijän velvollisuudet, tietojen säilytyspaikan sekä henkilötietojen käyttötarkoituksen (esim.

henkilöstöhallinta, palkanmaksu tms.) osalta. Esimiehen on tärkeätä päivittää myös olemassa olevat sopimukset vastaamaan EU tietosuoja-asetuksen ehtoja.

Ruotsin ajoneuvohallinto ('Transportstyrelsen') ulkoisti tietotekniikkapalvelunsa IBM:lle huhtikuussa 2015 ja sen seurauksena Tshekissä toimivat yhtiön teknikot saivat vapaan pääsyn ajoneuvohallinnon ajoneuvo- ja ajokorttirekistereihin. Teknikoiden taustoja ja rikoshistoriaa ei tarkistettu turvallisuusselvityksillä ja heille oli myönnetty pääsyoikeudet rekisterien arkaluontoisiin tietoihin. Eräs synkimmistä esitetyistä uhkakuvista oli se, että piiloidentiteeteillä työskentelevien puolustusvoimien ja turvallisuuspoliisin virkamiesten henkilöllisyys olisi voinut paljastua tietovuodon seurauksena. Ruotsin pääministeri Löfven tiedotti pian asian päädyttyä julkisuuteen, että ajoneuvohallinto uudistetaan tietovuodon seurauksena kokonaan. Löfven tiedotti myös, että hallitus alkaa työskennellä sen eteen, että ICT-järjestelmiejn ulkoistamista rajoitetaan tulevaisuudessa, vastaavien tietopoikkeamien estämiseksi. (YLE 2017)

Vahti 3/2011, Sovellusten hankinnan, kehityksen ja ylläpidon tietoturva – ja tietosuojaohje.

Etätyöskentely

Ulkoministeriö kannustaa työnantajana tietoturvalliseen etätyöskentelyyn. Etätyöskentely perustuu ulkoministeriössä kirjalliseen päätökseen. Kirjallisessa etätyösopimuksessa esimies ja hänen alaisensa sopivat etätyöhön soveltuvasta etätyöskentelypaikasta. Etätyöpaikan on tarjottava edellytykset työskentelyyn ilman huovattavaa riskiä, että käsitellyt tiedot päätyvät vääriin käsiin. Etätyöpaikaksi voi soveltua työntekijän koti tai kesäasunto, mutta ei esimerkiksi suosikkikahvila tai lentokone. Etenkin julkisessa liikenteessä on aina riski, että takanasi istuva matkustaja voi lukea tietokoneen ruutua olkasi ylitse. Riski työaseman varkaudelle on myös korostunut, kun työskentelet ministeriön ulkopuolella. Etätyösopimuksessa hyväksytetään etätyöpaikan lisäksi myös työhön käytettävät työvälineet ja se tietoaineisto, jota työntekijä saa etätyöpaikalla käsitellä.

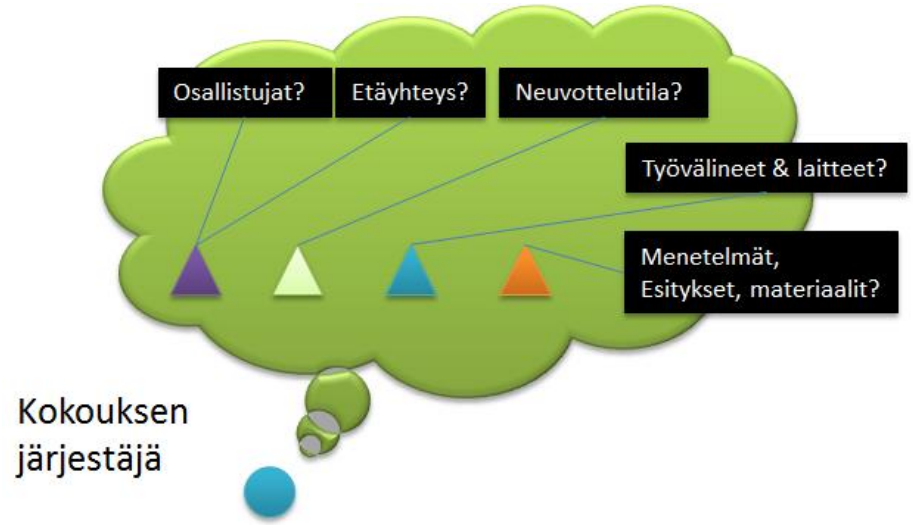
 Lähtökohtaisesti suojaustason ST III tai sitä korkeimmin luokitellun aineistojen sekä kansainvälisten turvaluokiteltujen tietoaineistojen käsittely viraston ulkopuolella on kielletty.

 Etätyöpaikkasi on pääsääntöisesti oma kotisi. Etätyöpaikassa sinun täytyy kyetä hallinnoimaan ketkä liikkuvat tiloissa, sekä huolehtimaan tilan lukituksesta ja työvälineiden ja asiakirjojen turvallisesta säilytyksestä, kun lopetat työskentelyn.

Katso:  #Etätyön tietoturvaohje

Kokousturvallisuus

Kokouksen järjestäjä on vastuussa tiedon suojauksesta kokouksen ajan. Kokouksen järjestäjän on ensin määritettävä kokoukselle suojaustaso (ST). Suojaustaso määrittyy korkeimmin luokitellun tiedon mukaan, jota kokouksessa mahdollisesti käsitellään. Kokouksen järjestäjä varmistaa tämän jälkeen, että kaikki kutsutut henkilöt omaavat luvan käsitellä heidän tietoonsa tulevaa tietoa (kansainvälisten velvoitteiden osalta ajantasaiset PSC:t). Kokousvälineiden ja kokouspaikan täytyy mahdollistaa edellytykset luottamukselliselle keskustelulle. Jos keskustelussa käsitellään ST III/EU-C/NC tai sitä korkeammin salassa pidettäviä keskustelunaiheita on suositeltavaa jättää älypuhelimet ja henkilökohtaiset älylaitteet toiseen huoneeseen.



Turvaluokitus	ST IV / EU-R / NR	ST III / EU-C / NC	ST I-II I / EU-S-TS / CS-CTS
Tila	Kokoushuoneen tarkistaminen: - Verhot kiinni - Ei ulkopuolisia tilassa eikä sen välittömässä läheisyydessä	Kuten IV. - Huomioi mahdolliset nauhoittavat AV-laitteet, kuten puhelimet.	Kuten III. - Kokoushuoneessa sähköllä toimivia laitteita. Varaa suojattu neuvotteluhuone, jos käytettävissä.
Osallistujat	Osallistuvilla on oikeus ja tarve osallistua kokoukseen. Kokoukseen osallistuneiden henkilöllisyys tarkistetaan.	Kuten ST IV.	Kuten ST IV. Osallistujien nimet kirjataan luokiteltujen asiakirjojen kontrollikirjaan
Laitteet	Kokousmuistiinpanot laaditaan UM-kannettavalla. Video-neuvottelumahdollisuus ST IV tietoon saakka UM hyväksymillä laitteilla.	Kokousmuistiinpanot laaditaan pysyvästi verkosta irti olevalla työasemalla. Henkilökohtaiset laitteet jätetään tilan ulkopuolelle. Viraston laitteet jätetään tilan ulkopuolelle järjestäjän harkinnan mukaan.	Kuten ST III. Kaikki sähköiset laitteet jätetään tilan ulkopuolelle, niille tarkoitettuun säilytystilaan.
Menetelmät, esitykset ja materiaalit	Esityksiä ei tallenneta ilman järjestäjän lupaa. Kokousmateriaalit ja muistiinpanot jätetään lukittuun tietoturva-astiaan. Huomioidaan äänen käyttö ja äänieristys.	Kuten ST IV. Kokousmateriaalit ja muistiinpanot hävitetään hyväksytyllä silppurissa. Jos kokouksessa jaetaan luokiteltua materiaalia, tarjoa edellytykset materiaalin turvalliseen säilytykseen kokouksen jälkeen.	Kuten ST III. Ei käytetä sähköisiä esitysmuotoja, mikäli suojattu neuvottelutila ei ole käytettävissä.

Taulukko. Harkittavia asioita Kokousturvallisuuden suhteen, tarkistuslista.

Liite 5: Edustuston tietoturvapeli

Abstrakti

Edustuston tietoturvapelin tarkoitus

Edustuston tietoturvapeli pohjautuu Beckersin & Papen (2016) turvallisuuspeliin A Serious Game on Social Engineering. Pelin runko on siirretty edustuston maailmaan ja peliin on lisätty myös riskejä fyysisen turvallisuuden maailmasta.

Edustuston tietoturvapelin tarkoitus on kehittää edustuston henkilöstön turvallisuustietoisuutta pelillistämisen keinoin. Peli on tarkoitettu pelattavaksi joko ulkoministeriön tietoturvatiimin tai edustuston esimiehen ohjauksessa. Peli asettaa edustuston henkilöstön jäsenet vuorollaan niin sanotun pahantahtoisen toimijan rooliin ja vastakkain edustuston olemassa olevia turvallisuusjärjestelyitä vastaan. Pelin aikana voidaan havaita puutteita arkiseen työhön liittyvissä järjestelyissä sekä ymmärtää paremmin niitä keinoja, joita huijarit ja rikolliset käyttävät muun muassa käyttäjän manipulaation (’social engineering’) keinoin. Tietoturvapeliä voidaan käyttää myös riskienhallintaa tukevana työkaluna.

Neuvoja pelin kulkuun

Suurin hyöty edustuston tietoturvapelistä syntyy, jos edustusto on mukana laatimassa omiin erityispiirteisiinsä liittyviä erikoiskortteja. Niiden avulla pelistä kautta löytyvät havainnot ovat entistä merkittävämpiä.

Pelin aikana on vältettävä loukkaamasta kollegoita ja keskusteltava havaituista puutteista vilpittömästi ja ketään syyttämättä. Pelissä voi olla ajoittain tarpeellista määrittää huijaus kohdistumaan tietyssä roolissa toimivaa henkilöä vastaan. Tästä hyvä esimerkki voisi olla:

”lähetän huijauslaskun kiinteistövastaavalle paikallisen hissihuoltoyrityksen nimissä juuri kun hän on vuosilomalla. Tuuraaja maksaa sen luultavasti enempiä kyselemättä, kunhan lomakkeessa on oikeat logot.”

Huonoa henkeä osoittava esimerkki voisi taas olla:

”Soitan huijaussoiton <henkilölle x>, koska hän on helpoiten huijattava henkilö edustustossa!”

Pelin aloitusjärjestelyt

Tietoturvapelin voi pitää muun henkilöstöpalaverin yhteydessä tai varata sille oman erillisen aikansa. Pelille kannattaa varata aikaa 45 minuutista 90 minuuttiin. Peliä varten tarvitaan:

Pelilauta (optionaalinen) – Pelilauta on visualisointia helpottava kartta, joka kuvastaa edustustorakennusta. Edustuston hätäpoistumiskuva sopii tähän tarkoitukseen varsin hyvin. Pelilaudan voi myös heijastaa kannettavalta piirtoheittimelle tai esittää näytöltä.

Pelinappulat (optionaalinen) – Edustuston työntekijöiden asettaminen kartalle heidän normaaleihin työpisteisiinsä on myös hyvä visualisointiapu.

Tavoitekortit – Tavoitekortit sisältävät kunkin pelivuoron rikollisen tavoitteen. Tavoite voi olla esimerkiksi a) haittaohjelman toimittaminen edustustoon b) Edustustoon sisäänpääsy valehtelemalla tai jokin muu hyökkääjää hyödyttävä tavoite.

Hyökkäyskortit – Hyökkäyskortit sisältävät työkaluja tai työtapoja, joilla hyökkäyksen tavoitteisiin pyritään.

Heikkouskortit - Heikkouskortit sisältävät etupäässä ominaisuuksia, joita huijarit käyttävät käyttäjän manipulaatiossa. Nämä ominaisuudet liittyvät ihmisluontoon ja sosiaalisen kulttuurimme kehitykseen, joka ei toimisi ilman luottamusta toisiimme.

Poikkeustilakortit (optionaalinen) – Pelistä voi tehdä vielä kiinnostavamman nostamalla ajoittain poikkeustilakortin. Kortit ovat tilanteita, joissa edustuston arki ei noudata rutiinia. Näissä tilanteet monesti avaavat ovia pahantahtoiselle toimijalle. Poikkeustiloja voisivat olla esimerkiksi: sähkö- tai verkkokatkos, kansallinen juhlapyhä tai väistötiloihin siirtyminen vesivahingon vuoksi jne.

10 Pelin kulku

Korttien nosto:

Ensimmäinen hyökkäysvuorossa oleva pelaaja nostaa: tavoitekortin, 2 hyökkäyskorttia ja 3 heikkouskorttia. Hän voi päättää nostaako poikkeustilakortin vai jättääkö sen nostamatta.

Esimerkki (korttien nosto):

Nostetut kortit ovat: **Tavoitekortti**: ”Haittaohjelman asennus ulkoministeriön työasemalle”.

Hyökkäyskortti (1): ”haittaohjelma muistikortilla**”, hyökkäyskortti (2):** ”Asuleikki ja valehteleminen”

Heikkouskortti (1): ”häiriön luominen”, **heikkouskortti(2)**: ”laiskuus” ”Heikkouskortti (3): ”tarve ja ahneus”

Tarinan kerronta:

Pelaaja lukee kortit ja keksii hyökkäyksen, jonka voi suorittaa yhdellä tai useammalla hyökkäys- ja heikkouskortilla.

Esimerkki (tarinan kerronta):

”Tavoitteeni on saada joku asentamaan haittaohjelma ulkoministeriön työasemalle. Käytän hyökkäyskortti valeasun. Valeasu-kortin kautta tekeydyn apua tarvitsevaksi turistiksi päästäkseni sisälle lähetystön konsulaattiin. Pudotan siellä muistikortin, jossa haittaohjelma on ja toivon, että joku, joka on liian laiska lukemaan tietoturvaohjeita, nostaa sen ja avaa sen työasemallaan.”

Tarinan arvioiminen:

Kun hyökkäysvuorossa oleva pelaaja kertoo tarinansa, kaikki muut pelaajat arvioivat sen mahdollisuudet onnistua. Jos tarinan hyökkäys on heidän mielestään todennäköinen, he myöntävät tarinan kertojalle **2 pistettä.** Jos he katsovat, että tarina voisi onnistua vain harvoin, he myöntävät tarinan kertojalle **1 pisteen.** Jos tarinan kuvastama hyökkäys on mahdoton tai äärimmäisen epätodennäköinen, he eivät myönnä pisteitä.

(!) *Jos kerrottu tarina katsotaan olevan 0 tai 1 pisteen arvoinen, eli mahdollinen mutta epätodennäköinen ja toinen pelaaja keksii siihen lisän tai pienen muutoksen, joka tekee siitä kaikkien mielestä 2 pisteen arvoisen, saa hän itselleen 1 ylimääräisen pisteen.*

Kun tarina on arvioitu, lasketaan pisteet ja seuraava pelaaja siirtyy hyökkääjän rooliin ja tarinansa päättänyt pelaaja siirtyy arvioitsijaksi.

Esimerkki (tarinan arviointi):

arvioitsija 1: ”Hyökkäys ei onnistuisi koska edustustossa on ehdoton sääntö, ettei asiakastiloista löytyviä löytötavaroita kytketä kiinni tietokoneisiin. 0-pistettä!”

arvioitsija 2: ” Itse asiassa kyllä minä tiedän, että noita löydettyjä muistitikkuja on tarkistettu, vaikka ohjeet kieltävätkin, etenkin jos joku tulee myöhemmin kertomaan hukanneensa moisen. 2 pistettä”

arvioitsija 3: ”aika harvinaista moinen on etenkin, kun emme käytä tuuraajia. Kaikki ovat läpikäyneet tietoturvan verkkokoulutuksen, jossa tuo selkeästi kerrotaan 1 piste”

Tarina sai täten **3 pistettä** ja vuoro siirtyy seuraavalle pelaajalle ja tarinansa päättänyt pelaaja siirtyy arvioitsijaksi. Tässä kohtaa muut pelaajat voivat pyrkiä kehittämään hyökkäystä tehdäkseen siitä todennäköisempi.

Pelin päättäminen ja havaintojen arviointi

Kun peli on ohitse ja kaikki ovat saaneet toimia vuorollaan hyökkääjinä vähintään kerran. Tämän jälkeen havaintojen arviointia varten on hyvä varata vähintään 15 minuuttia. Kaikki pisteitä saavuttaneet tarinat käydään lävitse vielä kerran ja arvioidaan, löytyykö niiden kautta konkreettisia riskejä, joita vastaan ei ole varauduttu. Havaitut konkreettiset puutteet on hyvä huomioida omassa toiminnassa, lisätä oman toiminnon tietoturvakorttiin ja tiedottaa niistä ulkoministeriön tietoturvatiimiä ja turvallisuusosastoa.

Heikkouskortit – eli miksi me lankeamme huijauksiin?

Saamme kiittää tästä ominaisuudesta evoluutiota sekä sosiaalisen kulttuurimme kehitystä. Yhteiskunta ei kykenisi toimimaan ilman luottamusta jäsentensä välillä. Me luotamme luontaisesti siihen, että posti pyrkii kuljettamaan kirjeemme perille saakka, me luotamme siihen, että kotiimme tilaamamme huoltomies on ammattitaitoinen, eikä varasta pöytähopeitamme, me luotamme siihen, että vakuutuksemme kattavat sopimusehdoissa määritellyt vahingot jne.

Seuraava listaus on kerätty useamman järjestelmäturvallisuuden tutkijan julkaisemista päätelmistä. Hieman mahtipontisenakin olettamana on se, että jokainen ihmisluontoa hyväksikäyttävä huijaus voidaan yhdistää yhteen ja useampaan alla listattuun inhimilliseen ominaisuuteen.

Huijauksille altistavia käytösperiaatteita:

Häiriön luomisen periaate	Rikollinen luo harhautuksen, joka kiinnittää uhrin huomion muualle kyetäkseen toimimaan vapaasti tämän selän takana.
Sosiaalisen yhteensopivuuden periaate	Yhteiskunta opettaa yksilöitä olemaan kyseenalaistamatta auktoriteetteja. Rikollinen hyväksikäyttää tätä seikkaa tekeytymällä uhrin kunnioittamaksi auktoriteetiksi.
Lauma periaate	Ihmiset ovat sosiaalisia eläimiä. Jos kaikki ympärilläsi jakavat saman riskin, niin seuraat herkästi esimerkkiä.
Epärehellisyyden periaate	Jos saat uhrisi rikkomaan lakia, voit käyttää tietoa hyväksesi ilman pelkoa, että hän ilmiantaa sinut.

Tarpeen ja ahneuden periaate	Rikollinen selvittää, mitä hänen uhrinsa todella tarvitsee ja haluaa, käyttäen tietoa hyväksi manipulaatiossaan.
Kiireen periaate	Rikollinen luo tai hyväksikäyttää uhrinsa työtehtävään liittyvää kiirettä ja painetta saadakseen hänet noudattamaan vähemmän turvallisia työtapoja.
Luontainen halu olla hyödyllinen	Suurin osa meistä on kasvatettu olemaan auttavaisia ja solidaarisia. Rikollinen käyttää tätä ominaisuutta hyväkseen tietoa kalastaessaan.
Laiskuus	Ihmisen laiskuus yhdistettynä luontaiseen olettamaan, ettei mitään pahaa tapahdu juuri hänelle, saa hänet laistamaan turvallisista työskentelymalleista.
Pelko jonkin arvokaan menettämisestä	Rikollinen voi hyväksikäyttää työntekijän pelkoa joutumisesta ongelmiin tekeytymällä tahoksi, joka voi aiheuttaa hänelle ongelmia. Tarkoitus on yleensä saada työntekijä rikkomaan organisaation sääntöjä.
Taipumus luottaa ihmisiin	Osa ihmisluontoa on luottaa toisiin ihmisiin kunnes he osoittavat, etteivät ole luottamuksen arvoisia.
Uteliaisuus	Rikollinen voi luoda tilanteen, jossa uhrin uteliaisuus ylittää hänen varovaisuutensa. Tämä on usein käytetty keino välittää sähköpostitse ja sosiaalisen median kautta haittaohjelmia.
Syyllisyys	Rikollinen voi käyttää uhrin syyllisyyden tuntoa hyväkseen, esimerkiksi hyväntekeväisyyteen liittyvissä huijauksissa. Hän voi myös luoda ensin olosuhteet, joissa uhri rikkoo (oletetusti) häntä vastaan ja syyllisyyden tunteen pakottamana suorittaa vastapalveluksia.
Tuntemattoman pelko	Ihmiset pelkäävät luontaisesti tuntematonta. Mukavuusalueen ulkopuolelle astuminen on monelle ikävä tilanne. Rikollinen voi luoda tilanteen, jossa uhri tuntee symbolisesti hukkuvansa ja takertuu hyökkääjän apuun kuin psykologiseen pelastusrenkaaseen selviytyäkseen tilanteesta kuiville.
Pelko jonkin menettämisestä	Psykologisesti tunne saavutetun edun tai asian menetyksestä on kaksi kertaa voimakkaampi kuin alkuperäinen hyvänolontunne edun saavuttamisesta. Rikollinen voi uhata uhrille tärkeätä asiaa (esim. kiristämällä) saadakseen hänet valtaansa.

Vastuun jakaminen	Yhteinen vastuu on heikko vastuu. ”*joku muu tekee asialle jotain*”-ajattelu johtaa helposti tilanteeseen, jossa kukaan ei suorita tarvittavia toimenpiteitä. Rikolliselle tämä on hyödynnettävä mahdollisuus.
Tietämättömyys / huolimattomuus	Tietotaidon / motivaation puute on mahdollisesti vakavin listatuista, potentiaalisesti hyväksikäytettävistä henkisistä käytösmalleista. Nämä luovat puitteet kaikkien muiden listattujen ominaisuuksien onnistuneelle hyväksikäytölle.

Hyökkäyskortit:

Lista hyökkäyskorteista on esimerkillinen. Organisaation on hyvä laatia omaan toimialaansa tai aiempien turvallisuuspoikkeamien pohjalta oma hyökkäyskorttipakkansa.

Phishing	Tekeytyminen luottamusta herättäväksi tahoksi saadaksesi uhrisi suorittamaan haluamasi toiminnon (esimerkiksi sähköpostin linkin klikkauksen)
Tailgating	Kiinteistön suljetuille alueelle sisään pyrkiminen seuraten kiinteistön henkilökunnan perässä.
Asuleikki ja näyttelemi-nen	Tekeydy luottamusta nauttivaksi henkilöksi joko fyysisesti tai puhelimitse.
Avainten kopiointi	Hankit hetkeksi avaimen haltuusi ja luot siitä kopion. Kyse voi olla kulkukortista tai mekaanisesta avaimesta.
Haittaohjelma muisti-tikulla	Hallussasi on haittaohjelma, jonka voit antaa henkilölle tai jättää lojumaan paikkaan, josta se varmasti löydetään.
Tekaistu kirje/faksi	Väärennät uskottavan näköisen kirjeen tai faksin saadaksesi uhrisi uskomaan jotain, mikä ei ole totta.
Näpistys	Sinulla on näppärät sormet, joilla voit näpistää esillä olevia pieniä esineitä.
Sisäpiiriläinen	Sinulla on sisällä edustustossa kontakti, joka voi tehdä sinulle pieniä palveluksia.
Roskien tonkiminen	Jätteen mukana voidaan heittää pois hyökkääjälle hyödyllistä tietoa.

Verkkosivun saastuttaminen	Saastutat sivuston, jolla uskot uhrisi vierailevan saadaksesi hänet lataamaan sieltä haittaohjelman tai syöttämään sille tarvitsemaasi tietoa.
Palveluhenkilöstö	Palveluhenkilökunta (siivoojat, huoltomiehet) voivat liikkua useissa tiloissa ilman valvontaa.
Kolmannen osapuolen auktoriteetti	Mainitset uhrin tunteman auktoriteetin nimen saadaksesi hänet tekemään jotain mitä hän ei normaalisti tekisi.
Murto yöaikaan	Monesti vähemmän hienovaraiset keinot ovat tehokkaimpia. Pidetäänkö keittiön ikkunoita auki kesäkuumalla vai onko rikosilmoitinjärjestelmä ollut epäkunnossa ja pidemmän aikaa?

Poikkeamakortit:

Lista poikkeamakorteista on esimerkillinen. Organisaation on hyvä laatia omaan toimialaansa tai aiempien turvallisuuspoikkeamien pohjalta omat poikkeamakorttinsa.

Poliittinen paine kiireellisestä raportoinnista	Jotain on tapahtunut ja asioita täytyy tehdä kiireellä. Tämä saattaa vaikuttaa normaaliin varovaisiin ja turvallisiin työskentelymetodeihin.
Hybridivaikuttaminen	Organisaatiota vastaan on käynnissä onnistunutta hybridivaikuttamista, jolla on seurauksensa.
Sähkö- tai verkkoyhteydet ovat alhaalla	Normaalit työvälineet eivät ole käytettävissä.
Muutostila	Käyttöön on juuri saatu uusi työväline tai työpiste, joka on kaikille tuntematon ja sen käyttö saattaa altistaa virheille.
Tietovuoto	Joku tai jokin välittää tietoa taholle <X>, mikä vaikuttaa normaaliin toimintaan.
Rotaatio	Henkilöstössä on tapahtunut juuri vaihdos ja uusi/uudet paikalle lähetetyt eivät vielä tunne paikallisia toimintatapoja ja yhteistyökumppaneita, mikä altistaa virheille.