LAUREA

Tietoturvapolitiikan implementoinnin kehittäminen

Hämäläinen, Lauri

2010 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvapolitiikan implementoinnin kehittäminen

Hämäläinen, Lauri
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Joulukuu, 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Hämäläinen, Lauri

Tietoturvapolitiikan implementoinnin kehittäminen

Vuosi 2010 Sivumäärä 26

Opinnäytetyössä tutkittiin erään Pohjoismaissa toimivan yrityksen tietoturvapolitiikan täytäntöönpanoa. Yrityksen aikaisempi toimintatapa tietoturvapolitiikan käytännön täytäntöön panemisessa (usein puhekielessä myös jalkauttamisessa), ei ollut tyydyttävällä tasolla, joten tällä aiheella oli opinnäytetyölle sopivia aineksia. Opinnäytetyön lähtökohtana oli haastatteluiden ja alan kirjallisuuden pohjalta luoda näkemys siitä, missä tilassa tietoturvapolitiikan jalkauttaminen tilaajayrityksessä oli ja missä sen haluttiin tulevaisuudessa olevan. Lisäksi tilaajayrityksen tietoturvallisuushenkilöstö halusi, että mikäli opinnäytetyön päätteeksi löytyisi mahdollisia uusia keinoja jalkauttamisen parantamiseksi, niiden käyttöönottaminen uudessa tietoturvapolitiikkasuunnitelmassa otettaisiin vakavasti harkintaan.

Alun perehtymis- ja tutkimusvaiheessa käytettiin pääsääntöisesti Petri Puhakaisen Oulun yliopistolle tekemää väitöskirjaa samankaltaisesta aiheesta sekä muita alan julkaisuja ja haastatteluja tilaajayrityksessä. Selvitysvaihe piti sisällään ennakkoaineistoon tutustumisen niin tietoturvan, tilaajayrityksen kuin jalkauttamisenkin näkökulmista. Tämän vaiheen jälkeen aloitettiin suunnitteluvaihe, jossa käytiin tarkasti läpi, miten sekä opinnäytetyö että tutkimus, selvitys ja kehitystyö suoritettaisiin loogisesti ja tarkasti. Lopulliseksi toteutustavaksi muodostui kehittämistyö eli olemassa olevan jalkauttamismallin nykytilan selvittäminen ja edelleen kehittäminen sekä parantaminen.

Seuraavaksi toteutettiin haastattelut, joihin osallistuivat turvallisuushenkilöstö, neljä myyntikoordinaattoria ja heidän esimiehensä. Näillä henkilöillä koettiin olevan kriittisimmät osat jalkauttamisen vaiheissa. Turvallisuushenkilöiden vastuulla oli tietoturvapolitiikan ja implementoinnin kehittäminen ja ylläpito. Ryhmän esimiehellä oli vastuu jalkauttamisesta ja sen seurannasta. Lopuksi tiedon jalkauttamisen alimmalla tasolla olivat tutkittavan ryhmän työntekijät. Näin saatiin koko organisaation läpileikkaus. Haastatteluiden tuloksia verrattiin sekä keskenään että alan kirjallisuuteen. Suurimmat huomiokohdat olivat ehdottomasti kaikkien haastateltavien näkemys siitä, että koulutuksia tulisi lisätä ja päätöksentekoon haluttiin lisää mielipiteitä myös alemmilta organisaatiotasoilta. (Lähdeteoksista löydettiin kohtia jotka tukivat haastatteluiden näkemyksiä, joten nämä tulokset esitettiin tietoturvaryhmälle).

Esitettyjen väitteiden ja tulosten pohjalta päädyttiin hyväksikäyttämään jatkossa suunniteltavan uuden tietoturvapolitiikan suunnitteluvaiheessa seuraavia kohtia: Suunnitteluvaiheeseen osallistuu johtoryhmän ja tietoturvaryhmän lisäksi sekä tiimien esimiehiä että heidän alaisiaan tuomaan erilaisia näkökulmia käytännön työskentelystä. Jalkauttamisen vaiheet eritellään tarkemmin omaksi dokumentikseen osastoittain ja niiden toteutusta ja seurantaa valvovat ylemmällä tasolla tietoturvaryhmä ja alemmalla tasolla ryhmien esimiehet. Koulutuksia järjestetään lisää hyväksikäyttäen ulkoisia tietoturvakoulutuksiin erikoistuneita konsultteja tai niihin erikoistuneita yrityksiä. Koulutussuunnitelma laaditaan samalle ajalle kuin koko tietoturvapolitiikkakin. Lisäksi myöhemmässä vaiheessa aiotaan tutkia tarkemmin mahdollisuutta ja keinoja palkitsemis- ja tavoitetapojen kehittämiseen.

Asiasanat: jalkauttaminen, implementointi, tietoturva, tietoturvapolitiikka

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Business information technology

Hämäläinen, Lauri

Developing the implementation of information security policies

Year 2010 Pages 26

This thesis studies an unnamed company's information security policy implementation methods, and how to develop them to work more efficiently. The company wishes to be anonymous for security reasons. The idea of this thesis is to gather information from different levels of the organization by interviewing the workforce, as well as from literature concerning both information security and implementation in general and then create a set of guidelines on how to better the current implementation.

The first step was to research the areas of information security and implementation. The main source of background information for this thesis was a dissertation by Mr. Petri Puhakainen at Oulu University. The second step was to determine how this paper should be constructed for it to be logical and well presented. There are no other documents, the thesis also acts as a working document, and it was created at the same time as the research and reporting phase.

After the pre-studies and planning were completed, the next phase was to start the interviews. The company's contacts toward the researcher in this thesis were the security team, a group of employees and their superior. The main objective of the developing of current implementation methods was that at the end of the research some new methods would be presented. All of the interviews were conducted in the same way, as an open interview. This method allows conversation and produces a lot of details compared to other possibilities. The interviewees were the head of the security team, a team of four individuals who are a part of the business sales unit and their superior. This setup allowed a good view of the whole organization.

The most important findings during the interviews were as follows: every level of the organization thought that adding and planning a precise education in security policies and involving lower levels of organization in the process of planning the implementation would be beneficial. Another finding in the research was that the management should be more involved in the implementing phase and set a leading example to other workers. The same ideas were also found in the pre-study phase from many sources. After the results were written down, they were presented to the security team.

The results were presented and compared to the security teams' previous, self made plans. The discussions about the findings in this thesis with the security team were successful. The presented solutions on improving the current way of implementing the security policies and educating the workforce were seen as beneficial. In the future, a consultant will be hired to handle the educating part of the new implementation plan. Every single step of the implementation of the information security policies will be written in detail in a separate document. The team that is responsible for the information security planning will also include new members from the lower levels of the organization in the future as presented in this thesis, to give fresh ideas and a view from a different angle. Supervising and helping to implement the information security policies as agreed will also be more carefully carried out by the superiors of all teams in the organization.

Keywords implementation, information security, information security policies

Sisällys

1 ESITTELY

1.1 Opinnäytetyön kuvaus

Tutkimuksellisena kehittämistyönä toteutettava opinnäytetyö käsittelee yrityksen nykyisiä sisäisiä tietoturvakäytäntöjä, niiden täytäntöön panoa (eli kansanomaisemmin jalkauttamista) ja ennen kaikkea jalkauttamisen kehittämistä. Tavoitteena on tutkia nykyisen jalkautusmallin toimivuutta ja erityisesti etsiä menetelmiä, joilla nykyistä jalkauttamista saataisiin paremmaksi. Tämä tarkoittaa sitä, että mikäli nykyisten menetelmien lisäksi löydetään erilaisia ja teoriatasolla käytännölliseksi havaittavia tapoja, ehdotetaan niitä tämän raportin lopputuloksena yritykselle. Lopuksi päätellään, oliko löydetyistä menetelmistä mitään käytännön etua yrityksessä. Kehittämistyö kirjataan opinnäytetyöraporttiin eikä erillistä aineistoa tilaajayritykselle ei luoda.

Ideana on toteuttaa haastatteluiden, kirjallisuuden ja aiempien tutkimusten pohjalta selvitys erään suomalaisen yritykseltä aiheesta; kuinka hyvin työntekijät omaksuvat annetut toimintaohjeet ja tietoturvakäytännöt. Onko osaamista mitattu ja millä tasolla osaamisen haluttaisiin olevan? Lisäksi selvitetään tämänhetkisten menetelmien toimivuus asiakkaan (tietoturvatiimi) näkökulmasta ja verrataan saatuja tuloksia muiden tietoturvan jalkauttamiseen perehtyneiden näkemyksiin – lähinnä lähdekirjallisuuden avulla. Yrityksen sisältä määritettävän testiryhmän, sen esimiehen ja asiakkaan eli tietoturvatiimin haastatteluiden jälkeen tutkitaan alan kirjallisuutta ja tutkimuksia. Sekä tietoturva että implementointi ovat käsitteitä, joista löytyy paljon tutkimuksia ja lähteitä työn tueksi. Esimerkiksi Petri Puhakaisen Oulun yliopistolle vuonna 2006 tekemä väitöskirja sisältää paljon erilaisia näkökulmia tietoturvapolitiikasta. Yritysjohdon strategian jalkauttamisesta löytyy lukuisia kirjoja, ja tietoturvakoulutuksistakin on tehty varsin kattavasti erilaisia tutkimuksia. Lisäksi teoreettisella puolella tukena käytetään ISO (International Organization for Standardization) standardin sarjaa 27000.

Haastatteluiden perusteella kartoitetaan ne alueet, joita tietoturvallisuudessa tämän yrityksen osalta pidetään tärkeimpänä. Sen jälkeen etsitään erilaisia keinoja, joilla nämä aiheet saataisiin parhaiten jalkautettua osaksi työntekijöiden ja mahdollisesti koko yrityksen arkirutiineja. Testiryhmänä käytetään yhtä organisaation osaa, jonka koko on viisi henkilöä. Lisäksi heidän esimiestään, ja yrityksen tietoturvajohtoa kaikkia haastatellaan avoimen haastattelun keinoin.

Tutkimuksellisen kehittämistyön ja opinnäytetyön yhdistäminen tähän yhteen tuotokseen perustellaan sillä, että kaikki muu materiaali jota kehittämistyötä tehdessä on luotu, on siirretty tilaajayritykselle aiheen arkaluontoisuuden, anonymiteetin vuoksi.

Tutkimuksen lopputulokset ja raportit arvioitetaan yrityksen tietoturvatiimillä ja ryhmän esimiehellä, ja tämä arvio sisällytetään opinnäytetyöhön: Saatiinko tutkimuksen kautta löydetyillä menetelmillä haluttua muutosta asenteissa ja voidaanko tämänkaltaisia menetelmiä käyttää jatkossa mielekkäästi ja hyödyllisesti?

1.2 Toimeksiantaja

Opinnäytetyön arkaluontoisen aiheen vuoksi toimeksiantajayritys jää nimettömäksi. Yrityksen sisältä useilta eri tasoilta saatiin selkeä viesti siitä että anonymiteetti haluttiin ehdottomasti, mikäli työ julkaistaan julkisena dokumenttina.

Toimeksiantajana opinnäytetyössä toimii suomalainen, Helsingissä toimiva yritys, joka tarjoaa palveluita ainoastaan yrityksille. Yrityksen asiakkaat ovat lähinnä yli 100 henkilöä työllistäviä pääkaupunkiseudulla sijaitsevia yrityksiä, joilla on useampia toimipisteitä joko Suomessa tai Pohjoismaissa. Jälleen on korostettava, että koska kyseinen yritys haluaa ehdottomasti pitää kiinni anonymiteetistä, ei työssä voida paljastaa tarkempia asioita tilaajayrityksen taustoista.

1.3 Kehittämistyö

Opinnäytetyö tehdään tilaajayritykselle tutkimuksellisena kehittämistyönä. Koska nykyistä toimintatapaa on tarkoitus tutkia ja kehittää aiempaa tehokkaammaksi, sopii kehittämistyö parhaiten tämän opinnäytetyön menetelmäksi. Näiden asioiden tarkemmat taustat selvitettiin Hirsjärven, Remeksen ja Sajavaaran teoksesta Tutki ja Kirjoita (2009). Kehittämistyön keinoina käytetään kvalitatiivisin menetelmin haastatteluja tilaajayrityksessä, Petri Puhakaisen väitöskirjaa sekä alaan liittyvää kirjallisuutta. Kvalitatiivisia eli laadullisen tutkimuksen menetelmiä voidaan hyödyntää parhaiten juuri silloin, kun tutkittava ryhmä on varsin pieni (viisi henkilöä) ja kvalitatiivisella menetelmällä voidaan hyödyntää syvempää tasoa muun muassa haastatteluissa. Lisäksi pohditaan erilaisia näkökulmia, objektiivisesti, jotta työn painoarvo akateemisella toimintatavalla olisi mahdollisimman suuri.

1.4 Toteutusympäristö

Työ toteutetaan lähinnä yrityksen tiloissa (haastattelut, keskustelut sekä kyselyt). Työ toteutetaan yksilötyönä, ja asiakkaana on asiakasyrityksen tietoturvatiimi. Lopputulos kuitenkin arvioitetaan yrityksen tietoturvatiimillä ja haastateltavan yksikön esimiehellä. Mikäli uusia jalkauttamismenetelmiä tai niiden tehostamiskeinoja löydetään, saatetaan niitä jatkossa käyttää tilaajayrityksessä.

1.5 Tietoturva

Tässä luvussa perehdytään sekä tietoturvaan käsitteenä että opinnäytetyön tilaajayrityksen tietoturvapolitiikkaan yleisellä tasolla. Tietoturvallisuuteen liittyvät asiat käsitellään seuraavaksi kevyesti syventymättä liikaa aiheeseen. Lähtökohtaisesti tämä teos on tarkoitettu lukijoille, joilla on jo kehittyneempää tietoa tietoturva-alasta yleisesti. Käsittelyssä on silti muutama tärkeä perusasia jotta mahdollisesti alaan vähemmän tutustuneet ymmärtävät jatkossa esitettyjen asioiden taustoja.

1.5.1 Yleisesti

Tietoturva ja tietoturvallisuus ovat käsitteitä, joita käytetään usein, mutta tietoturvan perusajatukset ovat harvemmin esillä. Se, mitä tietoturva oikeastaan on, voidaan tiivistää kolmeen pääkohtaan:

Tietoturvan peruskäsitteet Järvisen (2006) mukaan;

- **Luottamuksellisuus** – lukuoikeudet, kenelle tieto kuuluu, onko lähde/tekijä luotettava
- **Eheys** – oikeaa ja luotettava tietoa – aina ajantasaista
- **Saatavuus** – järjestelmät ja palvelut saatavilla niille jotka sitä oikeasti tarvitsevat

Tietoturvan tekninen puoli pitää sisällään ohjelmia ja järjestelmiä. Palomuurit, virustorjuntaohjelmat, haittaohjelmatorjujat, sähköpostisuodattimet ja internetsuodattimet ovat kaikki osa teknistä tietoturvaa. Toisaalta kuitenkin näiden ohjelmien toimivuus riippuu täysin siitä kuinka hyvin ja oikeaoppisesti niitä käytetään.

Esimerkiksi yleisesti Suomessa arvostettu tietokirjailija Petteri Järvinen on itse kertonut ajankohtaisohjelma ”Verkossa” haastattelussa (2009) käyttävänsä ainoastaan palomuuriohjelmaa omassa tietokoneessaan. Tämä siksi, että hän uskoo oikeaoppisen

tietokonekäyttökulttuurin johtavan siihen, että mitään virus- tai haittaohjelmaongelmia ei synny, mikäli osaa ennakoida tekemisensä internetissä tai sähköpostien parissa.

Tietoturvallisuudesta puhuttaessa asiaan vihkiytyneiden ihmisten kanssa törmää helposti käsitteeseen ”80/20”. Tällä tarkoitetaan inhimillisyyden ja tekniikan välistä suhdetta ongelmatapauksissa. Inhimilliset erehdykset aiheuttavat noin 80% kaikista tietoturvavirheistä, ja tekniset ongelmat edustavat vain 20%. Juuri tästä syystä koetaan, että yrityksissä tietoturvan jalkauttaminen ja tietoisuuden nostaminen on ollut toistaiseksi suurin kompastuskivi.

Yrityksien tietoturvapolitiikkaan liittyy myös useita tärkeitä standardeja joiden avulla minkä tahansa kokoiset yritykset voivat luoda, ylläpitää ja kehittää tehokasta tietoturvallisuustoimintaa.

Tärkein tietoturvapolitiikan edesauttaja oli Britannian hallituksen vuonne 1995 luoma BS 7799 ohjeistus, jossa määriteltiin tietoturvapolitiikan peruspiirteitä. Tämän julkaisun sisällön tärkeimpänä kohtana voidaan pitää ”Best Practices”, eli niin kutsuttuja ”parhaat toimintamallit” tapojen esilletuontia. Kyseisessä teoksessa käsitellään tietoturvan johtamista kymmeneltä eri kannalta. Myöhemmin samainen standardi otettiin käyttöön myös laajamittaisessa ISO - standardijärjestelmässä. ISO/IEC järjestelmän 27000 sarja keskittyy juurikin tietoturvapolitiikkaan ja sen eri osa-alueisiin. Esimerkiksi ISO/IEC 27003 keskittyy ohjeistamaan ja helpottamaan ns. ISMS (Information Security Management System) eli Tietoturvajärjestelmän jalkauttamista. Ja toisaalta esimerkiksi ISO/IEC 27011 on erityisesti teleoperaattoreille suunnattu standardi (www.2700.org, 28.11.2010)

1.5.2 Tietoturvajohtamisesta

Tietoturvan johtaminen on vastaavanlaista kuin muussakin strategiatoiminnassa, eli tavoitteiden asettamista, vastuiden määrittämistä sekä resursoimista. Johtamisessa kolmena kivijalkana voidaan pitää seuraavia kohtia:

- Hierarkia
- Tavoitteiden asettaminen ja seuranta
- Valvonnan jatkuvuus

Näiden kolmen kivijalan noudattamisella varmistetaan johdon kyky olla osana, varsinkin tietoturvapolitiikkaa ajatellen, sekä päätöksenteko- että jalkauttamisvaihetta. Mikäli johto sitoutuu tehtyihin päätöksiin ja toimii itse esimerkkinä päätöstensä mukaan, saadaan koko organisaatio hyväksymään tehdyt päätökset. Myös tietoturvapolitiikassa on yrityksillä

ongelmia muutosvastarinnassa, jonka vähentäminen vaatii johdolta selkeitä päätöksiä, sekä johdonmukaisuutta.

Valtionvarainministeriön VAHTI ohjeistuksessa käsitellään myös tietoturvallisuusjohtamista. Tärkeimpinä kohtina mainitaan että tietoturvallisuuden johtaminen tarkoittaa erityisesti riskienhallinnan toteuttamista. Toiminnallisten prosessien tulisi sisältää menetelmiä joiden avulla riskien hallinta helpottuu ja ennen kaikkea vähentyy. Hyvin johdetussa tietoturvallisessa organisaatiossa määritellään selkeästi tehtävät, vastuut ja raportointikäytännöt. (VAHTI - 2007_VAHTI 3_Yleisohje tietoturvajohtamiseen.pdf):

Tietoturvajohtamisen haasteina tilaajayrityksessä olivat heikot määritykset vastuurajapinnoista sekä seurannasta tai sen puutteesta. Tietoturvapolitiikan ja sen jalkauttamisen olemassaolo teoriatasolla tiedetään, mutta sen käytännön toteutuksesta ei ole selkeitä merkkejä. Tämän voidaankin olettaa johtuvan edellä mainituista kohdista, kuten johdon sitoutumisen puutteesta.

1.5.3 Toimeksiantajan tietoturvapolitiikka

Nykyisellään toimeksiantajayrityksen tietoturvaohjeita ja dokumentteja löytyy lähinnä yrityksen omasta intranetistä. Muun muassa Valtiovarainministeriön (VM) VAHTI:n (Valtionhallinnon tietoturvallisuuden johtoryhmä) ja ISO 27000 dokumentteja on käytetty hyväksi ohjeissa. Tämän lisäksi tietoturvatiimi keskittyy myös julkaisemaan uutisia ja erityiskäytäntöjä mahdollisista tietoturvauhista, jotka vaativat erityistä huomiota käyttäjiltä sekä intranetissä että sähköpostitse.

Toimeksiantajan tietoturvapolitiikan käytännön toteuttaminen ja kouluttaminen tapahtuu niin sanotusti hierarkkisesti, eli ylimmältä tasolta johdosta kohti organisaation alinta tasoa. Tämä tarkoittaa, että yrityksen ylin johto tekee yhdessä tietoturvatiimin kanssa strategiset päätökset, ja tätä tietoturvan perusrakennetta viedään alaspäin organisaatiossa kohti työntekijöitä. Viimeisessä vaiheessa tiimien vetäjät (ryhmien esimiehet) ovat vastuussa siitä, että kaikki heidän alaisensa ovat perillä uusista tietoturvamalleista ja toimivat ohjeiden mukaisesti.

Tällä hetkellä voimassa oleva tietoturvan koulutus- ja tiedonjakomalli ei kosketa organisaation alimpia tasoja, ja koska yrityksen ydintoimintoja tehdään pääsääntöisesti juuri näillä tasoilla, olisi tietoturvatietämyksen kasvattaminen erittäin tärkeä asia. Suurimpana ongelmana voidaan pitää tietoturvapolitiikan etäisyyttä suhteessa perustyöntekijän arkirutiineihin. Tässä työssä onkin selvitettävä osaltaan esimiesten roolia tietoturvapolitiikan jalkauttamisessa, sillä juuri esimiehet ovat tärkein linkki johtoryhmän ja alaisten välissä.

Suurimman vastuun todellisesta tietoturvan jalkauttamisesta voidaankin olettaa konkreettisesti kuuluvan esimiehille, kun tietoturvatiimi yhdessä johdon kanssa luo strategian ja käytännöt.

Kuten useissa yrityksen johdolle suunnatuissa strategian implementointia käsittelevissä teoksissa (Puhakainen 2006, ISO 27003) mainitaan, tulisi johdon harkita vakavasti ottaa strategisessa päätöksenteossa huomioon alaisten ja perustyöntekijöiden käytännönläheinen näkökulma, joka usein ylemmiltä tasoilta puuttuu. Usein strategiset päätökset koetaan alimmalla tasolla joko liian korkealentoisina tai vaihtoehtoisesti liian epämääräisinä. Toisaalta ylimmän johdon voi olla hankalaa hahmottaa alimpien organisaatiotasojen käytäntöjä. Tietoturvapolitiikassa ja yritysstrategiassa on hyvin samankaltaiset sudenkuopat, ja siksi varsinkin johtoryhmätason olisi syytä miettiä tapoja osallistuttaa työntekijät alimmalta organisaatiotasolta mukaan tietoturvapolitiikan parantamiseen nimenomaan käytännön osaamisen ja näkökulmien suhteen.

2 MENETELMÄT

Seuraavissa kohdissa etsitään ratkaisumenetelmiä aiemmin ilmenneille ongelmille ja kysymyksille.

2.1 Asiantuntijoiden näkökulmat

Toimeksiantajana toimivan yrityksen tietoturvapäällikkö haastateltiin avoimen haastattelun keinoin yrityksen tiloissa. Kysymyksien lähteinä käytettiin tästä työstä löytyviä ongelmia ja ennakkopäätelmiä. Haastattelua vietiin eteenpäin käyttämällä ennakkoon määriteltyjä avainsanoja, joista pyydettiin haastateltavan näkökulma. Tämä näkökulma kirjattiin ylös haastattelutilanteessa, ja kirjoitettiin jälkikäteen puhtaaksi. Lopullinen kirjattu haastattelu hyväksytettiin vielä jälkikäteen haastateltavalla, jotta haastattelijan tulkinta vastauksesta ei poikkeaisi alkuperäisestä tarkoituksesta. Tämän haastattelun tuloksia verrataan kirjalliseen aineistoon muun muassa yrityksen strategian jalkauttamisesta. Lopuksi eri asiantuntijamielipiteet vedetään yhteen ja näistä tuloksista sovelletaan uusia tapoja kehittää nykyistä menetelmää toimeksiantajayrityksessä myöhemmissä kappaleissa.

2.2 Tietoturvapäällikön näkemykset

Toimeksiantajayrityksen tietoturvallisuudesta vastaavan henkilön haastattelu suoritettiin yrityksen tiloissa siten, että ennen haastattelua vaihdettiin sähköposteja koskien muutamia kohtia joista olisi tarkoitus haastattelutilanteessa keskustella. Tämä siksi ettei kummallekaan haastattelun osapuolelle tulisi yllätyksiä koskien haastattelun aihetta tai sisältöä. Haastattelu

käytiin keskustelevassa ilmapiirissä, ja haastattelija teki kysymyksen johon haastateltava vastasi, jonka jälkeen asiaa käsiteltiin vielä keskustellen mielipiteitä ja näkemyksiä vaihdellen.

Aluksi haastattelussa kysyttiin tietoturvapäällikön näkemyksiä tilaajayrityksen tietoturvallisuustason nykytilasta. Näkemyksenä oli selkeästi se, että nykyisen organisaation aikana tietoturvallisuuteen käytetty panostus on kasvanut merkittävästi aiemmista vuosista. Sekä järjestelmät että henkilöstö ovat molemmat jatkuvan kehitys- ja seurantatyön alla. Yleisen tietoturvallisuustason tietoturvapäällikkö koki varsin hyväksi.

Kysyttäessä nykyisistä toimintamalleista haastateltava ilmensi ne tavat joilla organisaation tietoturvapolitiikka oli perustettu, ja miten sitä oli suunniteltu kehitettävän. Ideana on johtoryhmävetoinen politiikka. Tämä tarkoittaa sitä, että tietoturvajohtoryhmällä on vastuu tehdä viisivuotisesti tietoturvasuunnitelma koko organisaatiolle. Suunnitelma sisältää sekä koulutuksen, ylläpidon, seurannan ja jalkautuksen osia. Erikseen määritelty tietoturvatiimi seuraa tarkasti määritettyjen sisäisten mittareiden avulla sekä tietoturvateknisiä että henkilötasolla tapahtuvia tietoturvauhkia ja skenaarioita. Johtoryhmä vastaa siitä että tietoturvapolitiikan mukainen toiminta jalkautetaan oikein, eli hierarkkisesti johtoryhmästä katsoen alaspäin, aina tiimijohtajille saakka. Viime kädessä tietoturvapolitiikan jalkauttamisesta ovat vastuussa siis esimies- tai tiimijohtajatehtävissä olevat työntekijät.

Seuraavana kohtana haastattelussa nostettiin esille ongelmakohdat. Tietoturvapäällikön mielestä suurimpina ongelmakohtina koettiin kaksi asiaa: resurssit sekä motivointi. Resurssien pienuus aiheuttaa tietoturvatiimille ongelmia varsinkin koulutusten järjestämisessä, sekä kaikessa kehittämistyössä. Tilaajayrityksen tietoturvatiimin koko on kaksi jäsentä ja päällikkö. Tällä kokoonpanolla suurin osa ajasta käytetäänkin mittareiden valvomiseen ja muuhun ylläpitoon. Uuden kehittämiselle ei löydy tarpeeksi aikaa eikä aina edes resursseja. Toisena ongelmakohtana koettiin henkilöstön motivointi tietoturvallisuusasioissa. Motivointi on kirjattuna yhtenä kohtana tietoturvapolitiikassa, mutta resurssipulan takia motivointikeinojen kehittäminen on jäänyt muun toiminnan taka-alalle. Kuitenkin jonkinasteista parannusta tähän on luvassa, sillä tietoturvapäällikkö kertoi tehneensä jo aloitteen lisäresursseista ulkoisen tietoturvakouluttajakonsultin hankinnasta sisäiseen projektiin, jossa tarkoituksena on kehittää koulutusta ja motivointikeinoja turvallisuushenkilöstölle.

2.3 Aiheeseen liittyvä kirjallisuus

Tärkeimpänä lähdeteoksena on käytetty Oulun Yliopistolle vuonna 2006 tehtyä väitöskirjaa, jonka on tehnyt Petri Puhakainen. Väitöskirjan nimi on ”A DESIGN THEORY FOR INFORMATION

SECURITY AWARENESS", ja sen keskeisimpänä teemana on selvittää tapoja joilla yritykset voivat parantaa henkilöstönsä tietoturvallisuusasioiden tietoisuutta.

Suurin tietoturvauhka yritykselle on sen oma henkilöstö, joten sen asenteen muokkaaminen on varsin tärkeässä asemassa. Kaikkien työntekijöiden tulisi olla tietoisia, noudattaa, ja tarkkailla käytäntöjä joilla tietoturvallisuutta pidetään yllä. Tärkein yleisen asenteen vaikuttamiseen liittyvä tekijä on mielipidevaikuttajien käytännön osallistuminen esimerkkinä muille. Lisäksi mainintaan, että käyttäjien osallistuminen politiikan luontivaiheessa lisää sen hyväksyntää jalkauttamisvaiheessa. ISO standardin 17799:2005 (toinen versio) mukaan työntekijöiden tulisi saada työhön liittyviä koulutuksia ja jatkuvia päivityksiä koskien tietoturvaa yrityksen tietoturvapolitiikan mukaisesti. Standardi määrittelee myös, että uusien työntekijöiden sisäänajo yrityksen tietoturvallisuuspolitiikan mukaisesti hoidetaan ennen kuin työntekijälle annetaan oikeudet päästä käsiksi arkaluontoiseen materiaaliin. Lisäksi standardissa luetellaan että käynnissä olevien koulutuksien tulisi sisältää muun muassa turvallisuusvaatimuksien määrittelyjä ja tietoa siitä kuinka menetellä työntekijän kohdalla joka on tehnyt tietoturvarikkeen. (Puhakainen 2006, s19)

Vuonna 2002 Martins ja Eloff esittivät mallin jolla tietoturvallisuuskulttuuria voidaan jalkauttaa ja kehittää. Heidän mallissaan oli kolme eri organisaatiotasoa: organisaatiotaso, ryhmätaso ja yksilötaso. Tämän mallin kantava idea oli että kaikessa organisaation tietoturvassa tulee ottaa huomioon ihmisen käyttäytyminen. He ehdottivatkin että jokainen työntekijä koulutetaan ja ohjataan kohti yrityksen tietoturvapolitiikkaa yksilöllisten, omaan työhön liittyvien vaatimuksien kautta. (Puhakainen 2006, s21)

Murrayn julkaisu vuonna 1991 korostaa, että huonoon tietoturvallisuuteen liittyy usein tietämättömyys varsinkin niiden työntekijöiden osalta, jotka eivät ole tutustuneet kunnolla tietoturvallisuuteen. Hänen mielestään tärkeimpiä parantamiskeinoja olisivat organisaation sisäiset tietoisuuden lisäysohjelmat, joilla kaikkien työntekijöiden kiinnostuneisuus tietoturvallisuusasioissa saataisiin herätettyä. Tämänkaltaiseen toimintaan voisi kuulua kurssit, seminaarit, videot, oheismateriaali, ohjeet, muistutukset sekä uutiskirjeet. (Puhakainen 2006, s21)

Seuraavaksi on lueteltuna lista tärkeimmistä kohdista Parkerin tutkimuksessa 1998 – 1999 koskien tietoturvallisuuden jalkauttamisen toimivasta rakenteesta työympäristössä (Puhakainen 2006, s22):

1 – Johdon tuki
2 – HR osaston tuki
3 – Työnkuvaukset, joissa määritelty tarkasti tehtävät
4 – Arvioinnit ja keskustelut
5 - Dokumentointi
6 – Johtajien motivointi

Esimerkkinä toimiminen sekä koulutuksissa että käytöksellä työelämässä toimii paremmin, kuin pelkkä yksipuolinen koulutus alaisille. Johtopäätöksenä voidaan pitää, että mikäli johto tukee tietoturvallisuutta se myös näyttää sen. Mikäli johto tukee tietoturvaa vain ylemmällä tasolla, itse kuitenkaan noudattamatta tekemiään ohjeita, saattaa koko muu organisaatiokin jättää noudattamatta ohjeita. (Puhakainen 2006, s29)

Puhakaisen väitöskirjassa nostetaan myös esille neljä tärkeintä kohtaa koulutuksessa: Harjoitukset, kampanjat, palkitseminen ja rangaistus. Palkitseminen ja rankaisu voidaan yhdistää yhdeksi kokonaisuudeksi, joten jäljelle jäisi kolme kokonaisuutta. Harjoitukset (1), kampanjat (2) sekä palkitseminen ja rankaisu (3). (Puhakainen 2006, s69 – 70).

Tietoturvallisuus- ja konsultointipalveluita tarjoavan Ymon Oy:n toimitusjohtaja Pasi Yliluoma kirjoitti Talouselämän verkkojulkaisussa kesäkuussa 2010 mielenkiintoisen artikkelin koskien yrityksen johdon tietoturvaa, jossa hän listasi 10 kohtaa joita johdon tulisi huomioida tietoturvallisuuden suhteen. Nämä kohdat ovat erittäin osuvia verrattuna muiden asiaa koskevien mielipiteiden kanssa:

1. Näytä esimerkkiä 2. Tee selkeä vastuutus 3. Suojaa aineeton omaisuus 4. Anna riittävät resurssit 5. Tarkkaile poikkeamia 6. Tee ohjeista todellisuutta 7. Analysoi sisäiset uhkat 8. Analysoi ulkoiset uhkat 9. Hyödynnä uusia mahdollisuuksia 10. Muista aina ihminen
Yliluoma, Pasi 2010, luettu 25.6.2010. Tietoturva on osa johtamista. [WWW-dokumentti]. (http://www.talouselama.fi/minavaitan/article431279.ece?s=r&wtm=talouselama/-21062010)

ISO standardisarjan 27000 mukaisesti tietoturvapolitiikan ja ennen kaikkea sen jalkauttamisen (ISO27003) suhteen on viimeisen viidentoista vuoden aikana tehty laajamittaisesti kehittämistä. Viiden vuoden välien päivitettävät ISO - standardit toimivat erinomaisina ohjenuorina kaikenkokoisille yrityksille. ISO 27003 dokumentissa tuodaan esille paljon

huomiota saanut PDCA toimintamalli. ”Plan-Do-Check-Act” eli PDCA malli on varsin hyvin yleistynyt jalkauttamiseenkin soveltuva tapa, jossa ideana on yksinkertaisen neljän kohdan avulla luoda, ylläpitää ja kehittää toimivia toimintatapoja. PDCA malli on siten ongelmanratkaisu- ja kehittämismenetelmä. Ensin suunnitellaan, jonka jälkeen toteutetaan suunnitelma. Sitten tarkistetaan tuotos, ja lopuksi suoritetaan tarkistuksen mukaiset muutokset. Tämän menetelmän käyttäminen esimerkiksi tilaajayrityksessä voisi olla järkevää varsinkin silloin kun uusien menetelmien jalkauttamista suunnitellaan.

2.4 Yhteneväisyydet ja huomiot

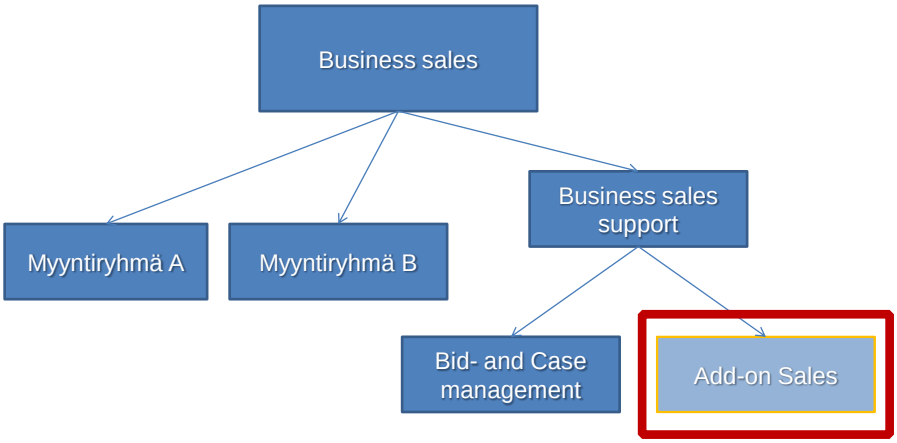
Sekä alan kirjallisuuden että tilaajayrityksen tietoturvapäällikön näkemykset tuovat mielikuvan siitä, että jalkauttamisen peruspilareina toimii henkilöstön osallistuttaminen suunnitteluvaiheeseen ja aktiivinen motivointi toteutusvaiheessa. Ulkopuolisen tahon käyttäminen jalkauttamisen tehostamisessa oli erinomainen huomio tietoturvapäälliköltä, mikäli kaivattuja resurssien lisäyksiä vain on tiedossa. Johdon vastuu on selkeästi pidetty tärkeänä kohtana kirjallisissa julkaisuissa ja ennen kaikkea johdon esimerkkinä toimiminen myös käytännön tietoturvallisuusasioissa koettiin selkeästi positiiviseksi asiaksi.

Nämä kohdat otetaan huomioon tutkimuksen myöhemmissä vaiheissa ja niitä jalostetaan edelleen yrityksen tarpeisiin sopiviksi.

2.5 Kehittämistyön seurantaryhmä

Jotta olisi mahdollista kehittää jonkin olemassa olevan menetelmän toimintaa, on tässä työssä oltava seurattava ryhmä. Työssä vertaillaan yhtä toimeksiantajayrityksen organisaation osaa (ryhmää), johon kuuluu neljä työntekijää ja heidän esimiehensä. Seurattava ryhmä sijoittuu organisaatiokaaviossa Business Sales yksikköön. Business Sales yksikkö koostuu kolmesta pääryhmästä; myyntiryhmät A ja B, sekä business sales support. Tukitoimintoja sisältävä business sales support ryhmä on jaettu kahtia; bid- ja case management ryhmään sekä nimenomaiseen add-on sales ryhmään, joka on tutkittavan ryhmän virallinen nimi organisaatiossa (selventävä kuva tämän dokumentin lopussa). Add-on Sales ryhmällä on myös muita toiminnallisiin tehtäviin liittyviä nimiä kuten lisätilaukset, pohjoismaiset myyntitapahtumat, yritysmyynti sekä asiakaskohtaisia tilaustenhallintanimiä.

Haastatteluiden kautta on tarkoitus selvittää ryhmän jäsenten mielipide tietoturvapolitiikkaan ja käytäntöihin, sekä näkökulmia siihen miten ryhmä haluaisi itse asioita mahdollisesti muuttaa tai parantaa. Lisäksi tähän ryhmään testataan uusia menetelmiä, mikäli sellaisia löydetään.



Kuva 1: Organisaatiokaavio: tutkittava ryhmä

Seurantaryhmä koostuu neljästä henkilöstä, joiden kaikkien työtehtävänimike on myyntikoordinaattori. He vastaavat toimeksiantajayrityksen olemassa olevien asiakkuuksien muutoshallinnasta, pitäen sisällään esimerkiksi toimipisteiden muutot, palveluiden lisätilaukset, toimipisteiden lisäykset, käyttäjien lisäykset ja niin edelleen kaikkien asiakkaille tarjottavien tuotteiden osalta. Pääasiallisesti seurantaryhmän vastuulla on luoda sopimuksia asiakkaiden tarvitsemien muutosten mukaisesti, eli luoda näistä toiminteista raportoitavaa liiketoimintaa. Seurantaryhmän jäsenillä ei ole vastuuta uusien asiakkaiden hankkimisessa, joten he eivät ole myyjiä, vaikkakin ryhmä voidaan organisaatiossa helposti rinnastaa myyjiin toimenkuvien ja mittareiden osittaisten vastaavuuksien takia.

Seurantaryhmän tiedot: Kaikki työntekijät ryhmässä ovat miehiä, heidän ikähaarukkansa on välillä 26 – 35 vuotta. He kaikki ovat olleet töissä samalla työnantajalla vähintään kaksi vuotta. Tässä kokoonpanossa ryhmä on työskennellyt nyt vuoden ja kaksi kuukautta (maaliskuussa 2010). Ryhmän jokapäiväisten työsuoritteiden välineinä ovat puhelin, sähköposti ja MS Office 2007 tuotteet Excel, Word sekä sisäiset järjestelmät liittyen tilausten käsittelyyn.

Seurantaryhmän toiminta edellyttää erityisesti sähköpostien ja liitteiden lähettämistä sisäisesti ja ulkoisesti, ja yhtenä varsin tärkeänä osana on sopimusten solmiminen asiakkaiden kanssa. Tietoturvallisuusasioissa ryhmän yhteneväisenä mielipiteenä nostettiin tärkeimmiksi kohdiksi kaksi asiaa; työvälineiden tietoturvallinen käyttö esimerkiksi tietoturvaohjelmistojen luotettavuuden osalta (työpisteen tietokone ja keskitetysti hoidettu tietoturvaohjelmistojen

päivitys ja ylläpito), ja sopimuksien osalta tietoturvallinen toiminta on äärimmäisen tärkeää (esimerkiksi luku- ja katseluoikeusasiat). Sopimukset tulisivat olla poikkeuksetta aina oikein täytettyjä sekä tuotteiden, osapuolten että henkilöiden ja allekirjoitusten osalta, ja ennen kaikkea dokumenttien tulisi olla aina tilanteen mukaan oikeassa muodossa (esimerkiksi; kaikkien muokattavissa oleva DOC, vai vain luettava PDF).

Seurantaryhmän esimies on jo 10 vuotta talossa työskennellyt yli 40-vuotias mieshenkilö. Hänellä on vahvaa osaamista tietoturvallisuusasioissa, kuten myös myynnin tuen ja ratkaisusuunnittelunkin alueilla. Tutkimuksessa tutkittavan testiryhmän esimiehen tehtävissä hän on toiminut marraskuusta 2009 lähtien. Hänen alaisuudessaan toimii kaksi eri ”tiimiä”, eli ryhmää, jotka esiteltiin aiemmassa kappaleessa nimellä ”business sales support”. Esimiehen tehtäviin kuuluu testiryhmän suhteen HR (Human Resources) vastuu, sekä työvälineiden toimivuuden ja muiden tukitoimintojen varmistaminen. Esimiehen tehtäviin tietoturvallisuuspuolella kuuluu perehdyttää ja kouluttaa uudet talossa aloittavat alaisensa yrityksen tietoturvapolitiikan mukaisesti, sekä valvoa että tietoturvallisuuspolitiikan mukainen osaamistaso säilyy korkeana. Käytännössä kuitenkin tämänhetkinen tietoturvakoulutus on lähes olematonta ja lähinnä tietoturvatiimin pitämien koulutusten varassa.

2.6 Haastattelut

Kaikki haastattelut suoritettiin tilaajayrityksen tiloissa. Haastattelussa välineinä käytettiin etukäteen mietittyjä kohtia, joita käytäisiin läpi keskustelevassa ilmapiirissä – käytetty menetelmä oli avoin haastattelu. Haastattelun kulkua johti etukäteen kirjatut avainsanat, jotka haastattelija kysyi tietyssä järjestyksessä. Puhevuorojen aikana haastattelija kirjasi ylös tärkeimmät asiat koskien haastattelun teemaa, eli haastateltavien omaa näkemystä. Haastattelija kirjasi tärkeimmät kohdat muistiinpanoihin, ja haastattelun jälkeen kokosi mielipiteet yhteen. Kaikki haastattelut hyväksytettiin vielä kirjallisena jälkikäteen haastateltavilla, jotta mielipiteet eivät värittyisi tai vääristyisi poikkeaviksi alkuperäisistä toteamuksista.

2.6.1 Seurantaryhmä

Haastattelutilanne pidettiin yrityksen tiloissa. Haastatteluun osallistuivat kaikki ryhmän jäsenet samanaikaisesti, ja haastattelu kirjattiin ylös paperille keskustelutyylisen haastattelun aikana. Myöhemmin haastattelu kirjattiin puhtaaksi ja hyväksytettiin erikseen kaikilla haastateltavilla.

Ensin keskusteltiin testiryhmän näkemyksistä tietoturvasta. He kokivat tietoturvan käsitteenä lähinnä teknisinä sovelluksina, kuten palomuuri ja virustorjuntaohjelmistoina. He kehuivat näiden ohjelmistojen olevan erittäin hyvällä tasolla, ja niiden toimivan poikkeuksetta vähintäänkin riittävästi. Mitään muuta tietoturvaan liittyvää näkemystä ei tullut. Kaiken kaikkiaan testiryhmän mukaan toimeksiantajayrityksen tietoturvan tekninen puoli on hyvin kunnossa.

Tämän jälkeen kysyttiin rutiineista jota ryhmä tietää liittyvän tietoturvaan, ja he käyttävät päivittäin. Ensimmäisenä kohtana löydettiin salasanat, sekä niiden ylläpito ja hallinta. Salasana on pakotettu vaihdettavaksi joka 60. päivä. Tämä koettiin ongelmalliseksi asiaksi, koska salasanan jatkuva vaihtaminen on hankalaa muistamisen ja käytettävyyden takia. Tietoturvan kannalta asia ymmärrettiin tärkeäksi, mutta silti kritisoitiin sen hankaloittavaa vaikutusta. Toisena akuuttina kohtana pidettiin asiakkaille lähetettävien sopimusten ja hinnastojen luottamuksellisuusaspektin säilymistä – ryhmä koki, että ulos annettavien tietojen luottamuksellisuuden valvonta oli hankalaa. Ryhmä oli kuitenkin selkeästi tiedostanut tämän ongelman, ja he käyttävätkin usein arkaluontoisen tiedon kuten hinnastojen, sopimusten tai sähköpostiketjujen lähettämisessä varovaisuutta ja lisäävät sähköposteihin muistutuksia ja toimintaohjeita koskien luottamuksellisuutta.

Seuraavaksi kohdaksi haastattelussa nostettiin tietoturvapolitiikka. Ryhmän kaikille jäsenille ei ollut selvää mitä tietoturvapolitiikalla edes tarkoitetaan. Yksi neljästä haastateltavasta kuitenkin tunsi asiaa hieman tarkemmin ja kertoi tuntevansa ainakin periaatetasolla työnantajansa tietoturvapolitiikan piirteet. VM VAHTI ja siihen liittyvä toimintatapa oli tämän testiryhmän jäsenen tietoturvatietämys, ja hän uskoi että VAHTI ohjeistus oli myös osittain käytössä tilaajayrityksessä. Lyhyehkön tietoturvapolitiikka-idean muille ryhmän jäsenille avaamisen jälkeen testiryhmän näkemys oli, että tietoturvapolitiikka olisi erittäin hyödyllistä jalkauttaa kaikille organisaatiotasoille. Mikäli johtoryhmä yhdessä tietoturvatiimin kanssa luovat toimivan konseptin, on sääli jos tätä työtä ei jalkauteta ajatuksella ja innolla sille tasolle joka ohjeistusta eniten tarvitsee. Jalkauttamisessa järkevimpänä tahona ryhmä piti esimiehiä ja tietoturvatiimiä.

Tietoturvakoulutuksesta testiryhmä oli yksimielinen; sitä ei ole riittävästi. Ryhmän mielestä olisi vähintäänkin suotavaa että uusille työntekijöille perehdytettäisiin oman toimenkuvan mukaiset tietoturvallisuusohjeet. Pelkkä salassapitosopimus ja yleiset ohjeet koettiin etäisinä ja hankalina muistaa. Kuten jo tietoturvapolitiikkakeskustelussa hetkeä aiemmin, myös koulutuksesta puhuttaessa ryhmässä korostettiin toivetta ryhmien esimiesten aseman nostamista vastuulliseksi alaisten tietoturvaosaamisen kehittämisessä ja ylläpidossa. Koulutuksen toivottiin olevan sekä ryhmä- että yksilötasolla räätälöityä. Lisäksi toivottiin,

että koulutuksissa näytettäisiin tarkkoja keinoja ja tapoja toimia mahdollisimman tietoturvallisesti.

Kysyttäessä tämänhetkistä koulutustarvetta, ryhmä yllättäen ilmoitti tarpeen olevan erittäin pieni. Vaikka parannuskohtia löydettiin, ei ryhmällä ollutkaan yllättäen tarvetta nostaa omaa osaamistasoaan – ainakaan tuntuvasti. Jatkuvat ja toistuvat osaamista ylläpitävät koulutukset sekä järjestelmällinen toiminta kuitenkin todettiin tarpeelliseksi myös ryhmän sisällä.

2.6.2 Esimies

Testiryhmän esimies haastateltiin vasta kun ryhmähaastattelu oli valmis. Tällä tavoin pystyttiin tekemään tarkentavia kysymyksiä, mikäli jokin kohta nousisi selkeästi poikkeavaksi verrattuna testiryhmään. Tietoturvapolitiikan tietämys on esimiehellä esimerkillisen hyvällä tasolla, johtuen useista eri asiakastapaamisista ja asiakkaiden vaatimuksista tarjouksissa ja sopimuksissa joita hän on ollut tekemässä aiemmissa työtehtävissään. Testiryhmän esimiehellä on vahva ja pitkä kokemus alalta, ja hän on ollut mukana useissa suurissa hankkeissa joissa hän on päässyt tutustumaan useisiin eri näkökulmiin varsinkin tietoturvallisuusasioissa.

Haastattelun alussa kysyttiin esimiehen mielipidettä tilaajayrityksen sisäisen tietoturvan tilasta. Hänen näkemyksensä mukaan perusasiat ovat erittäin hyvin kunnossa; järjestelmät, tietoturvapolitiikka, oikeudet ja hallinta ovat kaikki selkeästi ja hyvin toteutettuja kokonaisuuksia. Esimiehen yksiselitteinen näkemys oli, että tietyistä tilaajayrityksen asiakkaista johtuen yrityksen sisäiseen tietoturvaan liittyvät komponentin ovat kaikki auditoituja ja standardien (mm. ISO ja ITIL) mukaisesti toimiviksi todettuja.

Tietoturvapolitiikasta esimies tunnisti varsin tärkeän seikan: Tietoturvapolitiikka määrittelee menetelmät (joita työssä käytetään). Jalkauttamisen osalta hän tunnisti joitain puutteita, sillä varsinkin testiryhmän kanssa käydyn keskustelun tulosten läpikäymisen jälkeen esimies selkeästi huomasi että korkealla tasolla tehdyt strategiset tietoturvapoliittiset päätökset eivät olleet jalkautuneet hänen alaisilleen saakka – ainakaan toivotulla tasolla.

Lisäksi esimies halusi tuoda esille, että suurin osa kaikkein tärkeimmistä tietoturvallisuutta korostavista hankkeista ja asiakkuuksista eivät tule koskaan kaikkien työntekijöiden tietoon. Tällä tavoin vähennetään mahdollisuutta tietovuodoista ja muista vastaavista riskeistä – varsinkin jos asiakas näin vaatii.

Tärkeimpinä teeseinä tietoturvallisessa työnteossa hän piti luottamuksellisuutta, oikein tehtyjä ja ylläpidettyjä salasanoja sekä koneiden lukitsemisia käyttäjien itsensä toimesta.

Esimerkiksi yksinkertainen lounaalla tai kahvilla käyminen ja työpisteen vahtimatta jättäminen voi johtaa tietoturvaongelmiin. Jos tietokone ja arkaluontoisia dokumentteja jää auki, saattaisivat ulkopuoliset tahot käyttää tilaisuutta hyväkseen. Vaikka työtiloissa ei saa kulkea luvattomia ihmisiä, on silti aina syytä muistaa että tietoja voi varastaa kuka tahansa – vaikkapa siivooja! Liiallista varovaisuutta ei tämänkaltaisissa toimissa voi haastatellun esimiehen mukaan olla.

Esimiehen näkemys kouluttamisesta poikkesi huomattavasti alaisten näkemyksestä. Esimies oli vahvasti sitä mieltä, että esimiesten vastuulla olisi tietoturvakoulutusten sijaan varmistaa alaisten mahdollisuus koulutuksiin ja oikeisiin työvälineisiin sekä menetelmiin. Itse koulutuksen hän näkisi toimivan parhaiten keskitetysti vaikkapa tietoturvatiimin tai ulkoisesti ostettavan palvelun kautta. Näin kaikille saataisiin samankaltainen viesti ja edellytys tehdä töitä mahdollisimman yhteneväisellä tavalla.

Lopuksi kysyttiin testiryhmän esimiehen näkemystä omasta tietoturvatietämyksestä. Hän piti omaa osaamistaan korkeana ja riittävänä nykyiseen työnkuvaansa – johtuen pitkälti aikaisemmista asiakastapahtumista joissa hänen on täytynyt opiskella sekä sisäisiä että ulkoisia tietoturva-aiheisia asioita kattavasti.

3 TULOKSET

Sekä tutkittavan ryhmän jäsenet että ryhmän esimies huomasivat osittain samankaltaisia puutteita. Tietoturvallisuus oli perustasoltaan varsin riittävä, mutta laajempi ja syvällisempi tietämys tietoturvallisuuspolitiikasta tuntui puuttuvan. Lisäksi koulutusta haluttaisiin ehdottomasti lisätä; alkukoulutusta uusille työntekijöille ja täydennys- sekä ylläpitävää koulutusta nykyisille työntekijöille. Järjestelmällinen ja hyvin suunniteltu koulutus tuntui parhaalta vaihtoehdolta kaikille osapuolille. Tutkittavan ryhmän jäsenet peräänkuuluttivat yksilöllistä lähestymistapaa koulutuksissa, kun taas esimiehen näkemyksenä oli pikemminkin keskitetty ja samankaltainen koulutus kaikille.

Haastateltavien näkemykset tiheämmin suoritettavista ja jatkuvista koulutuksista tukevat myös tutkittua kirjallisuutta, joissa painotettiin koulutuksen jatkuvuutta. Johdon tuki tulisi näkyä selkeämmin sekä kehittämisvaiheessa että koulutus ja ylläpitovaiheessa. Testiryhmän sisällä koettiin tarvetta uudistuneelle toiminnalle. Esimiehen näkökulmana oli pikemminkin se, että nykyinen malli oli toimiva mutta keskitettyä koulutusta tulisi lisätä ja tehostaa. Molemmat näkökulmat ovat myös tuettuina alan kirjallisuudessa, ja näiden kaikkien yhdistelmä voisi olla ehdottamisen arvoinen.

Tietoturvapäällikön näkemyksenä oli, että henkilöstön osaamisen ja jalkautusmallin nykyinen taso on varsin hyvä mutta haasteellisimmiksi kohdiksi nykytilanteessa koettiin tietoturvahallinnon puolella resurssien puute. Mahdollisten tulevien lisäresurssien myötä kehityskohteiksi mainittiin ainakin koulutuksien määrän ja laadun parantaminen sekä sisäisten mittareiden ja seurannan kehittämistyö.

Kaikkien yllämainittujen näkökulmien yhdistävänä tekijänä voidaan pitää koulutuksien esille nostaminen. Koulutuksien määrän kasvattamisella olisi varmasti näkyvä ja tuntuva vaikutus tietoturvallisuusasioissa läpi koko organisaation. Jalkauttamisen kannalta mittareiden kehittäminen ja niiden tuominen lähemmäksi henkilöstöä olisi myös selkeä parannus aiempaan toimintatapaan. Yhtenä varsin konkreettisena keinona toteuttaa koulutusten tuntuva lisääminen nykyiseen toimintaan, olisi lisätä tietoturvapäällikön mielipidettä mukaillen budjettia tietoturvahallinnon koulutus- ja kehittämishankkeissa.

Tämän luvun tärkeimmät huomiokohdat ovat;

1) Koulutuksia tietoturvallisuudesta ja asiakasyrityksen tietoturvapolitiikasta on lisättävä kaikilla tasoilla
2) Johdon tuki ja läpinäkyvyys tietoturvallisuusasioiden päätöksissä oltava selkeämpää
3) Tietoturvahankkeisiin tulisi ohjata lisäresursseja
4) Mittareiden luonti, jatkuvuus ja seuranta koskien tietoturvallisuusasioita on nostettava johtoryhmän tärkeysjärjestyksessä korkeammalle

3.1 Uudet menetelmät

Kuten Puhakaisen (2006) väitöskirjassa todettiin, kolmen päämotivointialueen yhdistäminen sosiaalis-teknisellä lähestymistavalla voisi toimia parhaiten. Mikäli sekä koulutukset, kampanjat että palkitseminen ja rankaisu otettaisiin käyttöön yhtenäisesti ja suunnitelmallisesti, voitaisiin tässä yrityksessä nähdä selkeästi uudenlainen tapa tehostaa tietoturvapolitiikan jalkauttamista ja käytänteitä.

Keskitettyjä ja yhteisiä yleisen tason koulutuksia kaikille, sekä yksilöllisempiä ja työkuvakohtaisempia koulutuksia voitaisiin alkaa suunnitella ja toteuttaa vuositasolla. Seuranta ja jatkuvuus tulisi luoda ainakin viisivuotisella suunnitelmalla siten, että esimiehet olisivat mukana sekä suunnittelu- että toteutusvaiheessa, kuten tähän asti on toimittu.

Pienemmissä koulutuksissa otettaisiin huomioon sekä ryhmän tarpeet että yksilölliset toiveet työhön liittyvien kysymysten osalta. Suuremmissa koulutuksissa käytäisiin pääasiallisesti läpi uudet kaikkia työntekijöitä koskevat toimintatavat ja välineiden esittelyt sekä laajat huomiokampanjat.

Koulutuksissa käytettäisiin ehdotetun mukaisesti ulkoista tietoturvakonsulttia sekä aikataulun että parhaan mahdollisen laadun varmistamiseksi.

Lisäksi tietoturvaryhmä voisi keskittyä enemmän mittareiden tarkentamiseen ja kehittämiseen. Tähän projektiin voidaan liittää selvitys siitä, kuinka voitaisiin seurata onnistuneita tietoturvatoimia joko yksilöittäin tai ryhmittäin. Tavoitteiden asettamisen kanssa parhaiten onnistuneiden ryhmien tai yksilöiden palkitsemiset voisivat olla eräs toimiva keino lisätä motivointia työyhteisössä niin ryhmien esimiesten kuin alaistenkin osalta.

Kehitysehdotukset jalkauttamisen parantamiseksi:

1) Koulutukset
2) Lisäresursseja tietoturvaan - Konsultti
3) Jatkuva kehitystyö ja kaikkien organisaatiotasojen osallistuttaminen
4) Mittarit, tavoitteet ja seuranta

4 LOPPUYHTEENVETO

4.1 Yleisesti

Lopputulokset tutkimuksen osalta esiteltiin haastatellulle ryhmälle, heidän esimiehelleen sekä tietoturvatiimille. Ryhmän mielipiteet lopputuloksista olivat positiiviset, varsinkin kohdat yksilöllisten koulutustarpeiden ja motivointikeinojen selvittämisen osilta saivat paljon kiitosta. Ryhmän esimies koki että kaikkia ehdotettuja menetelmiä tuskin voitaisiin hyödyntää, mutta silti hän piti myös motivointikeinoja varsin kiinnostavana kohteena jatkokehityksen kannalta.

Tietoturvatiimi käsitteli tämän opinnäytetyön tulokset kokonaisuudessaan erillisessä palaverissa johon osallistui heidän lisäkseen opinnäytetyön tekijä sekä yksi johtoryhmän edustaja. Palaverissa käsiteltiin kaikki opinnäytetyössä esitetyt mahdolliset jalkauttamisen tehostusmenetelmät. Käsittelyn aikana käytiin läpi miten ehdotukseen oli tultu, ja kuinka se voitaisiin mahdollisesti toteuttaa. Suurimmaksi ongelmaksi nousi opinnäytetyöstä kokonaan puuttunut kulurakenne uusien menetelmien taustalta. Toisaalta opinnäytetyössä ei ollutkaan tarkoitusta luoda valmista taloudellista esitystä ja ratkaisua, vaan etsiä ne kohdat joissa tehostaminen toisi parannusta vanhaan malliin verrattuna. Palaverin lopputuloksena oli, että tietoturvatiimi tutkii onko soveltuvaa konsulttipalvelua mahdollista tilata toistaiseksi määrittelemättömässä budjetissa. Johtoryhmän tehtäväksi jäi selvittää budjetin tarkastaminen, ja kuinka esimiesten jalkauttamista voitaisiin parantaa ylimmän johdon toimintojen osalta.

Tietoturvatiimi antoi loppupalautteena tämän opinnäytetyön osalta seuraavia asioita: He kiittivät opinnäytetyön tekijää rennosta otteesta ja mukavasta työskentelytavasta. Koko prosessin kesto oli pitkä (alkuselvityksineen yli puolitoista vuotta) jona aikana yhteistyö oli jatkuvasti toimivaa ja helppoa. Itse opinnäytetyöstä oli tietoturvatiimille paljon apua, ja tärkeimpänä kohtana pidettiin konkreettisten tehostuskeinojen löytymistä ja sitä että nämä asiat saatiin siirrettyä suunnitteluasteelta kohti toteutumista.

Tutkittavan ryhmän esimiehen palaute oli opinnäytetyöstä kovin vastaavaa kuin tietoturvatiimillä. Opinnäytetyön lopputuloksen hän koki positiivisena, vaikkakin jotkin osat lopputuloksista eivät olleet samassa linjassa hänen omien näkemyksiensä kanssa. Haastattelutilanteet sujuivat hänen mukaansa erittäin hyvin ja yhteistyö sujui kaikkien mukana olleiden osapuolten välillä mallikkaasti.

4.2 Tekijän loppukommentit

Tämän opinnäytetyön ja sen raportin tekeminen on ajoittunut hyvin pitkälle aikavälille. Osittain myös tästä johtuen opinnäytetyön raportoinnin sisältö on muuttunut useasti ja suuntaviivoja on siirrelty saatujen palautteiden perusteella lähes viikoittain. Varsinaisen opinnäytetyön tekeminen tilaajayrityksessä oli haastavaa, ja tämä kohta opinnäytetyöprosessia olikin kaikkein mielenkiintoisin. Haastattelut, niiden tuloksien analysointi ja kirjallisuuden sovelluttaminen työhön olivat kaikessa uutuudessaan erittäin mukavia haasteita. Yrityksen mielenkiinto tekemääni työhön oli alun perin melko etäistä, mutta useiden eri keskustelutuokioiden jälkeen työ sai enemmän huomiota ympäri organisaatiota. Tämän opinnäytetyön lopputulokset on esitetty johtoryhmälle ja on erittäin todennäköistä että työn perusteella tehtyjen johtopäätöksien avulla jalkauttamista tullaan suunnittelemaan ja toteuttamaan jatkossa eri tavalla kuin tähän asti. Siitä olen ylpeä ja tyytyväinen. Henkilökohtaisesti koko prosessi venyi alkuperäisestä aikataulustaan melkein vuoden, lähinnä henkilökohtaisen elämäntilanteen takia. Onneksi pystyin kuitenkin jatkuvasti pitämään mielessäni opinnäytetyön aiheen. Mikäli en tuottanut raporttia tai keskustellut yrityksessä, niin kuitenkin asia oli jatkuvasti mietinnässä ja harkinnassa. Voisinkin kuvitella että pitkät pohdinnat aiheen tiimoilta ovat osaltaan edesauttaneet sitä että tilaajayritys otti mielipiteeni vakavasti harkintaan eikä vain sivuuttanut opiskelijan kommentteja olankohautuksilla.

Lähteet

Hirsjärvi, S., Remes, P., Sajavaara, P. 2009. Tutki ja Kirjoita. Helsinki: Tammi

Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo

Puhakainen, P. 2006. A design theory for information security awareness. Viitattu 25.4.2010. http://herkules.oulu.fi/isbn9514281144/

Puhakainen, P: 2006. Tietoturvakäyttäytymisen parantaminen. Viitattu 25.4.2010. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20061215Valtio/04_Puhakainen_15.12.2006.pdf

The ISO 2700 Directory. Viitattu 28.11.2010. www.27000.org

Valtionvarainministeriö 2007. Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 15.4.2010. http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp

Yliluoma, P. 2010. Tietoturva on osa johtamista. Viitattu 21.6.2010. http://www.talouselama.fi/minavaitan/article431279.ece?s=r&wtm=talouselama/-21062010

Kuvat ja kuviot