LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoturvallisuusopas vaihtokaupan yritykselle

Vesa Valasuo

2017 Laurea

Laurea-ammattikorkeakoulu

Tietoturvallisuusopas vaihtokaupan yritykselle

Vesa Valasuo
Turvallisuusala
Opinnäytetyö
Joulukuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusala
Turvallisuusala (AMK)

Vesa Valasuo

Tietoturvallisuusopas vaihtokaupan yritykselle

2017 Sivumäärä 38

Opinnäytetyön tavoitteena oli tuottaa tietoturvaopas vaihtokauppaa tuottavalle yritykselle. Organisaatio oli juuri päivittänyt tietoturvasuunnitelman, joka tulisi jalkauttaa heidän henkilöstölleen. Opinnäytetyön tarkoituksena oli tehdä tietoturvaopas, joka sisällöltänsä kattaisi tärkeimmät osa-alueet sekä että opas oli itsestään helppolukuinen eikä käytetty liikaa tietoturvan ammattisanastoa.

Tietoperustana käytin tietoturvallisuuden organisaatioita, jotka ovat tuottaneet valtiolliselle tasolle tietoturvaohjeistuksia. Alan kirjallisuutteen tutustuin ja hain tietoa netistä, jotta saisin mahdollisimman hyvä kuvan tietoturvallisuusalasta ja sen tarjonnasta. Haastattelin alalla toimivia henkilöitä ja sitä kautta sain paljon tietoa oppaaseen. Näin sain hyvin laadullista tulosta työlleni.

Kyselytulosten perusteella kävi ilmi, että näillä lähteillä kirjoitettu tietoturvallisuusopas ja siihen lisättynä ammattilaisten tuomia neuvoilla, on varsin onnistunut paketti henkilöstölle. Heidän mukaansa opas oli kattava mutta ei liian hankala luettavaksi henkilöille, joilla ei ole tietoturvallisuusalan aikaisempaa kokemusta. Tuloksista selvisi myös, että oppaassa tulisi olla selkeämpi yhteenveto, jota voisi käyttää myös tarkistuslistana ja muistin virkistyksenä tietoturvallisuuteen.

Asiasanat: Opas, Tietoturvallisuus, Tietoturvaopas, Turvallisuus

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

Vesa Valasuo

Drawing up an Information Security Handbook for a Trading Company

2017 Pages 38

The objective of this thesis was to produce an Information Security Handbook for a trading company. The company had just upgraded their information security plan, which should be introduced to the staff. The challenge with the handbook was to create a guide that would cover the most important aspects of information security and that the guide would be understandable, easy to read and that it would not include incomprehensible information security jargon.

An information security organization that has produced information security guidelines for the state level was benchmarked for the theoretical section of the thesis. Literature on information security was studied to gain a comprehension of the information security industry and supplies within the field. Information from people working in the security field was surveyed for the purpose of establishing the information security handbook. The outcome of the study is qualitative.

The results showed that the guide resulted in a very successful package for the staff. According to the staff the handbook was comprehensive, especially for people with no previous experience in the information security field. The survey results showed that the handbook should have a clearer table of contents, which could also be utilized as a checklist for and a refresher on information security.

Keywords: Guide, Information Security, Information Security Handbook, Security

Sisällys

1 Johdanto

Tietoturvallisuus on tullut yhä tärkeämmäksi yrityksille ja lähes kaikki yrityksen asiakirjat ovat sähköisessä muodossa. Huonosti hoidettu tietoturvallisuus saattaa altistaa yrityksen tietovarkaudelle. (Rousku 2015.) Tietoturva koskettaa yhä useampaa työntekijää. Tieto tulee käsitellä oikein. Esimerkiksi väärän tiedon säilyttäminen tietokoneessa voi johtaa rikossyytteeseen (Henkilötietolaki 11§/1999). Kun taas huolimattomalla tiedon käyttämisellä tai koneessa piilevän vakoiluohjelman takia voi luottamuksellinen tieto levitä (Microsoft 2015b). Esimerkkinä yrityksen antaman tarjouksen joutuminen kilpailevalle yritykselle saattaa aiheuttaa taloudellisia tappioita. Tietoturvallisuus on nykypäivää ja sen tarpeellisuus kasvaa koko ajan. (Hänninen 2014.)

Useissa kolmansissa maissa tietoturvallisuus on ollut vähemmän tärkeässä asemassa, muihin turvallisuuden osa-alueisiin verrattuna. Afrikassa autoon jätetty tietokone saattaa saada ohikulkijan rikkomaan ikkunan ja varastamaan tietokoneen. Hän on tyytyväinen, jos saa koneen toimimaan ja poistaa todennäköisesti kaikki tiedostot, jotta hänen omat tiedot, kuvat ja elokuvat mahtuvat tietokoneeseen. Euroopassa tilanne voi olla aivan toinen, tietokoneen varastanut henkilö pyrkii pääsemään käsiksi tietokoneessa oleviin tietoihin ja lukemaan jos mahdollista. Hän saattaa pyrkiä käyttämään näitä tietoja hyväkseen esimerkiksi myymällä tietoa kilpailevalle yritykselle tai kiristämällä yksityiskuvilla lisää rahaa eli hänelle pelkkä tietokone ei ole se saalis vaan myös tieto sen sisällä. (Ristola 2015.)

Tietoturvallisuudella haetaan optimaalista turvallisuustasoa. Tällöin tietoturvallisuus on balanssissa. Toiselle puolelle laitetaan tiedon arvo ja toiselle tietoturvallisuuteen käytettävät varat. Tiedon arvoa voi määritellä sillä, mitä tapahtuu, jos tieto joutuu vääriin käsiin. Mitkä ovat tämän tapahtuman aiheuttamat tappiot unohtamatta imagollista vaikutusta. Tietoturvallisuudesta on ylläpidettävä ja huolehdittava asianmukaisesti, näin voidaan varmistaa tietoturvallisuuden hyvä taso vaikka hakkerit, virukset ja muut ohjelmat kehittyvät. On kuitenkin pidettävä mielessä, että 100%:sta turvallisuutta ei voida

saavuttaa tietoturvallisuudessa kuin myöskään perinteisessä turvallisuudessakaan. (Maunuksela-Malinen 2003.)

Tietoturvaympäristö kehittyy ja muuttuu nopeasti. Tietoturvallisuuden kysyntä ja tarve lisääntyvät koko ajan. Tietoja yritetään kalastella monilla eri tavoilla. Tietoturvallisuus pyritään kehittämään vastaamaan tämän päivän tarpeita, joskus etupainotteisesti, mutta toisinaan opitaan vasta kun vahinko on jo tapahtunut. Tietoturvallisuus kehittyy kaikilla osa-alueilla ja sen tiedon päivittäminen vaatii jatkuvaa tutkimusta, jotta voidaan pyrkiä suojautumaan kaikilta tietoturvallisuusuhilta. Kaikista ponnisteluista huomiotta, uusia turva-aukkoja tulee esille tiuhaan tahtiin ja kaikkia niitä ei ehditä tukkia resurssipuutteiden takia. Tietoturvallisuutta pyritään parantamaan myös lain avulla, esimerkiksi tietoliikenteestä, henkilötiedoista ja tietoaineistojen käsittelyistä. (Vahti 1/2004.)

2 Opinnäytetyön tarkoitus ja tavoite

Tietoturvallisuusopas pohjautuu yrityksen tietoturvasuunnitelmaan. Tietoturvasuunnitelma sisältää kaiken sen mitä ja miten yrityksen tulisi varautua tietoturvallisuuden riskeihin. Tietoturvallisuusoppaaseen liitetään tietoa henkilöstön tietoturvallisuudesta. Se ei siis sisällä kaikkea yrityksen tietoturvallisuuteen liittyvää. Tämä opas ohjeistaa työntekijät toimimaan yrityksen tietoturvallisuussuunnitelman mukaisesti.

Tässä työssä tarkoituksena on ollut luoda ohjeistus henkilöstölle, jolla ei ole tietoturvallisuudesta aikaisempaa osaamista. Varsinkaan sellaisista, joka kattaisi kaikki olennaiset tiedot ja taidot, joita työntekijät tarvitsevat. Ohjeistuksen tulisi olla mielenkiintoinen, eikä viljellä liikaa vaikeaselkoisia sanoja joita he eivät ehkä ymmärrä. Tässä työssä pyritään kuvaamaan tietoturvallisuuden jalkauttamisen keinoja, ei käsittelemään asiaa teoreettisesti. Asiat pyritään esittämään niin kuin ne ovat, mahdollisimman yksinkertaisesti ja helpossa muodossa.

2.1 Keskeiset käsitteet

Eheys on tietoa, joka pysyy muuttamattomassa muodossa, eikä sitä päästä muuttamaan toiseksi. Esimerkiksi kun tieto saadaan palvelimelta, niin tiedetään ettei sitä ole muutettu. (ISO/IEC 27001:2006,10.)

Käytettävyys, eheys ja luottamuksellisuus ovat suojattavan tiedon peruskäsitteitä. **Käytettävyydellä** tarkoitetaan, että henkilöllä, jolla on valtuutus päästä käsiksi tietoon, on tämä tieto saatavilla ja sitä voidaan hyödyntää, muokata ja tarvittaessa myös tuhota. (ISO/IEC 27001:2006, 10.)

Luottamuksellisuus varmistaa, että tieto on vain sille oikeutettujen ihmisten käytössä eikä luvattomilla henkilöillä, tahoilla ja prosesseilla ole pääsyä. tietoihin. (ISO/IEC 27001:2006, 12.)

Sosiaalinen manipulointi. Tällä tarkoitetaan yleisesti sitä, että joku yrittää saada tietoja toiselta osapuolelta. Esimerkiksi pääsyä salattuihin tietoihin tai saada salattua tietoa käsiinsä. Manipulointi voi olla fyysisestä tai eri haittaohjelmien kautta tehtyä. Se voi olla huijausta tai johonkin muuhun rikolliseen toimintaa tarvittavaa tiedon väärinkäyttöä. Usein kysymyksessä on rikollinen toiminta. (Microsoft 2015a.)

Tietosuoja on henkilötietojen luottamuksellista käsittelyä. Tietosuoja on määriteltynä henkilötietolaissa. Tämä pitää sisällään henkilötietojen keräämisen, tallentamisen, käytön, luovuttamisen, siirron, säilyttämisen, hävittämisen ja muun käsittelyn. Henkilökohtaisia tietoja ovat nimi, osoite, ikä ja muut henkilökohtaiset tiedot. Näitä tietoja tulee aina käsitellä luottamuksellisesti. On olemassa tietoja, joita ei saa käsitellä lainkaan, kuten esimerkiksi etninen alkuperä, uskonto, yhteiskunta-ajattelu ja seksuaalinen suuntautuminen (Finlex 2015.)

Tietoturvallisuus on tiedon suojaamista ja se estää luvattoman pääsyn tietojärjestelmiin sekä tiedon luovuttamisen, muuttamisen tai tuhoamisen (United States Code 2006). Yritysturvallisuus koostuu kymmenestä eri osa-alueesta, joista yhtenä on tietoturvallisuus. Tietoturvallisuus koskettaa kaikkia yrityk-

sessä ja yhteisöissä työskenteleviä henkilöitä, koska lähes jokainen työntekijä on tekemisissä tiedon kanssa. (Elinkeinoelämän keskusliitto 2016.) Osana tietoturvallisuutta on tiedon suojaaminen, kun tieto on useassa eri muodossa asiakirjoissa, sähköisessä muodossa ja henkilöstöllä (Leppänen 2006, 260).

2.2 Kohdeorganisaation esittely

Kohdeyritys toimii öljyalalla, johon öljykriisit, sodat ja poliittiset tapahtumat ovat vaikuttaneet voimakkaasti. Öljyalalla liikkuu miljardeja dollareita vuodessa ja tämä tekee alasta kiinnostavan myös vilpillisille ja epärehellisille toimijoille. Öljyalan tärkeimpiä tekijöitä on oikeiden yritysten kanssa toiminen. Yritysten toimiessa keskenään tietoa liikkuu paljon esimerkiksi sähköpostien, tekstiviestien, puheluiden välityksellä. Jos tämä tieto päättyy vääriin käsiin, saattaa joku epärehellisistä toimijoista tulla kaupanteon väliin ja varastaa kaupan. Kyseessä saattaa olla useiden miljoonien kauppa ja tiedon suojaaminen on siksi tärkeää. Epärehellinen toimija saattaa käyttää hyvinkin paljon resursseja, ei pelkästään rahaa, saadakseen tietoa öljyalan yrityksestä.

Kohdeyritys ostaa öljyä ja myy sen eteenpäin tai vaihtoehtoisesti yritys toimii välittäjänä ostajan ja myyjän välillä. Heidän toimistonsa sijaitsee Dubain Marinassa Yhdistyneissä arabiemiirikunnissa. Toimisto sijaitsee yhdessä alueen torneissa, josta aukeaa upeat merimaisemat. Toimistossa on vastaanottotiski, jossa toimii vastaanottoapulainen tehtävänään kulunvalvonta. Vastaanottoaulassa ovat odotustila asiakkaille sekä neuvotteluhuoneet. Vastaanottoaula ja neuvotteluhuoneet sijaitsevat ns. Likaisella alueella (likainen alue= ei jatkuvan valvonnan piirissä). Puhtaalla alueella (puhdas alue= yrityksen kontrolloima alue) ovat päälliköiden ja johtajien omat huoneet sekä avotoimisto muille toimihenkilöille.

Yrityksen palveluksessa työskentelee 20 henkilöä, joista suurin osa toimii Dubain toimistossa. Yrityksellä on Dubaissa oma laskentatoimi sekä laki- ja henkilöstöhallintaosastot, myyntihenkilöstö ja johtajat. Johtajat tosin matkustavat paljon Lähi-idän ja Venäjän alueella, jotka ovat heidän markkina-aluettaan.

Öljy- ja mineraalialan yrityksen johto oli herännyt tietoturvallisuuden varmistamiseen teknisellä ja fyysisellä puolella. He halusivat päivittää olemassa olevaa tietoturvasuunnitelmaa sekä tuoda sen henkilöstön tietoisuuteen. Yritys pyrkii pitkällä tähtäimellä saamaan ISO/IEC 27001 tietoturvallisuusstandardin. He teettivät ensiksi tietoturvallisuussuunnitelman, joka jäi sitten heidän pöydälleen pölyttymään. Tällöin johto teki päätöksen tuoda tietoturvallisuuden mukaan heidän prosesseihinsa. Tämä alkoi tietoturvallisuusoppaan tekemisellä yrityksen henkilöstölle.

3 Tietoturvallisuuden tiennäyttäjät

Tietoturvallisuuteen liittyen on olemassa useita eri standardeja. Näitä standardeja mukailemalla on helpohkoa suorittaa tiedonkeräys ja analyysi. KATAKRI määrittelee neljä eri viranomaistasoa turvallisuudelle. KATAKRI:n päätavoite on yhdistää viranomaisten ja yritysten ja yhteisöjen turvallisuustasot toisille ja täten helpommaksi auditoida, mitata ja parantaa turvallisuustasoja. Toisena päätavoitteena on auttaa yrityksiä, yhteisöjä ja viranomaissidosryhmiä heidän omassa sisäisessä turvallisuustyössään. Tästä muodostuvat elinkeinoelämän suositukset. (KATAKRI 2011, 3.)

Viranomaisvaatimukset noudattavat neliportaista tiedon luokittelun suojaustasoja: Perustaso (IV), Korotettu taso (III), Korkea taso (II). Suojaustaso (I) on määritelty erittäin salaiseksi ja siihen ei oteta kantaa KATAKRIssa. Kyseisen tason tietoja ei luovuteta yritykselle tai se on äärimmäisen harvinaista ja siihen tarvitaan viranomaisen erillispäätös. Elinkeinoelämän suositukset ovat yllä mainitut. (KATAKRI 2011, 3.)

Vahti on valtioneuvoston alla toimiva valtiohallinnon tietoturvallisuuden johtoryhmä. Vahti ohjeistaa valtiovallan organisaatiota ja heidän johtoaan, jotta heillä olisi päivitettyä tietoa tieturvallisuudesta. Heidän tehtävä on taas siirtää tietoa muulle henkilöstölle, jotta heillä olisi riittävät tiedot toimia tietoturvallisuusohjeiden mukaisesti. Ohje on osana Suomen kyberturvallisuusstrategiaa. (VAHTI 4/2013, 4.) Vahti seuraa tietoturvallisuuden kehittymistä ja pyrkii omien resurssiensa puitteissa torjumaan jo havaitut tietoturvallisuusuhat sekä ennalta ehkäisemään tulevia uhkia (VAHTI 1/2004.)

Kansainvälinen standardi ISO/IEC 27001:2006 määrittelee tietoturvallisuuden hallintojärjestelmän. Tämä standardi on laadittu kehittämään, toteuttamaan, käyttämään, valvomaan sekä katselmoinnilla, ylläpitämään ja parantamaan tietoturvallisuuden hallintojärjestelmää. Tämän olisi tarkoitus auttaa organisaatioita toteuttamaan heidän tietoturvallisuusohjelmaansa. Jos ohjetta noudatetaan, niin se kattaa koko kirjon siitä, kuinka tietoturvallisuus tulisi implementoida osaksi organisaation johtamisjärjestelmää. Standardilla on tarkoitus helpottaa eri organisaatioiden kanssakäymistä keskenään, jolloin tietoa vaihdetaan keskenään. Samoin standardien tarkoitus on ylläpitää tietoturvallisuuden tason mitattavuutta ja verrattavuutta muihin organisaatioihin nähden. (ISO/IEC 27001:2006.)

BSI on saksalainen tietoturvallisuuden organisaatio, joka kehittää tietoturvallisuusasioita pääsääntöisesti Saksassa. BSI on standardi perhe Saksassa ja siihen kuuluu kaikkiaan 4 eri standardia, jotka määrittelevät tietoturvallisuuden hallinnointia valtion ja yksityisten organisaatioissa. Sitä päivitetään säännöllisesti ja se saatetaan jopa kokonaan uudistaa, jos tietoturvallisuudessa tulee isompia muutoksia. (BSI-Standard 100-1 2008.)

4 Tietoturvaoppaan tiedon suunnanantajat

Tässä luvussa on kerätty aineistoa josta on haettu pohja tietoturvallisuusoppaan rakentamiseen ja sen eri osa-alueisiin. Alussa käsitellään tiedon synty ja sen elinkaarta. Tietoturva on jaoteltu kahteen osa-alueeseen fyysiseen ja tekniseen tietoturvallisuus. Tämä jälkeen on huomioitu erillisesti etätyöskentely, joka on lisääntynyt 2000 luvulla.

4.1 Tiedon synty ja suojaaminen

Ihmiset tuottavat tietoa erilaisin keinoin, jota sitten yritykset ottavat käyttöönsä ja usein muokkaavat sitä omaa käyttöään varten. Tietoa varastoivat ihmisten lisäksi tietokoneet, puhelimet, serverit, kirjoitettu asiakirjat jne. Tietoa on yrityksen ihmisillä, jotka ovat töissä yrityksessä, tätä tietoa sitten jaetaan yrityksen sisäiseen tai/ja ulkoiseen käyttöön. Tätä varten tietoa tulee

hallinnoida oikein, jotta se olisi oikeiden ihmisten saatavilla kun sitä tarvitaan. (Leppänen 2006, 263-265.)

Kaiken keskipisteenä on ihminen, joka käsittelee tietoa joko oikein tai väärin. Tiedon vuotaminen muille ihmisille saattaa aiheuttaa vahinkoa yritykselle, josta tieto on lähtenyt. Näin ollen oikean tiedon käsittelystä tulisi tiedottaa ja kouluttaa ihmisiä. Tämä jättäisi pois mahdolliset virheisiin liittyvät tietovuodot. Samoin kun ihmiset on koulutettu käsittelemään tietoa, yritys voi vedota tahalliseen toimintaan, jos tietovuoto kumminkin sattuu. Tietoturvallisuus voidaan jakaa monella eri tavalla osiin ja tätä kautta saada kokonaisuus, jota on helpompi hallinnoida ja johtaa kuten Juha Leppänen käsittelee kirjassaan yritysturvallisuus käytännössä. (Leppänen 2006, 263-265.)

Leppänen käsittelee kirjassaan tiedon käytettävyyden, eheyden ja luottamuksellisuuden kautta alkuun. Tiedon käytettävyydellä tarkoitetaan, kun henkilöstö tekee töitä ja siitä syntyy asiakirjoja ja muuta vastaavaa tietoa yrityksen käyttöön, sitä tietoa voidaan muokata ja jakaa turvallisella tavalla niille henkilöille jolla on oikeus käsitellä tietoa. Organisaatiot määrittelevät oikean tavan käsitellä tietoa, joka löytyy yrityksen tietoturvallisuus suunnitelmasta tai tietoturva oppaasta, tämä tulisi kouluttaa henkilöstölle. Eheydellä varmistetaan, että saatu tieto on pysynyt alkuperäisessä muodossa, ettei kukaan ole päässyt vääristelemään sitä. ”Luottamuksellisuudessa kuuluu tietojen luokittelu, käyttäjien hallinta, suojaamistoimenpiteet ja yksityisyyden suojan varmistaminen” Leppänen kirjoittaa. (Leppänen 2006, 260.)

Tieto voidaan myös kuvata aikajanana, jolloin syntyy tiedon elinkaari. Tämän elinkaaren vaiheiden ympärille tulisi tehdä tietoturvallisuussuunnitelma, jolloin kaikki tieto on hyvin hallittavissa ja tiedetään, kuka on vastuussa tiedosta sen eri elinkaaren vaiheissa. Näitä ovat syntyminen, käsittely, siirtäminen, varastointi ja hävittäminen. Tietoa syntyy eri lähteistä, joita ihminen käyttää ja muokkaa yrityksen tarpeisiin. Lähteet voivat olla yrityksen ulkopuolelta saatua julkista tietoa tai yrityksen omaa tietoa, omista tietokannoista, tai henkilön omaan kokemukseen perustuvaa tietoa, esimerkiksi ammatillista tietotaitoa. Henkilön, joka kerää tämä tiedon ja muokkaan sen yrityksen käyt-

töön, tulisi merkitä minkä luokan tietoa se on (käyn luokittelun myöhemmin läpi), milloin se on tehty, kuka sen on tuottanut ja mistä lähteestä. Näin pystytään varmistamaan tiedon laatu. Jos asiassa on jotain eriäviä yrityksen sisäisiä mielipiteitä, voidaan niitä muokata. (Leppänen 2006, 265-266.)

Tiedonluokittelussa tietoa tulee käsitellä aina huolellisesti ja jos ei tiedetä onko asiakirja julkinen tai suojaustasolla suojattu, tulisi se tarkistaa. Ohjeet sanovat, että jos asiakirjassa ei ole suojausmerkintää, niin se ei ole automaattisesti julkinen. Julkiset asiakirjat tulisi aina säilyttää erillään suojatuista asiakirjoista, jotta sekaannuksia ei pääsisi syntymään. (VAHTI 2/2010.)

Suojaustasoja on kaikkiaan neljä; Erittäin salainen, salainen, luottamuksellinen ja käyttö rajoitettu; Erittäin salainen (ERSAL (E)), tämän tiedon paljastuminen voi aiheuttaa suurta vahinko kansainvälisille suhteille, valtion turvallisuudelle tai maanpuolustukselle. Sen jakaminen vaatii aina kirjallisen luvan tekijältä ennen kuin se saadaan luovuttaa eteenpäin. Salainen (SAL (S)), Sen saa luovuttaa vain tarveperusteisesti eteenpäin. Luottamuksellinen (LUOT (L)), Luottamuksellinen tieto saattaa aiheuttaa vahinkoa yritykselle, henkilöstölle tai kolmannelle osapuolelle. Näitä voisivat olla esimerkiksi taloudelliset tiedot. Käyttörajoitettu (RAJ (R)), Tämän tiedon vuoto ulos ei aiheuta vakavaa uhkaa tai taloudellista vahinkoa. Tällaisia voivat olla sisäiset tiedotteet ja ne ovat usein koko henkilöstön saatavilla. (VAHTI 2/2010.)

Kun tieto on luotu, se tulee luokitella. Luokittelu määrittelee sen, kuka tietoa saa käsitellä. Millaisessa muodossa tieto on, onko se tehty ruutupaperille vai sähköisesti Word dokumenttiin tahi johonkin ohjelman sisään. Ehkä tieto onkin rakennettu mallikappale, joka tulee suojata. Kaikissa tapauksissa tiedon käsittelyllä on oma prosessinsa – yhdistävä tekijä on, että sitä ei saa päästää ulkopuolisten käsiin. Tieto tulee käsitellä niin, että se pysyy eheänä toisten käsitellessä tietoa. (Leppänen 2006, 263.)

Kun joku muu käsittelee tietoa tai ottaa sen haltuunsa, siitä tulisi pitää kirjaa ja näin nähdään mihin tieto on joutunut ja kuinka sitä ollaan pidetty. Tämä vain silloin kun kyseessä on luottamuksellista tietoa tai salaisempaa. Jos tie-

tovuoto sattuu, on helpompi lähteä tutkimaan sitä, mistä tieto on vuotanut. Kun tietoa aletaan siirtämään, tulee pitää huoli siitä, että se saadaan siirrettyä turvallisesti ilman, että sivullisilla on pääsyä tietoon. Tieto voi olla fyysisessä muodossa esim. paperilla tai sähköisessä muodossa esim. sähköpostit ja tietoa varaavat laitteet. (Leppänen 2006, 276-277.)

Tiedon säilyttäminen riippuu asiakirjojen turvallisuusluokituksesta ja siitä, onko tieto sähköisessä tai fyysisessä muodossa. Kummatkin vaativat omat ohjeistuksensa. Tietoa voi joutua säilyttämään hetken ajan, kun joku projekti sitä esimerkiksi vaatii. Tällöin tulee huolehtia siitä, että tiedot palautetaan tai tuhotaan kun niitä ei enää tarvita. Samoin jos tietoa joudutaan vielä säilyttämään, tulisi säilytyksen tapahtua lukitussa tilassa, esimerkkisi luottamuksellinen tieto voisi olla lukitussa pöytälaatikossa. Ei koskaan työpöydällä, jota ikävän usein näkee tapahtuvan. (Leppänen 2006, 281-283.)

Tiedon säilyttämiseen vaikuttaa lainsäädäntö, joka määrittelee esimerkiksi kirjapitoaineiston säilyttämisajan tai lakitoimistojen arkistot. Lakitoimistoilla on paljon asiakirjoja, jotka vievät paljon on tilaa. tällöin materiaalit voidaan skannata sähköiseen muotoon, käyttäen ohjelmistoa, joka jättää materiaaliin vesileiman ja näin ollen säilyy virallisena asiakirjana vielä jatkossakin. Fyysinen asiakirja voidaan tuhota tämän jälkeen. Tosin on hyvä säilyttää sekä paperinen että sähköinen versio, jos vain mahdollista. Tiedoilla on käyttöikä, joka tulisi määritellä jo sen syntyvaiheessa. Joissain tapauksissa se voi olla vain muutamia kuukausia ja joskus vuosikymmeniä. (Leppänen 2006, 281-283.)

Tiedon säilyttämiseen tulee tehdä tarkka arkistointia käsittelevä tiedosto, jotta kun tietoa tarvitaan, voidaan se myös löytää helposti. Tiedostossa voidaan tarkentaa, kuka on sen tehnyt, tekoajankohta, mitä tietoa siinä on ja ehkä lyhyt seloste. (Leppänen 2006, 282-283.)

Tiedon hävittäminen on seuraavana kun tietoa ollaan säilytetty sen tarvittavan ajan. Papereiden, CD/DVD, kasettien ja muiden muistivälineiden tuhoaminen vaatii tarkkuutta. Papereiden repiminen pieneksi ja heittäminen roskiin ei vielä takaa sitä, että tieto on tuhottu. Paperin tuhomainen halvalla pape-

risilppurilla ei sekään vielä takaa etteikö paperia saada kasaan kun silppu löydetään roskalaatikosta. On olemassa ohjelmia, jossa jokainen paperin pala kuvataan ja ohjelma kasaa ne kokonaiseksi kuin palapelin. Paperisilppurin tulisi tuhota paperit ja CD/DVD levyt. Niissä on eri leikkureita, jotka takaavat sen, että paperi tuhoutuu tarpeeksi pieneksi. NATO on antanut omat hyväksyntänsä siitä, kuinka oikeanlainen tuhoaminen tulisi tehdä. Tällöin paperia ei leikata vaan kone repii ensimmäisellä terällä paperin pieniksi ja sitten toinen terä tuhoaa sen lähes pölyksi. Tietokoneiden muistilevyt tulisi aina päällekirjoittaa ennen kuin ne irrotetaan koneesta ja tuhotaan, erillään muusta elektroniikkajätteestä. (Leppänen 2006, 283-284.)

Tietoa voidaan siirtää monella tavalla. Hallittavia tapoja ovat fyysiset ja sähköiset muodot. On myös muistettava, että henkilöstöt hallitsevat osaa tiedosta, jota he kantavat mukanaan loppuelämänsä. Tätä tietoa voidaan kontrolloida taas sopimusteitse esim. Salassapitosopimus. (Leppänen 2006, 267.)

4.2 Fyysinen tietoturvallisuus

Tietoturvallisuuden standardi ISO/IEC 27001, määrittelee kulunvalvonnasta, että henkilöstön vapaata liikkumista tulisi välttää eri osastojen välillä. Sisäänkäynnin ja eri osastojen välillä tulisi olla turvasulkuja. Niitä ovat esimerkiksi seinät, miehitetyt pisteet ja korttien avulla valvotut kulunvalvontaportit. (ISO/IEC 27001:2006, 38.)

Kulunvalvonta on yksi ulkoisen uhan tärkeimmistä tietoturvasuojautumistoimista yritykselle. KATAKRI ohjeistaa korkeatasossa (II) yritystä käyttämään kaksoistunnistusjärjestelmää. Esimerkkinä biotunnistusjärjestelmä (Iris, sormenjälki, kasvojen tunnistus), jolla varmistetaan henkilöllisyys. Nämä eivät kuitenkaan aina ole 100% varmoja, joten siksi käytetään toista tunnistusjärjestelmää lisänä (esimerkiksi koodi, RFID, henkilökortti jne.). Näillä kahdella voidaan varmistaa henkilön oikeus edetä turvatulle alueelle. Poistuessaan alueelta, tulee myös käyttää tunnistetta. KATAKRI :n korkea taso (II) määrittelee myös, että eri projekti- / osastoalueet tulee suojata niin, että vain oikeutetuilla henkilöillä on pääsy ko. tilaan. (KATAKRI 2011.)

Puhdas ja likainen alue liittyvät kulunvalvontaan ja siihen, kuinka ihmisten liikkumista rajataan eri aluille. Tommi Nyström, joka toimii turvallisuusasiantuntija monille yrityksille, mukaan puhdas alue käsitteellä tarkoitetaan yleisesti tiloja, joihin pääsyn edellytyksenä on turvatarkastus tai kulunvalvonnan läpi pääseminen. Esim. Lentokenttäalueella tarkoitetaan turvatarkastettua aluetta, jonka sisällä kulkeminen on sallittua vain luvansaaneella henkilöstöllä. Likainen alue voi siis olla esimerkiksi yrityksen aulatilat tai lentoasema-alueen yleiset aulatilat. (Nyström 2015.)

Tietokoneen kaikki tiedot tulee suojata, jotta tietokoneellesi murtautumista (hakkerointi) ei tapahtuisi. Näin olleen myös sinun käyttäjätunnuksesi on yksi este hakkereille ja jotta senkin selvittämiseen heille menee aikaa, on hyvä pitää nämä tunnukset myös salassa muilta ihmisiltä. (Microsoft 2015b.) **Hakkeri** on innokas tietokoneen harrastaja, jolla on tiedot ja taidot murtautua tietojärjestelmään. Hakkerit hakevat haavoittuvuuksia järjestelmästä ja hyödyntävät niitä omien eettisten käsityksiensä mukaisesti. (VAHTI 8/2008.)

Fyysisesti tietoa siirretään monilla eri tavoin; kirjeillä, paperin muodossa jne. Näitä kuljettavat postinjakaja, kuriiripalvelut, yrityksen oma jakelukeskus, työntekijät. Kaikissa muodoissa on usein sama haaste, että ne ovat jonkun henkilön käsissä ja tällöin huolimaton käyttäytyminen saattaa johtaa tiedon häviämiseen. Asiakirjat tulisi pitää henkilön hallussa, kunnes ne on viety ja luovutettu oikeaan paikkaan. Esimerkiksi yhteistyösopimus ulkomailla olevan yrityksen kanssa, jolloin sopimuspaperit olisi hyvä pitää käsimatkatavaroissa. Arvokuljetuspalvelut voivat tulla kyseeseen, jos asiakirjojen arvo tai luonne sitä vaatii. Arvokuljetusta käyttämällä voidaan varmistaa korkean turvallisuustason kuljetus ja vähäinen todennäköisyys joutua vääriin käsiin. (Leppänen 2006, 267.)

4.3 Tekninen tietoturva

Palomuuri suojaa tietokonettasi ja tietoja, jotta luvattomat käyttäjät eivät pääsisi käsiksi tietokoneen tietoihin. Käyttäjä voi hyväksyä yhteydenoton internetistä esimerkiksi pikaviestiohjelmien tai pelien kautta, jolloin palomuuri

hyväksyy siitä suunnasta tulevat tiedot. Taas vastaavasti jos käyttäjä ei hyväksy yhteydenottoa palomuuri estää tiedot sisääntulon. (Microsoft 2015b.)

Virustentorjunta suojaa käyttäjän tietokonetta. Virukset, madot ja troijalaiset ovat luvattomien käyttäjien luomia ohjelmia, jotka on tehty vahingoittamistarkoituksessa. Nämä ohjelmat voivat hidastaa konetta, tuhota tiedostoja tai jopa tuhota koko tietokoneen. Virukset leviävät sähköpostin ja internetistä ladattavien ohjelmien mukana. Viruksentorjuntaohjelma etsii, tarkistaa ja eristää viruksen tai poistaa sen kokonaan tietokoneelta. (Microsoft 2015b.)

Ongelmatilanteissa tulee seurata ohjeita, jotka auttavat käyttäjää toimimaan oikein tilanteessa. US-CERT on Amerikan Yhdysvaltojen tietokoneiden valmiusosasto, joka määrittelee kuinka Yhdysvaltojen virkailijoiden tulisi toimia tilanteessa, jossa on epäilys, että tietokone on otettu haltuun. Kuinka raportointi tulisi tehdä ja mitä tietoja siihen laitetaan. Samoin millä aikamääreillä liikutaan, kun jokin epänormaali tapahtuma on tapahtunut. (US-CERT 2014.)

KATAKRI mainitsee, että henkilötodennuksessa tulee käyttää vähintään salasanaa. Salasanalle on annettu ohjeistus, joka vaatii käyttäjää käyttämään tietyn tasoista salasanaa, mikä esimerkiksi sisältää 9 merkkiä, joista tietty osa tulee olla numeroita, erikoismerkkejä, isoja kirjaimia jne. Salasana tulee vaihtaa tietyin määräajoin. Jos tunnistus epäonnistuu liian monta kertaa peräkkäin, aiheuttaa tämä laitteen lukkiutumisen. (KATAKRI 2011.) Triviaalisalasanalla tarkoitetaan salasanaa, joka on helppo arvata. Triviaalisalasana perustuu yleensä käyttäjän nimeen, perheeseen, ammattiin tai johonkin muuhun henkilökohtaiseen ominaisuuteen (NASA 2014). Microsoftin mukaan vahva salasana muodostu muodosta ja pituudesta. Myös helppo sana käyttäjälle voidaan muokata vahvaksi salasanaksi. Tästä esimerkkinä voisi olla:

HelloU2! – tämä muutettuna vahvaksi salasanaksi – H3ll0 2 U!

Tällöin sana ei muodosta mitään olemassa olevaa sanaa, vaan sisältää vain merkkejä, jotka voidaan helposti tulkita sanaksi ja tätä kautta muistaa paremmin. (Microsoft 2015c.)

Sosiaalisen median käyttö yritystoiminnassa ja henkilökohtaisessa käytössä on yleistynyt viime vuosina räjähdysmäisesti. Monet käyttäjät eivät ota huomioon, että sosiaalinen media on avointa tietoa. Sitä rikolliset käyttävät myös haittaohjelmien levittämiseen. Organisaation tulisi tehdä hyvin selkeä linjaus siitä, kuinka sosiaalista mediaa saa käyttää työhön liittyvissä asioissa ja käyttääkö yritys sosiaalista media hyväkseen esimerkiksi markkinoinnissaan. Henkilöstö tulisi kouluttaa sosiaalisen median käyttöön, jotta asetukset ja salasanat olisivat tarpeeksi hyvin tehtyjä ja etteivät kaappausyritykset toteutuisi ja että he osaisivat kirjoittaa vain niitä asioita, joita on sopivaa tuoda esille yleisessä mediassa. (Vahti 4/2010.)

Telefax on vanha tapa siirtää dokumentteja, joka on vielä käytössä laajalti jopa Euroopan pankeissa. Fakseja voidaan kaapata ja toisena ongelmana on se, jos vastaanottajan faksi on yleisellä paikalla, saattaa dokumentti päätyä ulkopuolisten nähtäville. Tämän takia, jos kyseessä on luottamuksellinen tieto, on vastaanottajan syytä odottaa laitteen äärellä, kunnes faksi on saapunut fyysisesti hänen käteensä. Joissakin faksilaitteissa on muisti, joka tulisi tyhjentää, kun faksi on lähetetty tai vastaanotettu. (Leppänen 2006, 280.)

Tietokoneet, muistitikut (USB) tai muut tietoa varastoivat laiteet voivat kadota käyttäjältään. Jos niistä ei pidetä hyvää huolta, ne saattavat jäädä pöydälle, pudota taskusta tai päätyä varastetuksi. Esimerkkinä voisi olla autoon jätetty tietokone. Varas saattaa olla vain kiinnostunut koneesta eikä niinkään tiedosta koneen sisällä, mutta jos koneesta ei ole otettu varmuuskopiota, saattaa tämä aiheuttaa tiedon häviämisen ja sitä kautta vaikuttaa koko yritykseen. Tietoturvaoppaan tulisi opastaa oikeanlaiseen laitteiden kuljettamiseen työn ulkopuolella. (Leppänen 2006, 280.)

Sähköisesti siirrettävää tietoa tulee suojata tarvittavilla salausmenetelmillä. Tiedonluokituksen mukaan tulee miettiä mitä tietoa siirretään ja sen suojauksen riittävyyttä. Tulisi aina huomioida, että sähköisesti siirrettävät tiedot saattavat päätyä väärään paikkaan, kun kirjoitetaan sähköpostiosoite väärin tai valitaan yhteystietojen perusteella sähköpostiosoite ilman, että tarkistetaan, onko osoite oikea. Virheitä sattuu helposti. Tätä varten on hyvä varmis-

taa vastapuolen osoite esimerkiksi lähettämällä tälle viesti, jossa pyydetään lukukuittausta. Vasta kuittauksen jälkeen on turvallista lähettää luottamuksellinen viesti vastaanottajalle. Liian usein sähköpostitse lähetettään tietoa, jonka ei olisi soveliasta joutua muiden käsiin. Sähköposti voi joutua useastakin syystä vääriin käsiin ja se voidaan kaapata matkalla. Tällöin salaista ja erittäin salaista tietoa ei ole koskaan hyvä lähettää sähköpostitse vaan käyttää muita menetelmiä. Viesti voidaan myös kaapata välistä tai joku voi hakkeroida itsensä toisen sähköpostiosoitteeseen ja tätä kautta luottamuksellinen tieto joutuu vääriin käsiin. Tämä välttämiseksi tulisi käyttää tarpeeksi vahvoja salasanoja, virus-turvaa sekä käyttää esimerkiksi salattua yhteyttä (VPN yhteys). Tiedostot voidaan salata salasanalla. (Leppänen 2006, 280.)

4.4 Työskentely työpaikan ulkopuolella

Useissa yrityksissä työskennellään työpaikan ulkopuolella ja tämä tuo haasteita tietoturvallisuuden ylläpitämisessä samalla tasolla kuin olisi työpaikalla. Eräät yritykset eivät anna työntekijöille lupaa viedä töistä mitään laitetta kotiin tai ulkomaille, vaan yrityksestä siirretään sisäisesti tiedot, kun henkilö on paikan päällä. Tässä kappaleessa esittelen eri asioita, joita tulisi ottaa huomioon, kun olet töissä työnpaikkasi ulkopuolella.

Etätyöllä tarkoitetaan työskentelyä jostain muulta kuin työpaikaltasi. Näitä voivat olla koti, hotelli, asiakkaan tilat tai mikä tahansa paikka, joka ei ole oma työpisteesi. Kaikkea työtä ei voi tehdä ulkopuolelta käsin, jos tieto on salaista. Tietoa ei tulisi siirtää verkon yli, vaikka käytettäisiin salattua yhteyttä. Etälaitteiden tulisi olla niin valmistettuja, että ne on suojattu yrityksen tietoturvallisuuden mukaisesti. Etälaitteiden tulisi sisältää haittaohjelmasuojauksen sekä tarvittavat tietoliikenneyhteydet. (Vahti 4/2013.)

On hyvä huomioida, että tietokoneessa ei välttämättä tarvitse pitää kaikkea tietoa tietokoneen sisällä, vaan tiedot voidaan pitää palvelimilla, joihin voidaan ottaa suojattuja yhteyksiä myös kannettavalla tietokoneella. Näin tarvittava tieto voidaan siirtää vain tarvittaessa tietokoneellesi. Kannettavan tietokoneen asetukset pitää ohjelmoida tietoturvalliseksi. Yhteydet kuten Bluethooth ja Wi-Fi on pidettävä piilossa tai niin, että kukaan ei pääse käsiksi ko-

neeseesi ilman, että tiedät asiasta. On hyvä huomioida, että kannettava tietokone lukkiutuu automaattisesti ja salasana on riittävän vahva. Luottamukselliset tiedot tulisi säilyttää kryptattuina. (Vahti 4/2013.)

Vahti antaa hyvät ohjeet siitä, kuinka suojata älypuhelimet, joiden toimintamallit ovat lähes samaa tasoa kuin tietokoneilla. Ongelmanahan on, että nämä laitteet kulkevat ulos rakennuksesta ja sisältävät paljon luottamuksellista tietoa. Niihin voidaan asentaa ja niistä ottaa tietoja ilman, että käyttäjä sitä huomaa. Tähän Vahti on antanut hyvät ohjeet, joiden avulla yrityksen ja käyttäjän tiedot voidaan suojata. Vahti ohjeet jakautuvat neljään eri ryhmään: SIM-kortti ja liittymä, haittaohjelmien torjunta, tietoliikenneyhteydet, etähallinta. Tavalliset GSM-puhelimet, joissa ei ole tietoliikenneyhteyksiä ovat helpommin suojattavissa ja näiden käytössä ei ole niin suurta tiedonmenetysriskiä. Toki puhelimia voidaan kuunnella ja tekstiviestejä lukea, mutta esim. sähköpostia, joka sisältää usein paljon luottamuksellista tietoa, ei voida menettää. (VAHTI 2/2007.)

On hyvä huomioida, että kaikista asioista ei tulisi puhua julkisissa paikoissa, jossa voi olla muita ihmisiä kuulemassa. Aina ei pysty kumminkaan näitäkään tilanteita välttämään ja näin ollen on hyvä puhua asioista selkeästi, mutta käyttäen sovittuja projektinimiä ja välttää sanomasta yritysten tai henkilöiden nimiä. Esimerkiksi ”se henkilö, joka eilen tavattiin” tai ”se yritys, jossa oltiin käymässä viime viikolla”. Jos taas työskentelet tietokoneellasi esimerkiksi lentokoneessa, joku voi helposti lukea näytöltäsi mitä siinä lukee – tämä aiheuttaa tietoturvallisuusriskin – tämä tulisi estää esimerkkisi näyttösuojalla tai sitten ei tulisi tehdä mitään töitä vastaavanlaisissa paikoissa. Sama asia koskee myös kännyköiden käyttö. On hyvä aina huomioida ympäristö ja kuka istuu / seisoo sinun vieressäsi ja onko henkilö jostain syystä erityisen kiinnostunut sinun toimistasi. (Nyström 2007.)

Kotoa käsin työskentely on lisääntynyt. Työnantajat odottavat, että työntekijä on nykypäivänä saatavilla myös vapaa-aikana. Tämä aiheuttaa haasteita tietoturvallisuuden osalta. Työntekijöiden on osattava käyttää laitteitaan oikein ja ymmärrettävä tietoturvallisuusluokitukset. Yrityksen tulisi asentaa tarvittavat

yhteydet ja ohjelmat kotikoneelle, jotta työskentely kotoa käsin on yrityksen tietoturvallisuusohjeistuksen mukaista. Kotikoneelle tulisi luoda jokaiselle käyttäjälle oma henkilökohtainen käyttäjätunnus. Kotikoneella ei tällöin tulisi avata epäilyttäviä sähköposteja tai käyttää mitään ulkopuolisia USB-laitteita, jotka saattavat altistaa kotikoneen haittaohjelmille. Varmuuskopiointi tulisi järjestää myös kotikoneelle, jos työntekijä säilyttää tietoja siellä, mikä ei tosin ole suositeltavaa. (Leppänen 2006, 280.)

5 Kuinka opas tehdään?

Kun opasta aletaan kirjoittaa, sitä ei kirjoiteta itselle vaan lukijoille. Tällöin oppaan tulee voittaa lukijan aika ja mielenkiinto. Tarkoitan sitä, että jos asiaa ei ole kirjoitettu tarpeeksi tehokkaasti ja mielenkiintoisesti lukija kyllästyy ja jättää oppaan lukematta. Opas kirjoitetaan teoreettiseen pohjaan nojaten, mutta siihen voi lisätä värikkyyttä, joka herättää lukijan mielenkiinnon. Sanakikkailulla ei voiteta lukijan mielenkiintoa. Lukija ei välttämättä ymmärrä tekstin tarkoitusta tai merkittävyyttä, jos sanat eivät hänelle aukene. (Mertanen 2007, 24-25.)

Oppaan suunnitteluvaiheeseen pitää varata tarpeeksi aikaa ennen kuin aloittaa kirjoittamisen. Tulee suunnitella mitä, miksi ja kenelle kirjoitetaan, jotta vastaanottavan osapuolen kiinnostus saadaan heräämään. Ajatuksia kannattaa kirjoittaa paperille ja hahmotella kokonaisuutta. Kun alkaa kirjoittaa, on syytä yrittää miettiä kuulija kuntaa. Sitä mitä he haluavat tietää ja mitkä olisivat heidän tarkentavat kysymyksensä asiaan. Yleensä ensimmäinen versio ei tuota haluttua tulosta, joten tulee varautua siihen, että oppaasta tulee useampia versioita. Ensin kannattaa miettiä sisältöä, sitten järjestystä ja lopuksi korjata teksti. Tästä usein muodostuu se ensimmäinen versio, joka voi saada vielä paljonkin kritiikkiä. Tämän jälkeen kannattaa alkaa paneutua tekstiin tarkemmin ja varmistua siitä, että teksti on jouhevaa, seuraa punaista lankaa, eikä jätä kysymyksiä lukijalle. Kun viimeinen versio on tehty, Mertanen kertoo kirjassaan että; ”Alan vanha sääntö; viimeisen lukukerran jälkeen lue vielä kerran”. (Mertanen 2007, 30-31.)

Ohjeen kirjoittamisessa tulisi olla hyvä yhteenveto heti alussa, joka antaa selkeän kuvan mitä ohjeesta löytyy ja mistä sekä kenelle se on tarkoitettu. Koska ihmiset usein välttävät ohjeiden lukemista, nousee alku kaneetin tärkeys suureen arvoon. Hyvin kirjoitettu teksti on tärkeätä, koska jos jokin voidaan ymmärtää väärin, se ymmärretään väärin useasti. Myös liiallinen varoittelu aiheuttaa yleensä sen, että henkilö ei joko uskalla tehdä mitään tai sitten hukkuu kaikkiin varoituksiin ja sitä kautta ei muista edes niitä tärkeimpiä varoituksia. Varoittelusta tulee miettiä niin, että ne kaikista tärkeimmät asiat tuodaan selkeästi varoituksilla esille. (Korpela 2017.)

6 Opinnäytetyön tutkimuksellisuus

Toiminnallinen opinnäytetyön tekeminen ja sen teoriaa sekä tutkimuksen menetelmät. Käsitellään laadullinen menetelmät ja mittareita sekä lopuksi teemoittelun teoriaa.

6.1 Toiminnallinen opinnäytetyö

Toiminnallinen opinnäytetyö on yksi toteutustapa tehdä lopputyö. Toiminnallisessa opinnäytetyössä on raportointiosuus ja produkti eli tuotos. Tällöin näiden kahden työn kokonaisuus on olennaista lopputyössä. Näiden tulisi olla toistensa jatkumoa. Toiminnallisesta opinnäytetyöstä tulisi selvitä mitä, miksi ja miten asiat on tehty. Millainen on työprosessi, tuotos ja arvio opitusta. (Vilkka 2004, 51-53.)

Toiminnallinen opinnäytetyö sisältää produktisen osuuden, joka on suunnattuna yritykselle sekä raportin, joka kertoo prosessin siitä, kuinka produktinen osuus eli toiminnallinen tuotos on tehty. Produktiin vaaditaan toisenlaista tekstiä, koska se on tarkoitettu, tässä tapauksessa, yrityksen työntekijöille. Tekstin tulee silloin olla puhuttelevaa lukijoille, eikä se saa tuottaa tutkimuksellista työtä. (Vilkka 2004, 51-53.)

Opinnäytetyöraportti on kertomus, joka kertoo kuinka projekti ja työprosessi on tehty. Se kertoo sen, kuinka on päädytty kirjoittamaan toiminnallinen tuotos. Millaisia kysymyksiä tuotoksessa ollaan ratkomassa ja kuinka niihin on saatu vastaukset eli mitä keinoja on käytetty vastauksien saamiseksi. Opin-

näytetyö kertoo myös, kuinka tuotoksessa on päädytty tiettyihin valintoihin ja ratkaisuihin. (Vilkka 2004, 55-56.)

6.2 Haastattelu- ja kyselytutkimus

Tässä opinnäytetyön alussa haastattelin turvallisuusalalla jo pitempään olleita henkilöitä, joilta kysyin heidän mielipidettä; mikä tekee hyvän tietoturvallisuusoppaan? Tarkoituksena saada heiltä tietoa, mitkä heidän mielestä on olleet hyviä oppaita ja tätä kautta saada mahdollisimman toimiva opas organisaation henkilöstölle. Kun opas oli valmis, lähetin valmiin oppaan kohderyhmälle, jotka olivat osittain samoja henkilöitä kun haastattelussa sekä henkilöitä joilla ei ollut tietoturvallisuusalalla kokemusta. Tässä halusin mitatta kuinka olin onnistunut työssäni.

Useat meistä ovat joskus olleet haastateltavina kauppakeskuksissa ja ottaneet osaa kyselyihin ehkä jonkin palkinnon motivoimana. Nämä ovat tapoja, joilla tehdään tiedonkeruuta. Tietoa käsitellään eri mittarien ja analyysien kautta ja näin saadaan tutkimustuloksia. Tutkimustuloksia voidaan käyttää yrityksen tai tieteen kautta asioiden parantamiseen ja kehittämiseen. Kyselytutkimuksessa on tapana kerätä tietoa, jota voidaan tarkastella tiettyjen mittareiden tai analyysien kautta. (Vehkalahti 2008, 11.)

Kyselytutkimukset voivat olla määrällisiä tutkimuksia, joissa käytettään tilastollisia menetelmiä tiedon keruuseen, Ne sisältävät usein monivalintakysymyksiä. Kyselyt sisältävät useimmiten lukuja ja numeroita, joita sitten voidaan verrata ja mitata. Kyselytutkimukset voivat olla myös kysymyksiä, joihin tulee vastata sanallisesti. Sanallisesti vastatut kysymykset tuottavat laadullista tuloksia. (Vehkalahti 2008, 47-50.)

Tutkija tai haastattelija esittää ennalta tehdyt kysymykset suoraan vastaajalle. Tämä voi tapahtua tapaamisen tai puhelinyhteyden kautta. Tällöin usein tutkija voi auttaa vastaajaa, jos hän ei ymmärrä kysymyksen muotoa ja näin saada tarkempia vastauksia sekä tulos saattaa muodostua tarkemmaksi kuin kyselyssä. Haastattelut on hyvä nauhoittaa tai ainakin tehdä tarkat muistiinpanot, kun vastaaja vastaa kysymyksiin. Haastattelun huonona puolena on se,

että mittavien haastattelujen teko ja toteutus vievät paljon aikaa kun taas kyselyllä voidaan saavuttaa suuriakin määriä ihmisiä. (Hirsjärvi 1997, 205-206.)

6.3 Laadullinen ja määreellinen tutkimus

Mittarien kautta saadaan määrällistä tutkimustulosta ja analyysin kautta saadaan laadullisia tuloksia – erona on, että laadullinen tutkimustulos pureutuu tarkemmin saatuihin vastauksiin. Arvojen, asenteiden ja mielipiteiden tutkiminen ei ole yksiselitteistä, niissä on paljon epävarmuustekijöitä kuten esimerkiksi se, että ymmärrettiinkö kysymys oikein, mikä oli vastaajan asenne, tausta, ikä jne. Kun mitattavia tuloksia on riittävästi ja tulos on niin sanotusti kylläinen, voidaan alkaa tehdä johtopäätöksiä. Poikkeamat kuuluvat asiaan, mutta niiden mahdolliset aiheuttajat täytyy tutkia. (Vehkalahti 2008, 13.)

Mittareita löytyy paljon entuudestaan ja niitä voi rakentaa itsekin. On tärkeät ymmärtää, mitä halutaan mitata ja jos mittari ei toimi oikein, sitä tulee muokata, jotta tulokset saadaan mitattavaan muotoon. (Vehkalahti 2008, 13.)

Edellisessä kohdassa toin esille jo joitain asioita, jotka määrittelevät laadullisen ja määreellisen erot. Mielekästä on kuitenkin, jos näitä voidaan tutkia samanaikaisesti eli kysely perustuukin sekä numeraalisiin että sanallisiin kysymyksiin. Laadullinen on usein sanallista, joka antaa yksityiskohtaista tietoa asiasta. Sitä analysoidaan eri lähtökohdista (Hirsjärvi 1997). Vastaajat voivat olla tietyn alan ammattilaisia ja osaajia, kun taas jotkut vastaajista voivat olla käyttäjiä ja näiden eroavuutta voidaan tutkia. Määrällinen on usein numeraalista ja sitä voidaan tutkia kaavojen kautta ja näin saada keskimääräistä tietoa tutkittavasta asiasta (Vehkalahti 2008, 13.)

6.4 Teemoittelu

Teemoittelua varten tulee olla aineistoa, joka voi olla esimerkiksi haastatteluista tai kyselystä saatuja vastauksia. Teema löytyy kysymyksistä mitä ollaan kysytty. Teemoilla voi olla myös alakohtia, jotka tarkentaa pääteemaa. Kun kaikki vastaukset on laitettu niin sanotusti yhteen koriin ja niitä aletaan analysoimaan. Tällöin vastauksista aletaan hakemaan samanlaisuuksia tai erovai-

suuksia mitkä kuuluvat teema alueeseen. Joskus saattaa löytyä joitain uusia teemoja, joita ei edes ajateltu. Teemoittelun tulee seurata tarkasti vain vastauksia ei lisätä omaa tekstiä siihen. Teemoittelu voi olla myös kvantifiointaalista, jolloin haetaan yhteistä nimittäjää eli teemoja. Teemoissa voidaan myös käyttää sitaatteja, jotka toimivat eräänlaisina todisteina vastauksista. Sitaatteja ei tule käyttää liikaa vaan lähinnä semmoista joka vastaa teema kysymykseen parhaiten ja on siis keskiarvoinen vastaus ryhmästä. (Saaranen-Kauppinen 2006.)

7 Opinnäytetyön tekoprosessi

Työni lähti liikkeelle siten, että lähestyin yrityksiä kyselyllä, jossa selvitin yritysten kiinnostusta saada tietoturvallisuusoppaan tai päivittää olemassa olevaa. Tämä vaihtokauppa yritys oli minulle jo ennestään tuttu ja olin aiemmin puhunut heidän kanssaan tietoturvasuunnitelmasta. Tiesin, että heille oli juuri tehty tietoturvasuunnitelma ja näin ollen olin heihin yhteydessä tietoturvaoppaan tekemisestä. He hyväksyivät ehdotukseni ja aloitin projektini tutustumalla heidän tietoturvasuunnitelmaan. Tästä tietoturvasuunnitelmasta on otettu tiettyjä haluttuja prosesseja tietoturvallisuusoppaaseen. Kävin heidän kanssaan keskustelua muun muassa siitä, mitä he näkevät tärkeinä asioina tietoturvaoppaassa. Heidän mielestään tärkeitä asioita olivat tarpeeksi kattava sisältö, helppolukuisuus ja ymmärrettävyys. Lisäsimme siihen myöhemmin myös, lauselman seurannasta, ettei se vain jäisi pölyttymään hyllyn reunalle.

Ensimmäisessä vaiheessa tutustuin alan tärkeimpiin teoksiin ja olemassa oleviin oppaisiin. Katsoin tärkeäksi kerätä kaiken sen tiedon, jota työntekijät tarvitsivat päivittäisessä työssään, jotta kykenin valitsemaan relevantit tiedot oppaaseen. Tutustuin myös siihen, miten hyvä opas kirjoitetaan, jotta saisin siitä jouhevan kokonaisuuden. Tein muutamia haastatteluja ihmisille, jotka olivat olleet turvallisuusalalla jo pitempään ja kuuntelin heidän mielipiteitään hyvän tietoturvaoppaan kirjoittamisessa (liite 1). Kun olin saanut tietoturvaoppaan lähes valmiiksi, minä esittelin sen johdolle. Sain esittelyn yhteydessä vielä palautetta ja huomioita liittyen heidän päivittäisiin tehtäviin ja lisäsin ne vielä oppaaseen ennen kuin ojensin valmiin tietoturvaoppaan heille.

8 Tulokset

Tämän lopputyön tuloksia ovat tietoturvallisuusopas kohdeyritykselle ja kysely, joka mittaa oppaan onnistumista yrityksen henkilöstölle.

8.1 Yrityksen arviointi tietoturvallisuusoppaasta

Yrityksen toimitusjohtajan arvion mukaan tietoturvallisuusopas oli hyvä ja hyödyllinen opas työntekijöille. He kokivat saaneensa edistettyä monia asioita työntekijöiden keskuudessa. Toimitusjohtaja jatkoi, että IT työntekijän mukaan, virusten ja muidenkin virhekäyttöjen määrä laski huomattavasti sekä työntekijöiden kiinnostus tietoturvallisuuteen lisääntyi.

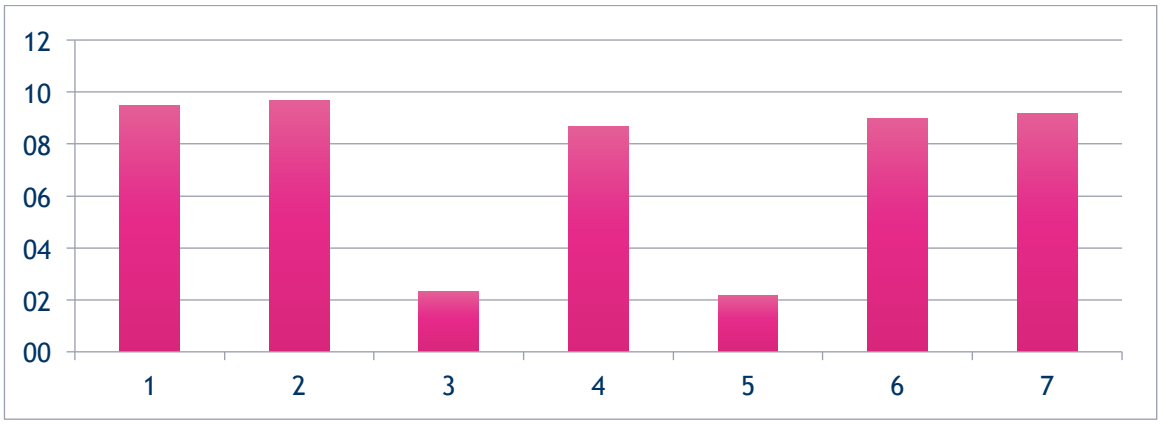
Aiemmin tehty tietoturvasuunnitelma oli hyvä, mutta tietoturvaoppaan kautta tämä tietotaito saatiin myös jalkautettua henkilöstölle. Nykyään uusien työntekijöiden tulee lukea opas ja allekirjoituksellaan vahvistaa, että ovat sen lukeneet ja ymmärtäneet.

8.2 Kyselyn tulokset

Kysely oli suunnattu eri toimialoilla työskenteleville käyttäjille sekä turvallisuusalan ammattilaisille, joilla on operatiivista kokemusta tietoturvasta. Kaikille kyselijöille lähetettiin englanninkielinen tuotos eli kyselykaavake (liite 2) sekä tietoturvallisuusopas (liite 3).

Kyselykaavakkeen kolme ensimmäistä kysymystä liittyi vastaajaan ja sitä kautta voidaan arvioida vastaajan taustat. Näistä selviää, että käyttäjätasolla harvoin on tietoturvallisuuskoulutusta takana. He eivät olleet opiskelleet aiheita. Turvallisuusalalla työskentelevät taas olivat käyneet kursseja ja he joutuvat olemaan työssään tekemisissä tietoturvallisuuden kanssa.

Alla olevassa kuviossa (kuvio 1) näkyvät vastanneiden kysymyskohtaiset keskiarvot alkaen kysymyksestä neljä ja päättyen kysymykseen kymmeneen. Nämä olivat määrällisiä kysymyksiä.



Kuvio 1; Kysymysten keskiarvot

Kuvio ylhäällä kuvaa kysymyksiä nelosesta eteenpäin sitten että, tolppa yksi on neljännen kysymyksen tulos (x-akselissa). Y-akseli kuvaa tuloksia 1-10 siten että, 1 vastaa; vähän tai ei olenkaan samaa mieltä. 10 vastaa; paljon tai täysin samaa mieltä. 4 – 10 olivat kysymyksiä, kuinka ymmärrettävä tietoturvallisuusopas oli sekä sisälsikö opas vaikeaa tekstiä. Määrällisestä tutkimuksesta voi tulkita, että opas on onnistuttu rakentamaan loogiseen järjestykseen, joka kasvaa, kun lukija pääsee vauhtiin oppaan kanssa. Teksti on tarpeeksi selkokielistä ja asioita on avattu oikealla tavalla, jotta ne olisivat ymmärrettäviä myös henkilöille, jotka eivät ole olleet tekemisessä tietoturvallisuuden kanssa. Oppaan pituus on saatu pidettyä tarpeeksi lyhyenä, vaikkakin asiaa on paljon eikä opasta ole yritetty lyhentää liikaa. Lähes kaikki olisivat tyytyväisiä, jos heidän työnantajansa antaisi vastaavanlaisen tietoturvallisuusoppaan heille luettavaksi, kun astuvat palvelukseen uutteen organisaatioon. Kysymys 10 oli tarkoitettu enemmän turvallisuusalan ammattilaisille ja kuinka he näkivät jos oppaaseen oli tuotettu kaikki tärkeimmät tietoturvallisuutteen liittyvät asiat. Tämän keskiarvoksi tuli 9,2, joka kertoo, että lähes kaikki antoivat täydet pisteet.

Kysymykset 11 ja 12 olivat laadullisia kysymyksiä, joihin kyselyssä pyydettiin sanallista vastausta. Vastaajina oli turvallisuusalan ammattilaisia, jotka joutuvat lähes päivittäin työssään tekemisiin tietoturvallisuuden kanssa. Heidän tuoma käytännönläheisyys ja osaaminen tuovat tarkkaa laadullista tuotosta. Näistä vastauksista tuli positiivista palautetta, että opas on hyvä paketti, joka

on tuonut esille kaikki tärkeimmät tietoturvallisuuteen liittyvät asiat. Eräs oli maininnut, että kirjoittaja on hyvin tuonut käytännön esimerkkien kautta vaikeat asiat ymmärrettävään muotoon. Puutteena nähtiin yhteenveto heti alussa, jossa olisi kaikki tarvittavat tiedot ja taidot. Eräs toinen puhui samasta asiasta käyttäen sanaa ”taulu”, jossa olisi tärkeimmät asiat. Eräs vastaajista olisi halunnut saada tarkistuslistan liitteeksi. Nämä kaikki puutteet olivat erittäin hyviä huomioita ja ehdottomasti sellaisia asioita, joita tulisi jatkossa ottaa huomioon.

9 Johtopäätökset ja oman työnarviointi

Saatujen tulosten pohjalta voidaan todeta, että tietoturvallisuusopas on suhteellisen hyvin onnistunut ja tuottanut tutkimuskysymykseen vastauksen, että oppaassa oli kaikki tärkeimmät asiat tuotu esille ymmärrettävässä muodossa yrityksen henkilöstölle. Saatujen tulosten myötä oli myös huomattavissa, että tiivistelmän teko olisi tärkeätä, koska henkilöstö voisi pitää se helposti saatavilla ja näin se pysyisi hyvin mielessä. Samoin tarkistuslistan tarpeellisuus, kun halutaan varmistua siitä, että kaikki osa-alueet tulee noudatettua. Jatkoa nähden tulen käyttämään näitä tietotaitoja hyväkseni tuoden ne uusiin organisaatioihin.

Saatu palaute kohde yritykseltä oli positiivinen. Heidän mielestä tietoturvallisuusoppaan jälkeen tietoturvan taso oli parantunut ja tietoturvallisuus suunnitelma oli saatu jalkautettua yrityksen henkilöstölle. Henkilöstö oli valveutunut tekemään tietoturvaa paremmin ja tulivat kysymään apua kun havaitsivat poikkeuksia normaali toiminnassa.

Tulosten luotettavuus on ollut hyvällä tasolla, perustuen vastaajien taustoista ja vastausten laadukkuudesta. Vastauksiin oli selkeästi käytetty aikaa ja vaivaa. Monet vastaajista olivat tuoneet hyvin asioita esille mikä kuvastaa heidän kiinnostuksesta asiaan. Tästä saadut hyödyt tulevat näkymään jatkossa minunkin työssäni.

Omasta mielestäni tietoturvaopasta voisi parantaa vielä useallakin eri tavalla. Yksi näistä on saatujen tulosten perusteella rakentaa tarkistuslista, jota työn-

tekijät voivat tarvittaessa käyttää kun haluavat varmistaa, että he ovat seuranneet opasta. Strategia kello, joka on vuoden mittainen, johon on merkattu että tiettyinä aika määreinä tulisi esimerkiksi vaihtaa salasanaa, tarkistaa tietokoneen viirusturva jne. Lisäisin myös tärkeimmät asiat taulun muotoon toimiston seinälle, jotta ne pysyisivät hyvin muistissa. Liitteeksi voisi myös rakentaa sarjakuvan, joka kuvaa tietoturvallisuuden asioita. Jotkut ihmiset eivät jaksa / ehdi lukea pitkiä oppaita, vaan halusi nopeasti katso sarjakuvat mikä kertoo tärkeimmät asiakohdat joita tulisi ottaa huomioon.

Lähteet

Painetut

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. 15 painos. Helsinki: Tammi.

ISO/IEC 27001:2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Turva-alueet. Helsinki: Suomen Standardisoimisliitto SFS.

KATAKRI. 2011. Kansallinen turvallisuusauditointikriteeristö. Versio II. Puolustusministeriö.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Tietoturvallisuus. Jyväskylä: Gummerus.

Mertanen, V. 2007. Tietokirjoittajan käsikirja. Tampere: Osuuskunta Vastapaino.

VAHTI. 2/2007. Älypuhelimien tietoturvallisuus – hyvät käytännöt. Helsinki: Edita Prima.

VAHTI. 4/2013. Henkilöstön tietoturva ohje. Helsinki: Edita Prima.

Vehkalahti, K. 2008. Kyselytutkimuksen mittarit ja menetelmät. Helsinki: Tammi

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

Sähköiset

BSI-Standard 100-1. 2008. Information Security Management System, 10. Versio 1.5. Tulostettu 14.1.2015.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

Elinkeinoelämän. 2016. Yritysturvallisuus. Tulostettu 14.1.2015. http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/.

Henkilötietolaki. (11§)/1999. Tulostettu 31.1.2015. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Hänninen, S. 2014. Tieto. Teollisuuden järjestelmien suojaustarve kasvaa. Tulostettu 27.4.2015. http://www.tieto.fi/menestystarinat/tietoturva-ja-teollinen-internet

Korpela, J. 2017. Ohjeen kirjoittaminen. Tulostettu 12.11.2017. http://jkorpela.fi/kirj/7.7.html

Maunuksela-Malinen, P. 2003. Sähköisen kaupankäynnin aapinen. Tulostettu 31.1.2015 http://www.tieke.fi/pages/viewpage.action?pageId=27590855

Microsoft. 2015a. Social Engineering. Tulostettu 9.1.2015. http://www.microsoft.com/security/resources/socialengineering-whatis.aspx.

Microsoft. 2015b. Tietokoneen suojaus ja turvallinen käyttö. Tulostettu 1.4.2015. http://windows.microsoft.com/fi-fi/windows/understanding-security-safe-computing#1TC=windows-7.

Microsoft. 2015c. Window-Vista. How to create a strong Password. Tulostettu 26.12.2014. http://windows.microsoft.com/fi-fi/windows-vista/tips-for-creating-a-strong-password.

Nasa. 2014. Non-Trivial password. Tulostettu 4.1.2015. http://www.nas.nasa.gov/hecc/support/kb/Password-Creation-Rules_270.html.

Rousku, K. 2015. Turvaopas. Uhkaako toimintaasi meteoriitti vai odotatko lottovoittoa?. Tulostettu 27.4.2015. http://www.turvallisuusopas.fi/tietoturva/uhkaako-toimintaasi-meteoriitti-vai-odotatko-lottovoittoa

Saaranen-Kauppinen, A & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Tulostettu 30.11.2017. http://www.fsd.uta.fi/menetelmaopetus/kvali/L7_3_4.html

VAHTI. 1/2004. Tärkeimmät kehityskohteet. Tulostettu 31.1.2015. https://www.vahtiohje.fi/web/guest/tarkeimmat-kehityskohteet

VAHTI. 2/2010. Tietoaineistojen luokittelu. Tulostettu 11.09.2017. https://www.vahtiohje.fi/web/guest/tietoaineistojen-luokittelu

VAHTI. 4/2010. Sosiaalisen median tietoturvaohje. Tulostettu 22.2.2015. https://www.vahtiohje.fi/c/document_library/get_file?uuid=8b44c0bf-cff3-4e6c-a587-eea58a9e3ad7&groupId=10128&groupId=10229

VAHTI. 8/2008. Valtionhallinnon tietoturvasanaston. Hakkeri. Tulostettu 14.1.2015. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2B_KANNET.pdf

United States Code. 2006. Information Security. Definitions. United States Code, 2006 Edition, Supplement 5, Title 44 - PUBLIC PRINTING AND DOCUMENTS. Tulostettu 21.4.2015. http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf

US-CERT. 2014. Reporting. Tulostettu 1.4.2015. https://www.us-cert.gov/government-users/reporting-requirements

Julkaisemattomat

Nyström, T. 2007. Haastattelu. Nauhoitettu 21.9.2007.

Nyström, T. 2015. Kysely. Sähköposti 9.1.2015. Tulostettu.

Ristola, M. 2015. Kysely. Sähköposti 25.3.2015. Tulostettu.

Kuvio

Liitteet

Liite 1: Haastatelu

Haastattelu

Päivä:
Paikka:
Nimi:

Haastattelu kysymykset, joilla haetaan vastaajan mielipidettä; mikä tekee hyvän tietoturvallisuusoppaan?

1. Oletko ollut tietoturvallisuusalalla?
2. Oletko tehnyt itse tietoturvallisuusopasta aiemmin?
3. Omin sanoin mikä tekee hyvän oppaan?
4. Mitkä osa-alueet tulisi oppaassa tuoda esille?
5. Muita aiheeseen liittyviä asioita joita haluaisitte tuoda esille?

Vastaukset on tallennettu ja kirjattu ylös.

Liite 2: Kyselylomake

I send these questions to you. Please make sure that you have read the attached ”Information Security Handbook”.

Some of the answers you need to choose from 1 to 10;
1 is little or poor and 10 is the best.

1. Did you read the Information Security Handbook?
   Yes / No
2. Have you been involved with information security in your work place?
   From 1 to 10
3. Have you studied information security? When and where?
   When (year only)
   Where (Country)
   Course Yes or No
   University Yes or No
4. The Handbook was made for corporate staff – would you be happy to receive such a Handbook once you start work in a new organisation?
   From 1 to 10
5. Did you understand all the subjects mentioned in the Handbook?
   From 1 to 10
6. Was the handbook too long?
   From 1 to 10
7. Was it easy to read?
   From 1 to 10
8. Was there difficult jargon in the text?
   From 1 to 10
9. How did you feel about the logical order?
   From 1 to 10
10. Did you feel that all the important parts were mentioned in the Handbook?
    From 1 to 10
11. If no, what was missing?
12. Please give short feedback on at least one positive and one negative aspect of the Handbook?

Liite 3: Tietoturvallisuusoppaan sisällysluettelo