

## Yrityksen henkilöstö – merkittävä tietoturvauhka

### Unileverin tietoturvakampanja

Petri Kosunen



Tietojenkäsittelyn koulutusohjelma

<p><b>Tekijä</b> Petri Kosunen</p>	<p><b>Ryhmä</b> Datra09</p>
<p><b>Opinnäytetyön nimi</b> Yrityksen henkilöstö – merkittävä tietoturvaohjelma Unileverin tietoturvakampanja</p>	<p><b>Sivu- ja liitesivumäärä</b> 35 + 4</p>
<p><b>Ohjaaja tai ohjaajat</b> Tiina Koskelainen</p>	
<p>Tämän HAAGA-HELIA ammattikorkeakoululle tehdyn produktityyppisen opinnäytetyön aiheena on yrityksen tietoturva ja siihen liittyvä muistutuskampanja. Opinnäytetyön produktina on yrityksen toimeksiannon perusteella kampanjaa varten tehty esitysmateriaali. Lisäksi produktiin kuuluu suunnitelma kampanjan toteutuksesta. Produkti esitellään opinnäytetyössä ja se on myös opinnäytetyön liitteenä. Sitä ei kuitenkaan yrityksen toivomuksesta jätetä liitteeksi arkistoitavaan kappaleeseen.</p> <p>Opinnäytetyön viitekehyksenä on yrityksen tietoturva sekä siihen liittyvät termit. Yrityksen ja produktin kannalta vain merkittävimmät termit on otettu mukaan työhön. Teoriaosuuden perustana on vuonna 2007 tehty verkkokysely yritysten tietoturvasta. Kyselyyn osallistui 220 yritystä. Verkkokyselyn lisäksi lähdeaineistona on käytetty syksyllä 2011 julkaistun ruotsalaistutkimuksen tuloksia sekä alan kirjallisuutta ja muita ajankohtaisia julkaisuja.</p> <p>Opinnäytetyön produkti on työnantajan toimeksianto. Kampanjan tarkoitus on parantaa yrityksen tietoturvaa muistuttamalla käyttäjiä yrityksen erilaisista tietoturvaan liittyvistä ohjeistuksista sekä tietoturvariskeistä, joita on sekä toimistossa että toimiston ulkopuolella. Yrityksestä toivottiin, että kampanjamateriaaliin käytettäisiin yrityksen globaalia, kesällä 2011 uudistettua tietoturvasivustoa.</p> <p>Lähdeaineiston perusteella yritysten on aiheellista kiinnittää huomiota henkilöstön tietoturvaosaamiseen, sillä ei ole olemassa järjestelmiä, joilla kaikkia inhimillisiä virheitä voitaisiin estää. Henkilöstön kouluttamisella ja säännöllisillä muistutuksilla voidaan yrityksen tietoturvariskiä kuitenkin pienentää merkittävästi.</p>	
<p><b>Asiasanat</b> Tietoturva, tietosuojat, tietokonevirukset, haittaohjelmat, pääsynvalvonta</p>	

Degree Programme in Information Technology

<p><b>Author</b> Petri Kosunen</p>	<p><b>Group or year of entry</b> Datra09</p>
<p><b>The title of thesis</b> Employees – significant information security risk Unilever’s information security campaign</p>	<p><b>Number of pages and appendices</b> 35 + 4</p>
<p><b>Supervisor</b> Tiina Koskelainen</p>	
<p>The subject of this thesis is corporate information security and it also involved an information security reminder campaign for the employer. The campaign consists of a large PowerPoint presentation, reminder slides, which will be shown at the employer’s offices in the Nordic countries, some reminder emails for employees and a plan how all the activities are scheduled. The employer’s material is attached for evaluation but it won’t be available in the archived version.</p> <p>The frame of reference of this thesis is corporate information security and terminology around it. As there are lots of terms the most relevant ones, which are meaningful especially for this thesis or for the campaign, are explained in the theoretical part of the thesis.</p> <p>The basis for the theory is an information security survey which was carried out in 2007 via the Internet. In total 220 companies answered to it. In addition to this survey one Swedish report from autumn 2011 and some literature together with other publications related to information security were used for this thesis.</p> <p>The output of this thesis is the reminder campaign of information security which was commissioned by the employer. The purpose of this reminder campaign is to improve information security within the company by reminding users about the instructions, which are available for them, and about information security risks, which are found within and also outside the company. It was also a wish from the employer that the company’s global information security portal should be used for the campaign material. That portal was renewed in summer 2011.</p> <p>The thesis concludes that companies need to pay attention to keeping the information security knowledge of their employees at least on a certain minimum level. There are no systems which can fully prevent human errors but with knowledge the risk can be reduced remarkably.</p>	
<p><b>Key words</b> information security, privacy protection, computer viruses, malware , access control</p>	

# Sisällys

1 Johdanto .....	1
2 Henkilöstö on yrityksen merkittävä tietoturvauhka .....	3
3 Tietoturva voi olla yritykselle kilpailuetu.....	6
3.1 Tietoturvan määritelmä .....	6
3.2 Tietoturvan osa-alueet .....	8
3.3 Tietoturvapolitiikka.....	9
3.4 Tietoturvasuunnitelma.....	10
3.5 Uhkat ja riskien kartoitus.....	11
3.6 Tietoturvastrategia.....	12
3.7 Jatkuvuussuunnitelma.....	12
3.8 Tietosuoja .....	13
3.9 Standardit.....	13
4 Tietoturvaan liittyvät termit auttavat asian ymmärtämistä.....	15
4.1 Hakkerointi- ja urkkimistapoja .....	15
4.2 Tietomurtojen tekijöitä .....	17
4.3 Muita tärkeitä tietoturvaan liittyviä termejä .....	18
4.4 Uusia trendejä, joilla on vaikutusta yrityksen tietoturvaan.....	20
5 Unileverin tietoturvakampanja .....	23
5.1 Yrityksen esittely.....	23
5.2 Information Security Campaign 2011 -kampanjan esittely.....	23
5.3 Kampanjan suunnittelu .....	25
5.4 Kampanjan toteutus.....	26
5.5 Kustannukset .....	26
5.6 Kampanjan tulosten seuranta ja ideoita jatkokehitystä varten .....	27
6 Yhteenveto .....	29
Lähteet.....	32
Liitteet.....	36
Liite 1. ISC2011-kampanjan lyhyt kuvaus (project charter) .....	36
Liite 2. ISC2011-kampanjan aikataulu.....	37
Liite 3. ISC2011-kampanjan esitysmateriaali .....	38
Liite 4. Kooste näyttötauluilla esitettävistä aineistoista .....	39

# 1 Johdanto

Tämän HAAGA-HELIA ammattikorkeakoululle tehdyn produktityyppisen opinnäytetyön aiheena on yrityksen tietoturva. Sen tavoitteena on selvittää, mitä on yrityksen tietoturva ja millaisia keinoja voidaan käyttää yrityksen tietoturvasta muistuttamiseen. Opinnäytetyön produktina on yrityksen toimeksiannon perusteella tehty suunnitelma kampanjasta, jolla henkilöstöä muistutetaan tietoturvasta. Suunnitelman lisäksi tuotteeseen kuuluu monipuolinen materiaali kampanjaa varten.

Opinnäytetyön aihe löytyi työnantajalta. Aihe on ajankohtainen, sillä lähes päivittäin uutisissa kerrotaan, kuinka yrityksiin on tehty tietomurtoja tai kuinka yksityisten henkilöiden tietoja on jaettu luvattomasti Internetissä. Suurin osa tietoturvaan liittyvistä rikoksista tehdään verkossa ja ne leviävät erittäin nopeasti ympäri maailman. Yrityksissä tietojen kunnollista suojaamista ei voi hoitaa pelkästään teknisillä ratkaisuilla. Tarvitaan lisäksi esimerkiksi käyttäjien koulutusta ja tietoturvaohjeita, jotta käyttäjät saadaan ymmärtämään tietoturvan tärkeys ja heidän oma vastuu asiassa.

Opinnäytetyössä produktiosuutta pohjustetaan selvittämällä teoriaosuudessa yritysten tietoturvatilannetta. Kirjallisessa osuudessa haetaan vastausta ensimmäiseen tutkimuskysymykseen yrityksen keskeisistä tietoturvan osa-alueista. Tässä opinnäytetyössä painopiste on nimenomaan tietovuodoissa ja niiden estämisissä. Tekniset ratkaisut, esimerkiksi palomuurit ja virustorjuntaohjelmat, ovat mukana ainoastaan siltä osin, kuin mitä niiden käyttäminen tai käyttämättä jättäminen vaikuttaa tietovuodon mahdollisuuteen. Sen lisäksi lukijoille määritellään tietoturva sekä avataan yleisimpiä tietoturvaan liittyviä termejä.

Toisena tutkimuskysymyksenä selvitetään, kuinka voitaisiin herätellä käyttäjien mielenkiintoa tietoturvaa kohtaan. Tuotteen toteutuksessa on käytetty hyväksi toisen tutkimuskysymyksen avulla löydettyjä vaihtoehtoja. Kampanjan haasteena on löytää keinoja, jolla henkilöstö saataisiin miettimään tietoturva-asioita. Aihe koetaan tärkeäksi, mutta kova kiire ja tiukat aikataulut ovat työntekijöiden arkipäivää. Näistä syistä johtuen tietoturvaan liittyvät asiat siirretään helposti odottamaan itselle sopivampaa ajankohtaa.

Kolmantena tutkimuskysymyksenä pohditaan, onko tietoturvasta mahdollista kerätä kattava ja mielenkiintoinen materiaali työntekijöille. Produktia varten lähdeaineistoa oli runsaasti. Materiaaliin valittiin mukaan ainoastaan ne yrityksen kannalta kaikkein tärkeimmät tietoturva-asiat, joihin työntekijät törmäävät työssään. Materiaalin kiinnostavuuden lisäämiseksi aineistossa käytetään paljon käytännön esimerkkejä.

Neljännellä tutkimuskysymyksellä selvitetään, kuinka kehittää ja ylläpitää työntekijöiden tietoturvaosaamista. Yleisesti oletetaan, että koulutus on tärkein keino osaamisen kehittämiseen. Henkilöstön osaamista tietoturvaan liittyvissä asioissa voidaan kuitenkin kehittää ja ylläpitää myös muilla keinoin, kuten säännöllisillä muistutusviesteillä.

Opinnäytetyön produkti rajataan yrityksen toivomuksesta kampanjaksi, jolla muistutetaan henkilöstöä tietoturvasta. Toivomuksena oli, että olemassa olevaa yrityksen globaalia aineistoa käytetään hyväksi mahdollisimman paljon ja käyttäjiä ohjataan yrityksen tietoturvasivuille hakemaan lisätietoja. Yrityksellä on valtavasti tietoa tietoturvasta, mutta käyttäjiä varten haluttiin lyhyempi ja helppolukuisempi aineisto, josta löytyisi tärkeimmät asiat nimenomaan yrityksen Pohjoismaiden työntekijöille. Materiaali haluttiin englanninkielisenä, jotta sitä voitaisiin käyttää eri maissa. Materiaalia tuetaan käyttäjille lähetettävillä sähköpostiviesteillä sekä toimistojen näyttötaululla viikoittain vaihtuvilla muistutusviesteillä. Produkti esitellään opinnäytetyössä ja se on myös opinnäytetyön liitteenä. Sitä ei kuitenkaan yrityksen toivomuksesta jätetä liitteeksi arkistoitavaan kappaleeseen.

## 2 Henkilöstö on yrityksen merkittävä tietoturvaus

Yrityksen tietoturva on aina ajankohtainen aihe. Lähes päivittäin saamme kuulla uutisista ja lukea lehdistä, kuinka yritysten tietojärjestelmiin on onnistuttu murtautumaan tai kuinka yksityisten henkilöiden henkilötietoja on paljastettu Internetissä. Maailma muuttuu nopeasti ja yhteydet maiden, yritysten ja ihmisten välillä lisääntyvät. Tämä kehitys tuo tullessaan jatkuvasti uusia tietoturvaus.

Tietotekniikan liitto ry, Symantec ja Rittal tutkivat vuonna 2007 verkkokyselyllä pienten ja keskisuurten yritysten tietoturvatilannetta. Kyselyyn vastasi 220 yritystä. Näiden yritysten työntekijämäärät olivat 20–250 henkilöä. Tutkimuksen perusteella tietoturvaus voidaan jakaa kolmeen ryhmään. Niistä ensimmäiseen kuuluvat verkkotietoturvaan ja IT-järjestelmiin liittyvät ongelmat ja uhat, kuten roskapostit, verkon yli tapahtuvat hyökkäykset sekä laitteisto- ja ohjelmistoviat. (Tietotekniikan liitto ry 2007.)







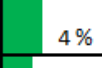
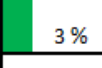
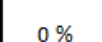
Fyysiset uhat, jotka kohdistuvat yrityksen tietoihin ja järjestelmiin, muodostavat toisen ryhmän. Näitä ovat esimerkiksi onnettomuudet, tulipalot, vesivahingot, salakuuntelu sekä laitevarkaudet. (Tietotekniikan liitto ry 2007.)

Taulukko 1. Yrityksen merkittävimmät tietoturvaus (Viestintätoimisto Conexio Oy 2007)

	10 %	20 %	30 %	40 %	50 %	60 %
Työntekijöiden tietämättömyys tai huolimattomuus						59 %
Virukset, troijalaiset, muut haittakoodit						49 %
Laitteistovika						36 %
Roskaposti						31 %
Fyysinen onnettomuus (tulipalo, vesivahinko, jne.)						27 %
Laitteen katoaminen, varkaus						27 %
Tietojen urkkiminen työntekijöiden hyväuskoisuutta käyttäen						26 %
Ohjelmistovika						24 %
Mainos- ja vakoiluohjelmat						24 %
Sisäisten tietoturvakäytäntöjen puuttuminen						24 %
Tietoturvausohjelmistot						20 %
Tietomurrot						14 %
Tietojen urkkiminen tai salakuuntelu teknisin keinoin						5 %

Kolmanteen ryhmään kuuluvat järjestelmien käyttäjät. Yritysten työntekijöistä on tullut suurin tietoturva-uhka yrityksille. Taulukosta 1 näkyy, että yli puolet verkkokyselyyn osallistuneista ilmoitti merkittävimmän tietoturva-uhkan aiheutuvan työntekijöiden tietämättömyydestä tai huolimattomuudesta. Neljäs kyselyyn vastanneista on ilmoittanut tietojen urkkimisen olevan merkittävä uhka yrityksessä ja lisäksi lähes neljäs on ilmoittanut sisäisten tietoturvakäytäntöjen puuttumisen aiheuttavan uhan yrityksen tietoturvalle. Taulukosta 2 selviää, että yleisin yksittäinen syy tietojen katoamiseen on työntekijöiden tahaton virhe. Myös varkaudet ja murrot, haittakoodit, sisäisten sääntöjen puute ja työntekijöiden ilkivalta aiheuttavat yrityksissä tietojen katoamista. (Tietotekniikan liitto ry 2007.)

Taulukko 2. Yrityksen tietojen katoamisen syyt (Viestintätoimisto Conexio Oy 2007)

		10 %	20 %	30 %	40 %	50 %	60 %
Työntekijöiden tahaton virhe							
Järjestelmävikä, järjestelmän kaatuminen							
EOS							
Varkaus, murto							
Haittakoodit							
Sisäisten sääntöjen / rajoitusten puute							
Fyysinen onnettomuus							
Työntekijän ilkivalta							
Tietomurto							

Verkkokyselynä tehdystä tutkimuksesta kävi myös ilmi, että tietoturvasoa heikentää merkittävästi esimerkiksi käyttäjien tietotaso, rajallinen tietoturva-budjetti sekä se tosiasia, että yritysjohto ei aina ymmärrä tietoturvan tärkeyttä. (Tietotekniikan liitto ry 2007.) Yksi viimeisimmistä ruotsalaistutkimuksista paljastaa, että yli puolet (55 %) ruotsalaisten pörssi-yhtiöiden IT-päälliköistä uskoo työnantajansa yritystietoa vuotavan yrityksen ulkopuolelle, esimerkiksi henkilökohtaisten sähköpostitilien kautta. Monet näiden yritysten johtajista eivät ole tietoisia siitä, kuinka paljon häiriötä yrityksen toiminnalle voi koitua tietovuodosta. (Tietoviikko 2011.)



Yksi suurimmista tietoturva-ongelmista yrityksissä aiheutuu työntekijöiden tietoturvakäytäntöjen laiminlyömisestä. Tietoturvakoulutus auttaa osaltaan tietoturvaongelmien ehkäisyssä. (Karjalainen 2011, 157.) Yritysten tulisikin kiinnittää enemmän huomiota nimenomaan tietoturvakoulutukseen, sillä tutkimuksen mukaan sekä pienet että keskiuuret yritykset keskittyvät suojaamaan IT-järjestelmiä pääasiassa teknisin keinoin (Viestintätoimisto Conexio Oy 2007).

### **3 Tietoturva voi olla yritykselle kilpailuetu**

Yleisesti puhutaan joko tietoturvasta tai tietoturvallisuudesta. Niillä tarkoitetaan samaa asiaa. Laaksonen, Nevasalo ja Tomula (2006, 17) kirjoittavat, että ”Tietoturvallisuus on pieniä tekoja osana jokapäiväistä toimintaa. Hyvä tietoturvallisuus on osa organisaatiokulttuuria, jolloin kaikki ymmärtävät tietoturvallisuuden merkityksen ja työskentelevät sen saavuttamiseksi ja ylläpitämiseksi.”

Yritykselle tietoturva on oikeastaan kilpailuetu edellyttäen, että se on hoidettu asianmukaisesti. Liiketoiminnan jatkuvuuden edellytykset paranevat, kun koko liiketoimintaympäristö huolehtii tietoturvasta osana jokapäiväistä, normaalia toimintaa. (Laaksonen ym. 2006, 17–18.) Tietoturvan voidaan kuvitella muodostavan ketjun useista laitteista ja ihmisistä. Perinteinen sanonta pitää hyvin paikkansa myös tässä kuvauksessa, sillä ketju on niin vahva kuin sen heikoin lenkki. Hyökkääjä yrittää jatkuvasti löytää yhdenkin heikon kohdan, jonka avulla voisi päästä sisälle yrityksen koko järjestelmään. (Järvinen 2002, 28.)

Henkilöstön kouluttaminen on yksi merkittävimmistä keinoista yrityksen tietoturvan kehittämisessä. Yrityksen henkilöstölle suunnatuilla tietoiskuilla voidaan tehokkaasti muistuttaa tietoturvan tarpeellisuudesta. Yrityksen tietoturvaa voidaan kehittää myös esimerkiksi laatimalla helposti ymmärrettäviä ohjeita käyttäjille ja kirjaamalla tietoturvaohjeiden noudattaminen työsopimukseen. Tietoturvaa voidaan yrityksessä lisätä myös esimerkiksi kannustamalla henkilöstöä positiivisesti siitä, että paperit on lukittu työpäivän päätteeksi laatikostoon. (Laaksonen ym. 2006, 250–259.)

#### **3.1 Tietoturvan määritelmä**

Tietoturvallisuus määritellään klassisesti tiedon arvoon perustuen. Tällöin se jaetaan kolmeen osatekijään, jotka ovat luottamuksellisuus (confidentiality), saatavuus (availability) ja eheys (integrity). Niin sanotussa laajennetussa määritelmässä osatekijöitä ovat lisäksi myös kiistämättömyys (non-repudiation) ja pääsynvalvonta (access control). (Hakala, Vainio & Vuorinen 2006, 4–5.)

Luottamuksellisuudella pyritään siihen, että tietoon eivät pääse käsiksi muut kuin ne henkilöt, joille on annettu etukäteen oikeus tiedon lukemiseen tai muokkaamiseen (Järvinen 2002, 22). Järvisen (2002, 24–25) mukaan luottamuksellisuus edellyttää todentamista (authentication). Sillä varmistetaan aitoudesta eli siitä, että esimerkiksi käyttäjä, laite tai tiedon alkuperä on juuri se, mitä pitääkin. Meistä jokainen tekee todentamista päivittäin sen kummemmin sitä ajattelematta. Todennamme kollegoita ja tuttavuuksia ulkomaailmaan, äänen tai jopa puhelinnumeron perusteella. Järjestelmissä käyttäjiä todennetaan käyttäjätunnuksen ja salasanan avulla. Näiden perusteella käyttäjälle voidaan antaa valtuutus (auktorisointi) tietojen käsittelyyn. (Järvinen 2002, 25.)

Saatavuudella halutaan varmistaa tietojärjestelmien toiminta niin, että tieto ja palvelut ovat saatavilla aina tarvittaessa. Esimerkiksi verkkopalvelussa tämä voi merkitä jopa joka päivä tarjottavaa ympärivuorokautista saatavuutta. Yrityksissä saattaa toimistojärjestelmien saatavuudeksi riittää normaali työaika, jolloin yöt sekä viikonloput voidaan hyödyntää tietojen varmistamiseen. (Järvinen 2002, 24.) Saatavuus on myös merkittävä tekijä yrityksen tietojärjestelmien tärkeysluokittelussa, sillä yrityksen jokaisella järjestelmällä se voi olla erilainen (Laaksonen ym. 2006, 159).

Tiedon eheydellä halutaan varmistaa, ettei mikään ulkopuolinen taho voi luvatta muuttaa tai poistaa tietoa. Esimerkkeinä voidaan mainita, että virukset rikkovat ohjelma- ja dokumenttitiedostojen eheyden tarttuessaan niihin tai että www-sivujen eheys rikotaan kun hakivistit lisäävät niihin luvatta omia iskulauseita tai merkkejä. Eheys voi rikkoutua myös tahattomasti. Näin voi käydä esimerkiksi levyille tulleen vika-alueen tai tiedonsiirrossa tapahtuneen virheen vuoksi. (Järvinen 2002, 22–23.) Yrityksen on huolehdittava, että muutokset tietojärjestelmässä olevaan tietoon ovat hallittuja ja vain auktorisoidun henkilön tai järjestelmien suorittamia. Liiketoiminnan kannalta on tärkeää, että järjestelmä on suunniteltu estämään tiedon tahaton muuntuminen. Tämä on myös lainsäädännön edellytys. (Laaksonen ym. 2006, 40.)

Kiistämättömyyden vaatimukset perustuvat yleensä lainsäädäntöön. Yrityksen on tarvittaessa todistettava kiistattomasti sekä tietojen luojan että käyttäjän henkilöllisyys. (Hakala ym. 2006, 86.) Kiistämättömyyden tarve tulee vastaan esimerkiksi sähköisessä kaupankäynnissä, jossa tilauksen tekeminen, vastaanottaminen ja toimittaminen tulee voida

todistaa sitovasti. Kauppiaan on kiistatilanteissa pystyttävä todistamaan, milloin tilattu tavara on ainakin lähetetty heiltä eteenpäin. Kiistämättömyys on saavutettavissa soveltamalla eheyden ja todennuksen periaatteita. Lisäksi kiistämättömyys edellyttää tapahtumien varustamista aikaleimoilla. Kyseisten leimojen on myös oltava luotettavia, joten aikatiedon lähde pitää tarvittaessa todentaa luotettavasti. (Järvinen 2002, 27–28.)

Pääsynvalvonnasta vastaavat käyttöjärjestelmä ja sovellus huolehtimalla, että vain todennetut henkilöt pääsevät käsiksi järjestelmässä oleviin tietoihin. Käytön seuranta (audit) on osa pääsynvalvontaa. Lokitiedostoja ylläpidetään järjestelmässä ja tarvittaessa niiden avulla nähdään, ketkä ovat kirjautuneet järjestelmään, käsitelleet tiedostoja tai käyttäneet ohjelmia. Näitä tietoja tarvitaan esimerkiksi tietoturvarikkomuksien selvittämiseen. (Järvinen 2002, 27.)

### **3.2 Tietoturvan osa-alueet**

Kun mietitään tietoturvaa, niin monille tulee ensin mieleen varmuuskopiointi tai hakkerit. Molemmat ovat osa tietoturvaa, mutta siihen liittyy paljon muutakin. Tietoturva kattaa tietojen saatavuuden ja oikeellisuuden. Se kattaa myös tietojen luottamuksellisuuden säilymisen käsittelyn, säilytyksen ja tiedonsiirron aikana. (Järvinen 2002, 21.) Tietoturvalla halutaan varmistaa, että tietokoneet ja ohjelmat toimivat tarkoitetulla tavalla ja ovat suojatut odotetuilta ja odottamattomilta riskeiltä. Lisäksi sillä halutaan varmistaa, että järjestelmän tiedot ovat käytettävissä aina tarvittaessa ja ainoastaan henkilöillä, jotka ovat oikeutettuja niitä käyttämään. (Ruohonen 2002, 2.)

Yrityksen näkökulmasta tietoturvan tulee suojata kaikki se tieto, joka on merkittävää yritykselle sen toiminnan jatkamiseksi. Näitä tietoja ovat esimerkiksi henkilöstöön, palkkoihin, tuotteisiin sekä myyntilukuihin liittyvät tiedot. (Järvinen 2002, 21.) Tietoa on suojattava yrityksessä kuten yrityksen omaisuutta, työntekijöitä tai brändiä (Järvinen 2002, 111).

Taulukko 3. Tietoturvan osa-alueet (Järvinen 2002, 112–113)

Tietoturvan osa-alue	Esimerkki
Hallinnollinen turvallisuus	Toiminnan organisointi
Henkilöturvallisuus	Työntekijöiden ohjeistus ja koulutus, heidän aiheuttamat tahattomat vahingot ja tahalliset vahingonteot
Käyttötoimintojen turvallisuus	Laitteiden huolto
Laitteistoturvallisuus	Varautuminen sähkökatkoksiin
Ohjelmistoturvallisuus	Lisenssit
Tietoaineistoturvallisuus	Luottamuksellisten tietojen turvallinen käsittely
Tietojenkäsittelyn turvallisuus	Laitteiden käyttö
Tietoliikenteen turvallisuus	Siirettävän tiedon salaaminen
Toimitilaturvallisuus	Kulunvalvonta
Yksityisyyden suoja	Henkilöiden tietojen suojaaminen

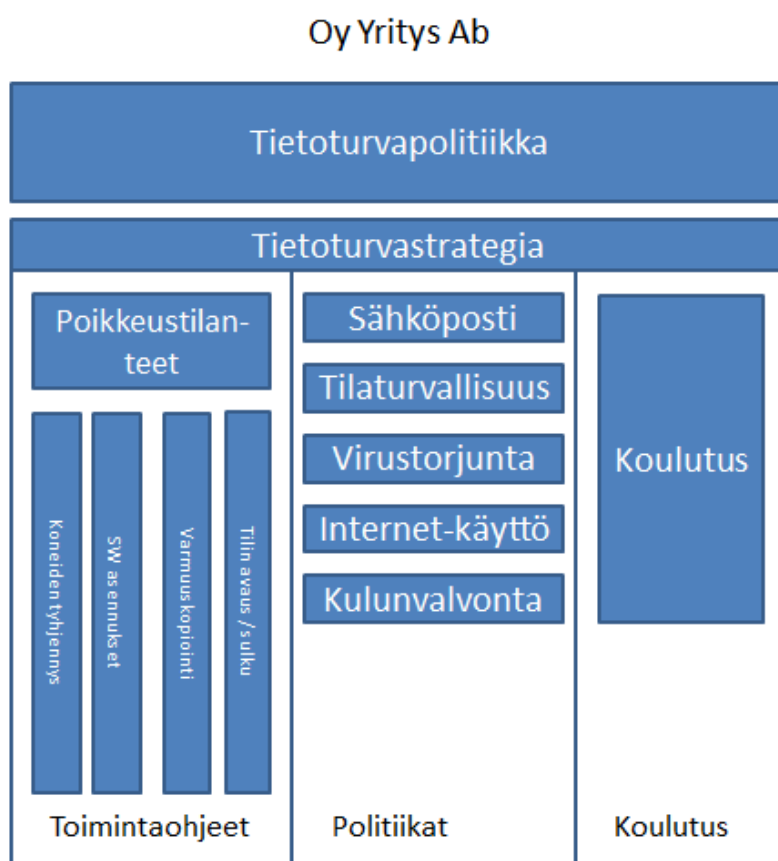
Tietoturva on käsitteenä melko laaja. Sen osa-alueita on listattu taulukkoon 3. Osa-alueita ovat esimerkiksi hallinnollinen turvallisuus, henkilöturvallisuus, toimitilaturvallisuus, tietojenkäsittelyn turvallisuus, tietoliikenteen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, käyttötoimintojen turvallisuus, tietoaineistoturvallisuus ja yksityisyyden suoja. (Järvinen 2002, 112–113.) Jokainen näistä osa-alueista tulee kartoittaa ja dokumentoida erikseen, jotta yrityksen omat tietoturvatavoitteet voidaan saavuttaa. Dokumenteista saadaan rakenteeltaan selkeämpiä, kun kokonaisuuden jaottelussa käytetään hyväksi osa-alueita. (Hakala ym. 2006, 10.)

### 3.3 Tietoturvapoliittikka

Järvinen (2002, 113) sanoo selkeästi, että ”Tietoturvapoliittikka on yrityksen tietoturvan kulmakivi”. Se on yrityksen johdon hyväksymä määritelmä yrityksen tietoturvan päämääristä, periaatteista sekä toteuttamistavasta. Kun yrityksen johto on sitoutunut poliittikkaan, niin se velvoittaa silloin myös kaikkia yrityksen työntekijöitä. (Järvinen 2002, 113.)

Usein tietoturvapoliittikka sekä tietoturvasuunnitelma käsitetään samaksi asiaksi. Ne ovat kuitenkin eri dokumentteja, sillä ne eroavat toisistaan tarkkuustasolla. Tietoturvapoliittikassa esitetään yleisluonteisia kuvauksia, kun taas tietoturvasuunnitelmassa määritellään kohdat yksityiskohtaisesti. Tietoturvapoliittikka on yleensä julkista tietoa, joten se voidaan julkaista vaikka yrityksen Internet-sivuilla. (Ruohonen 2002, 6.)

Kuten kuvioista 1 voi huomioda, tietoturvapoliittikka on yrityksen tietoturvaan liittyviä dokumenteista ylin. Sen lisäksi tarvitaan koko henkilöstöä koskevia ohjeita (politiikat) sekä yksityiskohtaisempia toimintaohjeita, jotka ovat tarkoitettu vain osalle henkilöstöstä. (Järvinen 2002, 116.)



Kuvio 1. Yrityksen tietoturvapoliittikka suhteessa muihin yrityksen tietoturvaan liittyviin dokumentteihin (Järvinen 2002, 116)

### 3.4 Tietoturvasuunnitelma

Tietoturvasuunnitelmaan kirjataan yksityiskohtaisesti työmenetelmät ja tekniset ratkaisut, joiden avulla saavutetaan käytössä oleviin tietojärjestelmiin haluttu tietoturvallisuuden taso. Suunnitelma laaditaan yleensä 2–5 vuodeksi ja se perustuu pidempiaikaisen tietoturvapoliittikan määrittelemiін suuntaviivoihin ja reunaehtoihin. Tietoturvasuunnitelma on syytä tarkistaa vuosittain sekä aina silloin, kun tietojärjestelmät tai työmenetelmät muuttuvat. (Hakala ym. 2006, 9.)

Tietoturvasuunnitelman laatimisen tavoitteena on varmistaa jokaisen tietojärjestelmän osan suojaaminen riittävän tehokkaasti. Riskianalyysiä, jossa on kartoitettu kaikki tietojärjestelmään kohdistuvat riskit ja niiden vaikutus, voidaan käyttää tietoturvasuunnitelman tavoitteiden määrittelemiseen. (Ruohonen 2002, 6–7.)

### 3.5 Uhkat ja riskien kartoitus

Ennen kuin yritykseen voidaan luoda tietoturvapoliittikka, on siellä määriteltävä, mitä halutaan turvata, ja mitkä ovat suurimmat tai tärkeimmät uhat. Yrityksessä täytyy myös olla selvillä omat ydinprosessit, sillä ne on tärkeää turvata. Riskikartoituksessa hahmotetaan ennakolta mahdolliset uhat, miten ne voivat toteutua sekä vahingosta tuleva kustannus. Ulkoistetut toiminnat aiheuttavat lisäriskejä, sillä suurin osa niistä on yrityksen suoran kontrollin tavoittamattomissa, vaikka yritys kantaakin vastuun niiden virheistä. (Järvinen 2002, 113–114.)

Usein yritykset keskittyvät ulkoisiin uhkiin ja hankkivat niiden torjuntaan kalliita suojaus- ja torjuntaohjelmia. Tietoturva on oikeastaan kuitenkin prosessi, jota ei yksinomaan ratkaista uusilla turvatuotehankinnoilla. Kallit suojaukset voivat loppujen lopuksi muodostaa uuden tietoturvariskin, mikäli henkilöstö ei osaa käyttää niitä kunnolla. (Järvinen 2002, 124.)

Yritykset eivät usein kiinnitä riittävää huomiota oman henkilökunnan muodostamaan tietoturvariskiin. Koska omat työntekijät tuntevat turvajärjestelmät, tietävät he myös, kuinka ne kierretään. Lisäksi oma henkilöstö tietää, mikä tieto on arvokasta ja missä sitä säilytetään. (Järvinen 2002, 124.) Irtisanomistilanteessa voi katkeroitunut IT-vastaava saada yritykselle paljon vahinkoa aikaiseksi kopioimalla mukaansa vaikka asiakasrekisterin sekä markkinointi- ja tuotekehityssuunnitelmat (Leidenius 2011, 18).

Mikäli tietoturvaohjeita ei noudateta yrityksessä, jää niiden hyöty hyvin vähäiseksi. Samalla se on riski yritykselle. Ei ole olemassa tekniikkaa, joka pystyy estämään käyttäjien oman, tietoturvaohjeista piittaamattoman toiminnan. Käyttäjä voi esimerkiksi luovuttaa uudelle työntekijälle oman käyttäjätunnuksensa ja salasansansa. Hän tarkoittaa hyvää auttaessaan esimerkiksi uutta kollegaa aloittamaan työt, mutta toiminta on täysin tieto-

turvaohjeiden vastaista. Toinen esimerkki on vaatia tietoturvan nimissä kohtuutto-  
muuksia vaikka salasanoihin, jolloin työntekijät alkavatkin kirjoittaa tunnuksiaan muisti-  
lapuille työpöydän laatikkoon. (Järvinen 2002, 122–123.)

### **3.6 Tietoturvastrategia**

Pääsääntöisesti tietoturvastrategia laaditaan, kun yrityksen riskit on kartoitettu ja halu-  
tun tietoturvan taso on määritelty. Strategiassa kuvataan, kuinka yrityksen tietoturvaa  
aiotaan kehittää, mitä tavoitteita turvallisuudelle asetetaan ja millä keinoilla haluttu tur-  
vataso saavutetaan. (Järvinen 2002, 115.)

Tietoturvastrategiasta löytyvät myös aikataulut sekä vastuuhenkilöt eri tehtäville. Teh-  
tävät voivat olla esimerkiksi henkilöstön tietoturvakoulutus tai uuden virustorjuntaoh-  
jelmiston valinta ja asennus. (Järvinen 2002, 115.)

### **3.7 Jatkuvuussuunnitelma**

Yrityksellä on oltava tietojärjestelmien pitkäaikaisten keskeytysten varalle jatkuvuus-  
suunnitelma (contingency plan), jossa kuvataan sekä tietotekniikan että tietoliikenneyh-  
teyksien varautuminen erilaisiin häiriötilanteisiin. Vakavimpia häiriötilanteita ovat esi-  
merkiksi maanjäristykset, tulipalot ja terroriteot. (Järvinen 2002, 114; Laaksonen ym.  
2006, 103.)

Jatkuvuussuunnitelman keskeinen osa on toipumissuunnitelma (recovery plan). Siinä  
määritellään yksityiskohtaisesti, kuinka yrityksen varajärjestelmät ja -yhteydet otetaan  
käyttöön. (Järvinen 2002, 114.) Toipumissuunnitelman tarkoitus on auttaa yrityksen  
tärkeitä liiketoimintaprosesseja toipumaan nopeasti erilaisista häiriötilanteista. (Laakso-  
nen ym. 2006, 227.)



### 3.8 Tietosuoja

Tietosuoja liittyy läheisesti tietoturvaan. Molemmissa on samoja piirteitä eikä niiden erottaminen toisistaan käytännössä ole aina helppoa. Tästä huolimatta ne ovat eri asioita. (Laaksonen ym. 2006, 17.)

Tietosuojalla suojataan erityisesti ihmisten tiedollista itsemääräämisoikeutta sekä yksityisyyttä. Tietoturva taas tarjoaa erilaisia keinoja tai toimintamalleja tietosuojan ylläpitämiseen; sillä ikään kuin rakennetaan muuri suojattavan tiedon ympärille. Jos muuri on heikko, on myös varsin vaikea suojata sellaista tietoa, jota tietosuojalla on tarkoitus suojata. (Laaksonen ym. 2006, 17.)

Tietosuojaa parannetaan tietojen luottamuksellisuuden varmistamisella, sillä sen avulla estetään ulkopuolisia tulkitsemasta keräämiään tietoja, kuten henkilötietoja tai henkilökohtaiseen toimintaan liittyviä tietoja. Myös ne tekniset ja toiminnalliset järjestelyt, joilla lisätään tietoturvaa, parantavat tietosuojaa. (Järvinen 2002, 21.)

### 3.9 Standardit

Tietoturvasuunnitteluun on olemassa useita kansainvälisiä ja kansallisia standardeja. Ne on tarkoitettu nimenomaan tiedon jäsentämiseen ja organisoimiseen. Standardeista on apua selkeän ja vertailukelpoisen dokumentaation tekemiselle, mutta niillä ei aseteta vaatimuksia tietoturvalle. (Hakala ym. 2006, 46.)

Merkittävin tietoturvallisuuden sisältöä ohjaava standardi on International Organization of Standardization –järjestön (ISO) yleinen tietoturvallisuuden menettelytapaohje, joka on nimeltään ISO/IEC 17799. Sen voidaan sanoa olevan yleisstandardi organisaation tietoturvallisuuden suunnittelussa, ylläpidossa ja kehittämisessä. Standardissa jaetaan tietoturvallisuus 11 klausuuliin (security control clause) ja näistä jokaisessa on 1–10 pääkategoriaa. Pääkohtina ovat esimerkiksi riskianalyysi ja riskien arviointi, turvallisuuspolitiikka, tietoturvallisuuden organisointi, omaisuuden hallinta, henkilöstöturvallisuus, pääsyn valvonta sekä toiminnan jatkuvuuden hallinta. (Hakala ym. 2006, 46–48.)

Toinen merkittävä standardi on ISO/IEC 27001. Se on pääasiassa tarkoitettu ohjenuoraksi tietoturvaluustoimintaan. Standardilla määritellään tietoturvaluuden hallinnan malli. Se sisältää esimerkiksi tietoturvaluuden hallintajärjestelmän perustamisen, käyttöönoton, käyttämisen, ylläpidon sekä valvonnan. Lisäksi mukana ovat myös katselmukset ja kehittäminen. (Hakala ym. 2006, 49.)

Tietoturvaluuteen liittyviä ISO-turvastandardeja on julkaistu paljon. Niistä merkittävimpiä ovat ISO/IEC 13335-1 ICT-turvallisuuden käsitteet ja mallit, ISO/IEC TR 13335-3 IT-turvallisuuden hallintatekniikat, ISO/IEC 11770-1 Salausavainten hallinta, ISO/IEC 15408-1 IT-turvallisuuden arviointikriteerien perusmalli ja ISO/IEC 18028-4 Etäkäytön turvaaminen. (Hakala ym. 2006, 51–52.)

Yrityksille on olemassa kansainväliset tietoturvastandardit korttimaksamiselle. Niillä määritellään tekniset minimivaatimukset turvallisuudelle, mikäli yritys haluaa käyttää kortteja maksuvälineenä. Kansainvälinen korttijärjestöjen perustama riippumaton PCI Security Standards Council -toimielin (Luottokunta 2010) on määritellyt kolme PCI-standardia:

- PCI DSS (Payment Card Industry Data Security Standard) on tietoturvastandardi sellaisille tietojärjestelmille ja prosesseille, jotka käsittelevät varmuuksia ja tapahtumia. Nämä minimivaatimukset ovat pakollisia kaikille yrityksille, jotka vastaanottavat, välittävät tai tallentavat korttimaksutapahtumia.
- PA-DSS (Payment Application Data Security Standard) on sertifiointistandardi korttimaksuja käsitteleville maksupäättejärjestelmille ja maksusovelluksille.
- PTS (PIN Transaction Security) on standardi PIN-tunnisteita käsitteleville järjestelmille. Standardi koskee erityisesti järjestelmien valmistajia ja toimittajia. Se sisältää neljä, erilaisille laitteille tarkoitettua sertifiointistandardia.

## 4 Tietoturvaan liittyvät termit auttavat asian ymmärtämistä

Kun puhutaan tietoturvasta tai tietosuojasta, joudutaan käyttämään termejä, jotka saattavat olla vieraita monille peruskäyttäjille. Jo lyhytkin kuvaus termin merkityksestä auttaa ymmärtämään sisältöä enemmän.

Taulukkoon 4 on kerätty taulukossa 1 esitetyt merkittävimmät tietoturvauhat sekä niihin liittyviä termejä. Vaikka moni tietoturvaan liittyvistä termeistä voi liittyä useampaan tietoturvaukkaan, niin tässä taulukossa jokainen esiteltävä termi on selvyuden vuoksi yhdistetty vain yhteen uhkaan termin päämerkityksen mukaan. (Taulukko 1.)

Taulukko 4. Merkittävimmät tietoturvauhat ja niihin liittyviä termejä

Merkittävimmät tietoturvauhat	Tietoturvaan liittyviä termejä
Tietojen urkkiminen työntekijöiden hyväuskoisuutta käyttäen	Henkilöllisyysvarkaus, social engineering, salasanojen kalastelu, pharming
Tietojen urkkiminen tai salakuuntelu teknisin keinoin	Huolimaton puhuminen, olanylisurffaus
Tietomurrot	Intruder, hakkeri, krakkeri, haktivisti
Roskaposti	Roskaposti
Tietoturvahyökkäykset	Bottiverkko, botti, hyökkäys, sanakirjahyökkäys
Virukset, troijalaiset, muut haittakoodit	Haittaohjelma, mato, takaovi, troijalainen, virus
Työntekijöiden tietämättömyys tai huolimattomuus	Näytönsäästäjä
Laitteistovika	Palomuri
Ohjelmistovika	Salaus
Sisäisten tietoturvakäytäntöjen puuttuminen	Varjo-IT, Bring your own computer
Fyysinen onnettomuus (tulipalo, vesivahinko, jne.)	
Laitteen katoaminen, varkaus	
Mainos- ja vakoiluohjelmat	

### 4.1 Hakkerointi- ja urkkimistapoja

**Henkilöllisyysvarkaus** (identity theft) on ollut yksi nopeimmin kasvaneista rikollisuuden aloista. Federal Trade Commission (FTC) on selvittänyt, että Yhdysvalloissa 8,4 miljoonaa ihmistä joutui henkilöllisyysvarkauden uhriksi vuonna 2007. Taulukkoon 5 on kerätty tutkimuksen tuloksia. Kyseisen tutkimuksen mukaan neljäsosa henkilöllisyysvarkauden uhriksi joutuneista on tuntenut tekijän. Yli kolmasosassa tutkimuksen tapauksista tekijä on ollut perheenjäsen tai sukulainen. Lisäksi joka toinen tutkimuksessa mukana olleista uhreista ei tiedä, kuinka heidän tietojaan on varastettu. Näiden tulosten perusteella voidaan päätellä, että kuka tahansa voi milloin tahansa joutua henkilöllisyys-

varkauden uhriksi. Henkilöllisyysvarkauksissa varkaita kiinnostavat erityisesti nimi- ja osoitetiedot, luottokorttitiedot, pankkitiedot, syntymäaika, sosiaaliturvatunnus sekä työnantajan tiedot. (Arata 2011, 10–11.)

Taulukko 5. Federal Trade Commission (FTC) tutkimustuloksia (Arata 2011, 11)

<b>Henkilöllisyysvarkaus</b>	10 %	20 %	30 %	40 %	50 %	60 %	70 %	80 %	90 %	100 %
Uhri on tuntenut tekijän	■	■	■	■	■	■	■	■	■	■
Tekijä on ollut perheenjäsen tai sukulainen	■	■	■	■	■	■	■	■	■	■
Uhri ei tiedä, kuinka tiedot on varastettu	■	■	■	■	■	■	■	■	■	■

**Social engineering** on toimintaa, jonka tavoitteena on kiertää teknisiä suojauksia psykologisin keinoin. Tietoja urkitaan käyttäjältä mitä erikoisimmilla keinoilla. Tavoitteena on saada tietoja verkon suojauksista, käyttäjätunnuksista ja salasanoista. Ei ole ennenkuulumatonta, että lyöttäydytään vaikka pubissa uhrin seuraan ja juomatarjoilun ohessa selvittelään yrityksen turvajärjestelyjä. Isojen yritysten työntekijöiltä saatetaan yrittää urkkimalla selvittää erilaisia käyttäjätunnuksia ja salasanoja esimerkiksi esittäytymällä yrityksen mikrotukihenkilönä. (Järvinen 2002, 307–308.)

**Salasanojen kalastelu** (phishing) on yksi social engineering -toiminnan muoto. Siinä kalastellaan sähköpostiviestien, pikaviestiohjelmien ja mainospalkkien avulla käyttäjiä valeverkkosivuille antamaan identiteetti- ja maksuvälinetietoja käytettäväksi laittomuuksiin. **Pharming**-huijaus on vielä vaikeammin havaittava salasanojen kalastelukeino. Siinä kuluttaja ohjataan automaattisesti valesivustolle, joka näyttää aivan alkuperäiseltä pankin tai kauppiaan sivustolta. (Symantec Corporation. 2006.)

Julkisuuteen on tullut useita tapauksia, esimerkiksi pankkialalta, joissa yrityksen nimissä on lähetetty henkilöille sähköpostiviestejä, pyytäen heidän kirjautumistietoja. Samoin julkisuudessa on esitelty myös tapauksia, joissa pankin nettisivujen näköisversioiden kautta on yritetty saada henkilöiden käyttäjätunnuksia rikollisten käsiin. Yksi uusimmista kalasteluyrityksistä tuli julki 29.9.2011, kun monet Nordean asiakkaat saivat sähköpostiviestin, joka osoittautui salasanojen kalasteluviestiksi. Nopealla lukaisulla viesti oli helppo uskoa Nordeasta lähetetyksi ilmoitukseksi tilin tilapäisestä estämisestä. Viestin

sisältöä tarkemmin katsomalla kalastelun pystyi päättelemään esimerkiksi kielioppivirheellisestä tekstistä sekä myös epämääräisestä sisällöstä. Viestissä mukana olleet linkit olivat nimetty houkuttelevasti, joten riski niiden käyttämiseen oli suuri. (YLE Etelä-Karjala, 2011).

**Huolimaton puhuminen** (loose talk) voi olla esimerkiksi kännykkäkeskustelu julkisessa kulkuvälineessä. Henkilötietojen, yritystietojen ym. vastaavien arkaluontoisten tietojen puhuminen saattaa kiinnostaa vieressä istuvaa kilpailevan yrityksen edustajaa erittäin paljon. (Arata 2010, 112.)

**Olanylisurffaus tai olan yli kurkkiminen** (shoulder surfing) on toimintaa, jonka avulla hankitaan tietoa toisesta henkilöstä kurkkimalla olan yli. Sitä tapahtuu esimerkiksi julkisissa kulkuvälineissä, kahviloissa ja lentokentillä. Kurkkimista voi tehdä kauempaa esimerkiksi zoomaamalla kameran linssin läpi. (Arata 2010, 111.) Olanylisurffaajat ovat kiinnostuneita käyttäjätunnuksista, pankkitunnuksista, salasanoista sekä työnantajan tiedoista.

## 4.2 Tietomurtojen tekijöitä

**Intruder** on termi, jota käytetään tietojärjestelmään tunkeutuvasta henkilöstä. Tunkeutujan päämäärästä riippuen, hänet voidaan tarkemmin määritellä esimerkiksi hakkeriksi, krakkeriksi tai haktivistiksi. (Järvinen 2002, 445.)

**Hakkerit** (hacker) ovat tietomurtautujia, jotka murtautuvat luvatta tietojärjestelmiin. Tärkeimpinä motiiveina heillä on yleensä uteliaisuus, kokeilunhalu, julkisuus tai arvostus. He pyrkivät toimimaan niin, että heidän käynneistään ei jää jälkiä. Sanalla on alun perin tarkoitettu innokasta ja lahjakasta tietokoneharrastajaa. (Järvinen 2002, 294.)

Henkilöitä, jotka murtautuvat tietojärjestelmiin luvatta ja tekevät siellä vahinkoa tarkoituksella kutsutaan **krakkereiksi** (cracker). He jättävät jälkiä käynnistään esimerkiksi sotkemalla www-sivujen sisältöä. Mikäli krakkeri-iskulla on aatteellinen motiivi, käytetään termiä **haktivisti** (hacktivist). Esimerkiksi turkistarhauksen vastustajat voivat

osoittaa mieltään sotkemalla www-sivuja tai ylikuormittamalla nettipalveluita. (Järvinen 2002, 294–295.)

### 4.3 Muita tärkeitä tietoturvaan liittyviä termejä

**Roskaposti** (spam, junk mail) on yhteisnimitys kaikille käyttäjien sähköposteja kuormittaville mainosposteilta (Järvinen 2002, 449). Niiden jakelulistoilta on vaikea päästä pois, mikäli on sinne kerran joutunut. Maailmanlaajuisesti toimivan Unileverin sähköpostiosoitteisiin lähetettiin elokuussa 2011 yhteensä 35 485 374 sähköpostiviestiä. Niistä 12 miljoonaa (34 %) todettiin virustarkistuksessa roskapostiksi. Roskapostiviestien määrät olivat elokuun 2011 aikana hienoisessa laskussa, mutta siitä huolimatta ilman roskapostitarkistusta jokainen Unileverin sähköpostiosoitteen omistava työntekijä ympäri maailman olisi saanut ylimääräiset 118 roskapostiviestiä. (Vikström, M. 12.10.2011.)

**Bottiverkko** (botnet) on jopa sadoista tuhansista uhritietokoneista omistajien tietämättä rakennettu verkosto, jota hyökkääjä hallinnoi. Kaikissa näissä yksittäisissä koneissa on **botti** eli haittaohjelma (web-robot), jonka avulla hyökkääjä pääsee hallitsemaan konetta ja muuttamaan sen ”zombie-tietokoneeksi”. Rikolliset käyttävät näitä verkkoja esimerkiksi tietoliikenteen häirintään, virusten levittämiseen ja roskapostin lähettämiseen. Botin saastuttaman koneen toiminta hidastuu, näytölle saattaa ilmaantua outoja viestejä tai se voi jopa kaatua odottamatta. Botit leviävät Internetin kautta ja kun suojaamaton tietokone löytyy, tartuttaa botti sen ja raportoi siitä botti-isännälle, jään odottamaan sille annettavaa tehtävää. (Symantec Corporation 2011.)

**Hyökkäys** (attack) on suunniteltu teko yksittäistä konetta, tietoverkkoa tai tietoliikenteen tietoturvaa kohtaan. Yleensä tavoitteena on murtautua kohteeseen ja estää sen toiminta. (Järvinen 2002, 445.)

**Sanakirjahyökkäys** (dictionary attack) on menetelmä, jossa käyttäjän salasana yritetään arvata sanalista käyttämällä. Tekemiseen valjastetaan ohjelma, joten sanalistat voivat olla käsittämättömän pitkiä. (Järvinen 2002, 449.)

**Haittaohjelma** (malicious code, malware) on yleisnimitys kaikille niille ohjelmille tai ohjelmien osille, joiden avulla on tarkoitus vahingoittaa kohdejärjestelmää tai ohittaa tietoturvajärjestelyitä (Järvinen 2002, 445). Haittaohjelmia ovat esimerkiksi virukset, madot, troijan hevoseset sekä erilaiset vakoiluohjelmat. Haittaohjelmia on huomattavasti helpompi välttää kuin poistaa niitä tietokoneelta. Käyttäjä voi välttää niitä huolehtimalla esimerkiksi siitä, että pitää virustorjuntaohjelman päivitettyinä ja lataa tiedostoja vain luotettavista lähteistä. (Phelps 2010.)

**Mato** (worm) on haittaohjelma, joka ei tarvitse levitäkseen isäntätiedostoa, kuten virus, vaan se leviää itsenäisesti. Se ei myöskään yleensä tuhoa tiedostoja, mutta voi kuormittaa muistia. (Järvinen 2002, 447.) F-Securen tutkimusjohtaja Mikko Hyppönen on sanonut haastattelussa, että 10 vuotta sitten madot levisivät jokaiseen mahdolliseen koneeseen ja verkkoon, mutta nykyään ne odottavat botnetin ylläpitäjän lupaa leviämiseen (Lehto 2011, 41).

**Takaovi** (back door) on tietokoneohjelma, joka avaa hakkerille pääsyn tietokoneeseen lähes täysillä käyttäjävaltuuksilla. Ohjelma voi raportoida kaikki koneella tehtävät toimenpiteet suoraan hakkerille, mukaan lukien käytetyt käyttäjätunnukset ja salasanat. Sen avulla voi käytännössä ottaa koko koneen haltuun. Takaovia voidaan kutsua myös **troijalaisiksi**, sillä ne on usein naamioitu toiseksi ohjelmaksi, esimerkiksi sähköpostin liitteenä lähetetyksi pilailuohjelmaksi. Takaovien kohteena on tarkoituksellisesti joku yritys tai käyttäjä. (Järvinen 2002, 256, 284.)

**Virus** on tietokoneohjelma, joka leviää tietokoneesta toiseen, saastuttaen ne monella eri tavalla (Järvinen 2002, 249). Ensimmäinen tunnettu tietokonevirus oli vuonna 1986 luotu virus nimeltä Brain. Ohjelmavirusten merkitys tietoturvariskinä on vähentynyt merkittävästi 2000-luvulla. (Pitkänen 2011.)

**Näytönsäästäjä** (screen saver) aktivoituu automaattisesti tietokoneen ruudulle, kun kone jää hetkeksi käyttämättä. Se estää ulkopuolisia pääsemästä käyttämään laitetta tai näkemään siellä olevia tietoja. (Järvinen 2002, 447.)

**Palomuri** (firewall) on suoja sisäverkon tai tietokoneen ja julkisen Internetin välissä. Muurina voi toimia reititin, erillinen laite tai ohjelma. Sen avulla halutaan estää ylimääräisten IP-pakettien pääsy järjestelmään. (Ruohonen 2002, 64.) Utm-palomuureilla (utm = unified threat management) saadaan rakennettua erilaisia molempiin suuntiin toimivia suojakerroksia yrityksen ja julkisen Internetin väliin. Näitä kerroksia ovat esimerkiksi hyökkäysten torjunta, virustorjunta, salakirjoitetut etäyhteydet, roskapostin suodatus, asiattoman nettisurffauksen estäminen ja ei-toivottujen sovellusten käytön esto. Lisäksi sen avulla voidaan rajata käyttöoikeuksia vaikka rajoittamalla esimerkiksi Facebookin käyttöä niin, että sallitaan sen käyttö, mutta kielletään siellä olevat pelit. (Kotilainen 2011, 49–51.)

**Salaus** (encryption) on tiedoston, sähköpostiviestin tai muun tiedon koodaamista muotoon, joka voidaan purkaa ymmärrettävään muotoon ainoastaan oikean salausmenetelmän ja avaimen avulla (Järvinen 2002, 449).

#### 4.4 Uusia trendejä, joilla on vaikutusta yrityksen tietoturvaan

Uusi merkittävä ilmiö, joka liittyy tietoturvaan, on **varjo-IT**. Ilmiöön kuuluvat kaikki ne ohjelmistot ja tietojärjestelmät, jotka käyttäjät ovat ottaneet työkäyttöön ilman työnantajansa virallisen IT-organisaation hyväksyntää. (Tuurila 2011, 45.)

Vielä joitakin vuosia sitten yrityksistä löytyi viimeisin teknologia, mutta nykyään työpaikan välineet ovat usein vanhoja ja hitaita. Sen sijaan monilta työntekijöiltä löytyy uusinta viestintäteknologiaa kotoa. Tästä voi seurata, että työntekijät turvautuvat kiellettyihin keinoihin, ja käyttävät työnantajan kielloista huolimatta omia laitteitaan, saadakseen tehdä töitä tehokkailla välineillä ja ohjelmilla. (Pulkinen 2011, B8.)

Koska virallinen IT-organisaatio ei ole hyväksynyt näitä ohjelmistoja tai tietojärjestelmiä yrityksen käyttöön, ei niille myöskään anneta tukea. Ongelmatilanteissa työntekijät turvautuvat organisoimattomaan ja piilossa olevaan, omaan ongelmanratkaisuyksikköön, jota kutsutaan **varjo-IT -osastoksi**. (Tuurila 2011, 45.)



Käyttäjien mahdollisuus käyttää mieleisiään sovelluksia ja järjestelmiä voi tehostaa sekä työn tekemistä että uusien ideoiden luomista, mutta varjopuolena tästä seuraa kasvavat tietoturvariskit (Tuurila 2011, 45). Käyttäjät eivät ehkä muista tai osaa huolehtia riittävästä tietojen suojaamisesta tai uskovat kaiken olevan kunnossa ilman, että heidän tarvitsee tehdä asialle mitään.

Uusi trendi on myös lisääntynyt älypuhelimien käyttö yrityksen tietojen käsittelyyn. Monissa yrityksissä älypuhelimiin ja kännyköihin liittyvät asiat hoidetaan IT-osastolla. Forrester Research on tehnyt kyselyn 1051 IT managerille Pohjois-Amerikassa ja Euroopassa. Kuten taulukosta 6 voi nähdä, kyselyn perusteella kolmannes yrityksistä ei tue henkilökohtaisia älypuhelimia ja kännyköitä, tai henkilöstöä on jopa kielletty käyttämästä niitä työasioiden hoitamiseen. Ainoastaan 16 % vastanneista kertoi yrityksen tukevan kaikkia henkilökohtaisia laitteita ja 14 % sanoi tukevansa tiettyjä malleja. (Hamblen 2011.) Mikäli yritys ei tue henkilökohtaisia älypuhelimia, mutta niitä kuitenkin käytetään yrityksen asioiden hoitamiseen, aiheutetaan merkittävä tietoturvariski ja edesautetaan varjo-IT -osaston muodostumista.

Taulukko 6. Forrester Researchin tutkimus henkilökohtaisten laitteiden tukemisesta yrityksessä (Hamblen 2011)

	10%	20%	30%	40%	50%
Työntekijöitä on kielletty käyttämästä omia laitteita		10%			
Yrityksessä ei tueta henkilökohtaisia laitteita				26%	
Yritys tukee ainoastaan tiettyjä henkilökohtaisissa käytössä olevia malleja			14%		
Yritys tukee kaikkia henkilökohtaisissa käytössä olevia malleja			16%		
Yrityksestä ei vastattu kysymykseen					34%

Uutena trendinä on myös toimintamalli, jossa vastuu tuottavaan työskentelyyn soveltuvan laitteiston valinnasta siirretään yritykseltä henkilöstölle. Tämä ”**bring your own computer** – tuo oma työasemasi” kiinnostaa esimerkiksi Yhdysvalloissa nuoria, lupaa-via työntekijöitä, sillä heille työnantajan valinnassa työvälineet on merkittävä valintakriteeri. (Toivonen 2010.) Omien työasemien liittäminen yrityksen ympäristöön asettaa

yrittäjien tietoturvalle uusia haasteita, joihin yrityksen IT:n on kuitenkin löydettävä toimivat ratkaisut. Yksi ratkaisu voi olla päätös siirtää sovellukset käyttöliittymineen verkkoon hoidettavaksi pilvipalveluna eli ns. **cloud computing**. Siirrossa on kuitenkin omat riskinsä, joita yrityksen on syytä miettiä huolella jo ennen kuin yrityksen tietoja päätetään siirtää pilvipalveluihin. Riskejä on paljon esimerkiksi palveluiden hankinnassa, käytössä sekä aikanaan tapahtuvassa palveluiden lopetuksessa. (Siltala 2010.)

## **5 Unileverin tietoturvakampanja**

Opinnäytetyön produkti on työnantajan toimeksianto. Työskentelen Unilever Finland Oy:ssä Information Security Officerina (ISO). Yrityksessä päävastuu eri maiden tietoturvan ylläpitämisestä on globaalilla organisaatiolla, mutta sen lisäksi joka maassa tai alueella toimii paikallinen ISO sekä Risk Manager. Toimin globaalin tietoturvaorganisaation Pohjoismaiden kontaktihenkilönä kaikissa tietoturvaan liittyvissä asioissa.

### **5.1 Yrityksen esittely**

Unilever Finland Oy on osa pohjoismaista myynti- ja markkinointiorganisaatiota. Se on myös osa kansainvälistä Unilever-yhtymää. Yritys on yksi maailman johtavista päivittäistavaroiden tuottajista. Sillä on toimintaa yli sadassa maassa ja sen tuotteita myydään yli 180 maassa. (Unilever Finland Oy 2011a; Unilever Finland Oy 2011b.)

Yrityksen liikevaihto Suomessa vuonna 2010 oli 213,6 miljoonaa euroa ja henkilöstöä oli keskimäärin 130 henkilöä. Suomen liiketoimintayksikköön kuuluvat puhdistus- ja hygieniatuotteet, elintarvikkeet sekä jäätelöt. Tuotemerkeistä tunnetuimpia ovat OMO, Bio Luvil, Pepsodent, Dove, Rexona, Flora, Becel, Lipton, KNORR, Magnum, Carte d'Or sekä Solero. (Unilever Finland Oy 2010.)

### **5.2 Information Security Campaign 2011 -kampanjan esittely**

Nordic Information Security Campaign 2011 (ISC2011) on yrityksen henkilöstölle suunnattu tietoturva-aiheinen muistutuskampanja. Se järjestetään Unileverin kontto-reissa Suomessa, Ruotsissa, Tanskassa sekä Norjassa. Kampanjan tavoitteena on muistuttaa yrityksen toimihenkilöitä ja edustajia, vuoden viimeisten viikkojen aikana, erilaisista tietoturvaan liittyvistä riskeistä. Samalla halutaan lisätä käyttäjien tietämystä yrityksen Intranet-sivuilla olevasta tietoturva-sivustosta. (Liite 1.)

Kampanjan ulkopuolelle jää tehtäillä työskentelevä henkilöstö, sillä heille tietoturvasta järjestetään erillinen koulutus/kertaus myöhemmin. Heidän työtehtäviin kuuluu ainoastaan rajoitettu pääsy yrityksen verkkoon. Heillä ei ole henkilökohtaisessa käytössä yrityksen laitteita, kuten tietokonetta tai kännykkää.

Yritykseen haluttiin suunnitelma ja toteutus tietoturva-aiheisesta muistutuskampanjasta, jossa käytetään hyväksi yrityksen globaalia tietoturvasivustoa. Kampanjalla halutaan korostaa henkilöstölle, että tietoturvaan liittyvää tietoa on paljon ja helposti heidän saatavilla. Yrityksen toinen toivomus oli, että aineistossa kerrotaan sivuston osoite eri yhteyksissä, jotta se tulisi käyttäjille tutuksi ja jäisi heidän mieleen.

Kampanjamateriaaliin haluttiin käyttää yrityksen omia värikkäitä esityspohjia. Taustavärit on kerätty yrityksen toivomuksesta yrityksen omasta värimaailmasta. Eri taustavärejä on hyödynnetty aihealueiden toisistaan erottamiseen. Esimerkiksi tiedon hallintaan liittyvät aiheet ovat keltaisella taustalla ja oman tietokoneen käyttöön liittyvät aiheet ovat sinisellä taustalla. Esityksen tekstissä on käytetty värejä huomion herättämiseen esimerkiksi korostamalla punaisella värillä asioita, joita ei pitäisi tehdä. (Liite 3; Liite 4.)

Kampanjaan on suunniteltu laaja, yli 80 sivua sisältävä PowerPoint-esitys. Tarkoitus on, että yhdestä materiaalista löytyy yritykselle keskeisimmät tietoturvaan liittyvät asiat. Esityksestä voidaan valita halutut osuudet esitettäväksi eri tilaisuuksissa, kuten esimerkiksi eri osastojen omissa viikko- tai kuukausipalaverissa. Esitysten toivotaan avaavan keskustelua ajankohtaisista tietoturvaan liittyvistä asioista. (Liite 3.)

Kampanja on tarkoitus käynnistää viikolla 46 eli marraskuun puolivälissä. Jouluvuikoilla kampanja on tauolla, mutta sitä jatketaan vielä loppiaisen jälkeen muutaman viikon ajan. (Liite 2.) Kampanjan aikana henkilöstölle lähetetään muistutuksia tietoturvasta sekä linkkejä yrityksen tietoturvasivuille. Lisäksi toimistojen näyttötauluilla näytetään viikoittain vaihtuvia muistutusviestejä esimerkiksi salasanojen vaihtamisesta, huolettomasta puhumisesta ja tietojen varmistamisesta (Liite 4).

Kampanjan lopussa käyttäjiä pyydetään tekemään yrityksen tietoturva-aineistosta kerätty kysely. Englanninkielinen kysely on globaalin tietoturvaorganisaation suunnittelema ja sitä ei ole aiemmin käytetty Pohjoismaissa. Kyselyyn liittyy kertaosioita, joissa käyttäjille palautellaan mieleen yrityksen tietoturvasääntöjä. Kysely järjestetään yrityksen nettipohjaisen koulutusjärjestelmän kautta. Järjestelmästä esimiehet näkevät, ovatko heidän alaiset vastanneet kyselyyn. Lisäksi järjestelmästä on mahdollista saada tietoja esimerkiksi osallistujamäärästä.

### 5.3 Kampanjan suunnittelu

Tietoturvakampanjan alustava suunnittelu alkoi syksyllä 2010. Yrityksessä haluttiin järjestää pohjoismainen tietoturvakampanja, jolla muistutettaisiin käyttäjiä tietoturvasta sekä yrityksen globaalista tietoturvasivustosta.

Kampanjaa ei haluttu tehdä ennen kesälomia, kesälomakauden aikana eikä heti kesälomakauden jälkeen. Aikataulu muodostui näin luontevasti loppusyksyyn. Kampanja jakautuu usealle viikolle. Joululomien sekä poikkeuksellisten työaikataulujen vuoksi joulun ja loppiaisen välisenä aikana halutaan pitää taukoa kampanjasta. Tauon jälkeen kampanja jatkuu yrityksen tietoturvasivustoista muistuttamisella. Kampanjan lopussa on tavoitteena saada henkilöstö osallistumaan tietoturvakyselyyn.

Taulukko 7. ISC2011-kampanjan valmisteluun käytetty aika

		10 h	20 h	30 h	40 h	50 h	60 h
Palaverit			13 tuntia				
Valmistelut							59 tuntia
Ylimääräinen lisätyö yrityksen uudistettuihin sivustoihin tutustumisesta		10 tuntia					

Kuten taulukosta 7 käy ilmi, niin ISC2011-kampanjan tekemiseen kului yhteensä 82 tuntia. Kampanjan valmisteluun oli mahdollista käyttää maksimissaan 100 työtuntia. Merkittävä osa ajasta (59 tuntia) tarvittiin itse aineiston eli kuvaesityksen valmisteluun, sillä työ oli hidasta. Yllättävä hidaste valmisteluun tuli siitä, kun yrityksen tietotur-

vasivustot uusittiin kesken projektin. Muutoksen vuoksi sivustoon piti tutustua uudestaan. Myös kaikki osoitteet, jotka oli jo kerätty esitykseen, piti päivittää vastaamaan uutta sivustoa. Kaikkiaan tämä muutos aiheutti 10 lisätuntia. Suunnittelu- ja seurantapalavereita kampanjan tiimoilta pidettiin noin 13 tuntia. Palavereissa suunniteltiin esityksen sisältöä ja seurattiin kampanjan valmistumista.

#### **5.4 Kampanjan toteutus**

Tietoturvakampanjan toteutusta varten haluttiin laaja esitysmateriaali (Liite 3). Se laitetaan yrityksen Intranet-sivuille henkilöstön saataville. Lisäksi haluttiin lyhyitä esityksiä viikoittain vaihtuviksi muistutusaineistoiksi toimistojen näyttötauluille (Liite 4). Esitysmateriaali ja näyttötauluilla esitettävät muistutusviestit ovat ulkoasultaan toistensa kaltaisia.

Käyttäjiä on tarkoitus lähestyä myös sähköpostiviesteillä, joissa on suora linkki yrityksen tietoturvasivuille sekä linkki esitysmateriaaliin. Suorilla linkeillä käyttäjät pääsevät nopeasti tiedon lähteelle etsimään lisätietoja. Samaa materiaalia jaetaan myös esimiehille, jotta he voivat kerätä haluamansa osuudet käytettäväksi viikko- tai kuukausipalaverissaan.

#### **5.5 Kustannukset**

Kampanjan toteutusta varten ei varattu erillistä budjettia. Sen tekemiseen sai käyttää normaalia työaika, sillä työ soveltui sellaisenaan Information Security Officerin työtehtäviin. Matkakustannuksilta vältyttiin, sillä palaverit pidettiin muiden matkustusta vaatineiden palaverien yhteydessä tai puhelinneuvotteluina.

Kampanjan toteuttamiseen soveltuvat yrityksen normaalit viestintävälineet ja viestintäkanavat, joten myöskään niihin ei tarvittu rahoitusta. Merkittävä valintakriteeri käytettävien viestintävälineiden valinnassa oli kustannustehokkuus, sillä kampanja haluttiin toteuttaa ilman lisäkustannuksia.

## 5.6 Kampanjan tulosten seuranta ja ideoita jatkokehitystä varten

Kampanja ajoittuu loppusyksyyn (Liite 2). Käyttäjäpalautetta on saatavilla aikaisintaan marraskuussa 2011, kun kampanja on käynnistynyt. Lokakuussa 2011 aineistolla tehtiin käyttäjättestaus. Lisäksi aineisto on esitelty esimiehille. Käyttäjätestauksen sekä esimiehiltä saadun palautteen perusteella esitysmateriaaliin on onnistuttu keräämään yrityksen kannalta oleelliset tietoturva-aiheet. Lisäksi aineiston ulkoasu sai kiitosta etenkin näyttötauluilla esitettävien muistutusviestien osalta (Liite 4). Myös kampanjan ajoitus sekä aikataulu soveltuvat esimiesten palautteen perusteella hyvin yrityksen muuhun henkilöstölle suunniteltuun viestintään.

Kansainväliseen tietoturvamateriaaliin tullaan esittämään kampanjan jälkeen parannusehdotuksia. Vaikka materiaali on valmistettu keskitetysti ja sitä käytetään samanaikaisesti useassa maassa, niin siihen tulisi saada mukaan jotain paikallista, sillä muuten se koetaan käyttäjien keskuudessa liian etäiseksi. Paikallisuus voi olla esimerkiksi sitä, että teksti käännetään kohdemaan omalle kielelle tai tekstistä poistetaan osuudet, jotka eivät koske kyseistä maata tai henkilöstöä. Esimerkiksi henkilö- ja vieraskorttikäytännöt vaihtelevat eri maissa, joten niihin liittyvä ohjeisto tulisi olla räätälöity maakohtaisesti.

Jotta tietoturvatietämys pysyisi yrityksen henkilöstön keskuudessa vähintään perustasolla, niin yrityksen johdolle tullaan kampanjan jälkeen esittämään muutamia kehitysehdotuksia. Yrityksessä voitaisiin miettiä esimerkiksi säännöllisempää tietoturva-asioista muistuttamista ja jonkinlaisen lyhyen koulutustilaisuuden tai luennoitsijavierailun järjestämistä. Lisäksi yrityksessä voitaisiin kokeilla säännöllisiä paikallisia tietoturvauutisia toimistojen näyttötauluilla. Ne voisivat toimia samalla myös muistutuksina tietoturvan tärkeydestä. Käyttäjien muistia voisi virkistää myös päivittämällä olemassa olevia tietoturvaan liittyviä ohjeita ja jakamalla niitä käyttäjille joko sähköpostilla tai paperiversioina. Näiden toimenpiteiden avulla henkilöstön tietoturvaosaamista saataisiin ylläpidettyä ja sitä kautta osaltaan varmistettaisiin yrityksen kilpailukyky myös tulevaisuudessa.

Tammikuussa 2012 järjestetään henkilöstölle mahdollisuus käydä tekemässä tietoturvakertaus nettipohjaisen koulutusjärjestelmän kautta. Sen kautta saadaan selville kävijöiden kokonaismäärä, jota verrataan henkilöstömäärään. Tarkempi tuloksen analysointi käydään läpi yrityksen tietoturvasta vastaavan henkilöstön kesken. Tulos tullaan raportoimaan yrityksen johdolle.



## 6 Yhteenveto

Opinnäytetyön tavoitteena oli selvittää, mitä on yrityksen tietoturva, miettiä erilaisia mahdollisuuksia tietoturvasta muistuttamiselle, löytää yritykselle keinoja kehittää henkilöstön tietoturvaosaamista sekä kerätä monipuolinen esitysmateriaali käytettäväksi erilaisissa yrityksen tilaisuuksissa.

Ensinnäkin opinnäytetyöllä haluttiin löytää yrityksen keskeisimmät tietoturvan osa-alueet. Yrityksen näkökulmasta tietoturvan tulee suojata kaikki se tieto, joka on merkittävää yritykselle sen toiminnan jatkamiseksi. Yritykselle tärkeitä tietoja ovat esimerkiksi henkilöstöön, palkkoihin, tuotteisiin sekä myyntilukuihin liittyvät tiedot. Yrityksen oman tietoturvatavoitteiden saavuttamiseksi kaikki tietoturvan osa-alueet tulee kartoittaa ja dokumentoida asiallisesti. Näitä osa-alueita ovat esimerkiksi hallinnollinen turvallisuus, henkilöturvallisuus, toimitilaturvallisuus, tietojenkäsittelyn turvallisuus, tietoliikenteen turvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, käyttötoimintojen turvallisuus, tietoaaineistoturvallisuus sekä yksityisyyden suoja.

Toisella tutkimuskysymyksellä haluttiin selvittää, kuinka saataisiin heräteltyä käyttäjien mielenkiinto tietoturva-asioihin. Monen vuoden käytännön kokemuksen perusteella olen huomannut, että käyttäjiä on vaikea motivoida oman työnsä ohella etsimään tietoa tietoturvasta ja sen jälkeen vielä lukemaan sitä ajatuksella läpi. Aihe on tärkeä, mutta se on myös helppo siirtää etsittäväksi ja luettavaksi myöhemmin. Käytännön esimerkit auttavat jokaista suhteuttamaan asiat omaan ympäristöönsä, mutta kuinka ne voi saada käyttäjälle tiedoksi, mikäli hän ei ehdi lukea materiaalia? Opinnäytetyön produktissa ongelma ratkaistiin sillä, että yrityksen tietoturva-aineistosta kerättiin Pohjoismaille tärkeimmät asiat yhteen yli 80 sivun esitysmateriaaliin, josta voidaan ottaa erillisiä osia käytettäväksi esimerkiksi osastopalavereissa. Näin asioista voidaan muistuttaa aihealue kerrallaan. Esitysmateriaali annetaan sisäisen verkon kautta koko henkilöstön käyttöön. Kampanjan aikana yrityksen toimistoissa oleville näyttötauluille laitetaan muistutusviestejä, jotka vaihtuvat viikoittain. Lisäksi henkilöstölle lähetetään sähköpostiviesteinä muistutuksia käynnissä olevasta kampanjasta. Viestit sisältävät suorat linkit sekä yrityksen tietoturvasivustolle että Pohjoismaille koottuun esitysmateriaaliin. Näin halutaan tarjota henkilöstölle mahdollisimman helppo tapa löytää tietoa tietoturvasta.

Kolmannella tutkimuskysymyksellä haluttiin selvittää, kuinka olisi mahdollista kerätä työntekijöille tärkeä ja samalla mielenkiintoinen materiaali tietoturvasta. Opinnäytetyön produktina toteutettu esitysmateriaali julkaistaan yrityksessä myöhemmin syksyllä. Esi- miehiltä sekä käyttäjätestauksesta saadun palautteen perusteella on esitysmateriaaliin onnistuttu keräämään yrityksen kannalta oleelliset tietoturva-aiheet. Esitysmateriaalista tuli laaja, kuten yrityksestä oli alun perin toivottu. Tosin aineiston laajuus voi olla myös uusi haaste, sillä se vaikeuttaa aineiston käsittelyä. Käyttäjää voi olla vaikea moti- voida lukemaan koko aineisto ajatuksella läpi, sillä sen läpikäynti vie melko paljon aikaa. Kovin lyhyttä versiota koko aineistosta ei pysty koostamaan. Tämä on huomioitu opinnäytetyön produktissa niin, että aineistosta voidaan helposti irrottaa erillisiä osia käytettäväksi mahdollisuuksien mukaan erilaisissa yrityksen info-tilaisuuksissa ja osasto- palaverissa.

Neljännellä tutkimuskysymyksellä haluttiin selvittää, kuinka ylläpitää ja kehittää työntekijöiden tietämystä tietoturvasta. Tietoturvakoulutuksella voidaan tutkimusten mukaan merkittävästi parantaa työntekijöiden tietoturvaosaamista. Lyhyet muistutusviestit ja tietoiskut sähköpostiin tai yrityksen näyttötauluille auttavat tietoturvaosaamisen ylläpi- tämiseen, mikäli niitä käytetään säännöllisesti. Ne ovat myös hyvä keino kehittää käyttä- jien yleistietämystä tietoturvasta. Muistutusviestit voivat olla esimerkiksi lyhyitä varoi- tuksia sisältäen tietoa muissa yrityksissä tapahtuneista tietomurroista tai vain yksittäisiä muistutuksia yrityksen toimintaohjeista.

Produktin esitysmateriaali on tehty englanninkielellä nimenomaan kansainvälisyyttä ajatellen. Materiaali annetaan käytettäväksi myös yrityksen muissa maissa toimiville or- ganisaatioille, sillä tämäntyyppistä koostettua esitysmateriaalia ei yrityksessä ole tällä hetkellä keskitetysti tarjolla. Useat eri maissa tietoturvatehtävissä toimivat henkilöt ovat olleet kiinnostuneita aineistosta. Riittävän laaja, mutta helposti ”pätkittävä” materiaali tarvitaan, jotta sitä voidaan käyttää hyväksi eri yhteyksissä. Esimerkiksi eri osastojen omissa palaverissa voidaan keskittyä lyhyesti niihin tietoturvan osa-alueisiin, jotka ovat kyseiselle osastolle tärkeimpiä.

Aineistoa opinnäytetyön tekemiseen oli tarjolla runsaasti. Tietoturva-ala kehittyi vauhdilla ja siitä syystä tuorein tieto löytyy pääasiassa Internetistä sekä alan lehdistä. Tärkeimmäksi opinnäytetyön tietolähteeksi muodostui Petteri Järvisen jo vuonna 2002 kirjoittama teos Tietoturva & yksityisyys. Järvinen on tietokirjailijana julkaissut tietotekniikka-aiheisia kirjoja jo 80-luvun puolesta välistä lähtien, joten hänellä on laaja näkemys tietoturvaan. Valtaosa teoksen tietosisällöstä on edelleen ajankohtaista, joten teosta voi kutsua alansa klassikoksi.

Opinnäytetyön produktille oli yritykseltä annettu selkeät ohjeet ja toivomukset. Materiaalia kasatessa olisi ollut kiinnostavaa syventyä tutkimaan, mitä muita keinoja perinteisen esitysmateriaalin, sähköpostin ja näyttötaulun lisäksi voisi käyttää tiedon esittämiseen ja välittämiseen. Kiinnostavaa olisi myös tietää, toimivatko esimerkiksi seinäjulisteet tai perinteiset paperiset henkilökohtaiset kirjeet tiedon välittämisessä nykyään vai menevätkö ne suoraan roskikseen. Kansainvälisessä yrityksessä on myös omat haasteet käytettävällä kielellä. Olisi mielenkiintoista selvittää, kuinka paljon kielellä on merkitystä tiedon välittämiseen. Menisikö viesti paremmin perille, jos esimerkiksi Suomessa käytettäisiin suomenkieltä vai onko sillä ollenkaan merkitystä kun valtaosa erikoissanastosta on kuitenkin käytössä englanninkielisenä?

Opinnäytetyön produktina toteutettavan kampanjan aikataulun vuoksi ei siitä saatavia kokemuksia voida analysoida tässä opinnäytetyössä. Tulevaisuudessa olisi kuitenkin mielenkiintoista selvittää, kuinka kampanjan toteutus onnistui. Esimiehiltä saadun palautteen perusteella yritys on kiinnostunut jatkamaan säännöllistä tietoturvasta muistuttamista, joten olisi kiinnostavaa tehdä kampanjasta pidemmän ajanjakson suunnitelma, esimerkiksi seuraaville kahdelle vuodelle. Lisäksi olisi mielenkiintoista tutkia pidemmän kampanjan vaikutusta henkilöstön tietoturvaosaamiseen.

## Lähteet

Arata, M. 2010. Identity Theft for dummies. Wiley Publishing, Inc. Indianapolis. United States of America.

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

Hamblen, M. 2011. IT managers start supporting employee-owned smartphones. Computerworld Inc. Luettavissa:  
[http://www.computerworld.com/s/article/9220145/IT\\_managers\\_start\\_supporting\\_employee\\_owned\\_smartphones?taxonomyId=17](http://www.computerworld.com/s/article/9220145/IT_managers_start_supporting_employee_owned_smartphones?taxonomyId=17)  
Luettu 9.10.2011.

Järvinen, P. 2002. Tietoturva & Yksityisyys. Docendo. Jyväskylä.

Karjalainen, M. 2011. Improving employees' information systems (IS) security behavior : Toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior. Väitöskirja. Oulun yliopisto. Oulu. Luettavissa: <http://jultika.oulu.fi/Record/isbn978-951-42-9567-6>  
Luettu 30.10.2011.

Kotilainen, S. 2011. Tietokone 07/2011. Yhden laitteen turvaa. Sanoma Magazines Finland Oy. Helsinki.

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

Lehto, T. 2011. Tietokone 03/2011. Netirikollisten metsästäjä. Sanoma Magazines Finland Oy. Helsinki.

Leidenius, K. 2011. Tietokone 05/2011. 10 Sisäistä uhkaa. Sanoma Magazines Finland Oy. Helsinki.

Luottokunta 2010. PCI-standardit. Luettavissa:

[http://www.luottokunta.fi/fi/toimialatietoa/pci\\_standardit/standardit](http://www.luottokunta.fi/fi/toimialatietoa/pci_standardit/standardit)

Luettu 30.10.2011

Phelps, J. 2010. How to Avoid Malware. Luettavissa:

[http://www.pcworld.com/article/210891/how\\_to\\_avoid\\_malware.html](http://www.pcworld.com/article/210891/how_to_avoid_malware.html)

Luettu 10.10.2011.

Pitkänen, J. 2011. Virukset kiusana jo neljännesvuosisadan. Luettavissa:

[http://www.tietokone.fi/uutiset/virukset\\_kiusana\\_jo\\_neljannesvuosisadan](http://www.tietokone.fi/uutiset/virukset_kiusana_jo_neljannesvuosisadan)

Luettu 29.9.2011.

Pulkkinen, P. 2011. Helsingin Sanomat 6.5.2011. Kotona on paremmat työvälineet kuin työpaikalla. Luettu 25.8.2011.

Ruohonen, M. 2002. Tietoturva. Docendo. Jyväskylä.

Siltala, T. 2010. Pilvipalvelujen tietoturva kuntoon. Luettavissa:

<http://www.tietoviikko.fi/edut/pilvi/pilvipalvelujen+tietoturva+kuntoon/a400099>

Luettu 30.10.2011.

Symantec Corporation 2006. Pharming on phishing-huijausta kehittyneempi ja vaikeammin havaittava hyökkäysmuoto. Luettavissa:

[http://fi.norton.com/library/familyresource/article.jsp?aid=article1\\_08\\_06](http://fi.norton.com/library/familyresource/article.jsp?aid=article1_08_06)

Luettu 28.9.2011.

Symantec Corporation 2011. Botit ja bottiverkot – kasvava uhka. Luettavissa:

<http://fi.norton.com/theme.jsp?themeid=botnet>

Luettu 29.9.2011.

Tietotekniikan liitto ry 2007. Pk-tietoturvatutkimus. Luettavissa:

<https://ssl.ttlry.fi/tutkimus/pk-tietoturvatutkimus>

Luettu 3.9.2011.

Tietoviikko 2011. Yrityksistä vuotaa enemmän tietoja kuin virastoista. Luettavissa:

[http://www.tietoviikko.fi/kaikki\\_uutiset/yrityksista+vuotaa+enemman+tietoja+kuin+virastoista/a698166](http://www.tietoviikko.fi/kaikki_uutiset/yrityksista+vuotaa+enemman+tietoja+kuin+virastoista/a698166)

Luettu 10.10.2011.

Toivonen, E. 2010. Bring your own computer – tuo oma työasemasi Pilvipalvelu trendi. Luettavissa: <http://www.thinking-business.net/blogi/2010/11/05/31>

Luettu 30.10.2011.

Tuurila, A. 2011. Tietokone 03/2011. Tietotyön kapinalliset. Sanoma Magazines Finland Oy. Helsinki.

Unilever Finland Oy 2010. Toimintakertomus vuodelta 2010. Helsinki.

Unilever Finland Oy 2011a. Unilever Finland Oy:lle uusi toimitusjohtaja. Lehdistötiedote. Luettavissa:

<http://www.cisionwire.fi/taitomyly/r/unilever-finland-oy-lle-uusi-toimitusjohtaja,c9156315>

Luettu 1.9.2011.

Unilever Finland Oy 2011b. Unilever Finland Oy:n nettisivut. Luettavissa:

<http://www.unilever.fi/aboutus/companystructure/default.aspx>

Luettu 12.10.2011.

Viestintätoimisto Conexio Oy 2007. Pk-yritysten tietoturvakysely. Luettavissa:

[https://ssl.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/PK-tietoturvatutkimus/pk-yritysten%20tietoturvakysely%202007.5.21\\_SZ.pdf](https://ssl.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/PK-tietoturvatutkimus/pk-yritysten%20tietoturvakysely%202007.5.21_SZ.pdf)

Luettu 3.9.3011.

Vikström, M. 12.10.2011. Nordic Risk Manager. Unilever Sverige Ab. Puhelinhaastattelun.

YLE Etelä-Karjala 2011. Nordean nimissä liikkuu jälleen huijausviestejä. Luettavissa:  
[http://yle.fi/alueet/etela-](http://yle.fi/alueet/etela-karjala/2011/09/nordean_nimissa_liikkuu_jalleen_huijausviesteja_2909979.html)

[karjala/2011/09/nordean\\_nimissa\\_liikkuu\\_jalleen\\_huijausviesteja\\_2909979.html](http://yle.fi/alueet/etela-karjala/2011/09/nordean_nimissa_liikkuu_jalleen_huijausviesteja_2909979.html)

Luettu 29.9.2011.

## **Liitteet**

Liite 1. ISC2011-kampanjan lyhyt kuvaus (project charter)

salassa pidettävä



Liite 2. ISC2011-kampanjan aikataulu

salassa pidettävä

Liite 3. ISC2011-kampanjan esitysmateriaali

salassa pidettävä

Liite 4. Kooste näyttötauluilla esitettävistä aineistoista

salassa pidettävä