



LAUREA

Selvitys tietoturvaohjeistuksen omaksumisesta yrityksessä



Saari, Jaro

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Selvitys tietoturvaohjeistuksen omaksumisesta yrityksessä

Saari, Jaro
Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
Tammikuu, 2011

Saari, Jaro

Selvitys tietoturvaohjeistuksen omaksumisesta yrityksessä

Vuosi 2011 Sivumäärä 36

Tämän opinnäytetyön tarkoituksena on selvittää kohdeyrityksen henkilöstön tietoturvaohjeistuksen tietämyksen tasoa sekä tehdä kehitysehdotuksia yrityksen tietoturvan ja tietoturvaohjeistuksen parantamiseksi. Opinnäytetyössä käsitellään tämän aihealueen keskeisimmät käsitteet, kuten tietoturvallisuus, tietoturvakäytännöt, tietoturvaohjeistus ja tietoturvatietoisuus.

Opinnäytetyön toimeksianto syntyi, kun yrityksen sisällä tehtiin elokuussa 2010 laatuauditointi. Laatuauditoinnin johdosta selvisi, että yrityksessä ei ole koskaan tehty tämän tyyppistä tutkimusta.

Henkilöstön tietoturvaohjeistuksen tietämyksen tasoa mitattiin kyselytutkimuksella marraskuussa 2010. Kyselytutkimus perustui kvantitatiiviseen menetelmään, koska se sopii hyvin laajojen tutkimuskyselyiden suorittamiseen. Kysely suoritettiin niin, että vastaajat pystyivät vastaamaan kyselyyn täysin anonyymisti.

Otannaksi valittiin kohdeyrityksen Helsingin toimipisteen henkilöstö. Kysely lähetettiin sähköpostitse kaikkiaan 295 henkilölle ja siihen vastasi 85 henkilöä. Vastausten avulla tehtiin kehitysehdotuksia tietoturvaohjeisiin sekä yleiseen tietoturvaan.

Kyselytutkimuksen vastaukset analysoitiin Excel-taulukkolaskentaohjelmaa apuna käyttäen. Ohjelmalla tehtiin myös kaaviot, jotka havainnollistavat vastausten tuloksia. Tämän lisäksi jokainen kysymys analysoitiin sanallisesti.

Kyselytutkimukseen vastanneet olivat suurimmaksi osaksi hyvin tietoisia tietoturvaohjeistuksen sisällöstä. Suurin epäröinnin aihe oli Internet-radiolähetysten kuuntelu yrityksen verkossa. Tämä on kielletty tietoturvaohjeistuksessa, tosin ei kovin selkeästi. Tästä asiasta tein yhden kehitysehdotuksen, jossa tätä tietoturvaohjeistuksen kohtaa voisi muuttaa selkeämmäksi. Tein myös kehitysehdotuksia liittyen yrityksen tietoturvaan yleisellä tasolla.

Saari, Jaro

Staff's knowledge of the company's information security instructions

Year	2011	Pages	36
------	------	-------	----

The purpose of this thesis is to examine the level of the staff's knowledge of the company's information security instructions. Another objective was to submit a development proposal for improving the information security and information security instructions of the company.

The assignment to this thesis was created when a quality audit was conducted in August 2010. The quality audit revealed that this type of study had never been undertaken in the company.

The staff's level of knowledge of the information security instructions was measured with a questionnaire survey in November 2010. The questionnaire survey was based on a quantitative method because it is suitable for performing comprehensive study inquiries. The inquiry was performed so that the interviewees were able to answer the inquiry totally anonymously. The staff of the Helsinki office was chosen to be the target group. The inquiry was sent by e-mail to altogether 295 people and 85 people answered it. The objective of the questionnaire survey was to analyze the staff's level of knowledge of the information security instructions.

Based on the answers, development proposals were made to the information security instructions and to the company's general information security. The answers of the questionnaire survey were analyzed using the Excel program. With the program, the schemes which illustrate the results of answers were created. In addition to this, every question was verbally analyzed.

The respondents were highly aware of the contents of the information security instructions. The major subject of hesitation was listening to Internet radio broadcasts in the company network. This had been forbidden in the information security instructions; however, not clearly. One development proposal was made concerning this subject, as well as development proposals concerning the company's information security on a general level.

This thesis contains the most central concepts of this subject, such as information security, information security policy, information security instructions and information security awareness.

Key Words information security instructions, information security awareness, information security

Sisällys

1	Johdanto	6
1.1	Tutkimusongelma	8
1.2	Yritys X.....	8
1.3	Keskeiset käsitteet.....	9
1.4	Tietoturvatietoisuuden kohottaminen henkilöstön keskuudessa	10
1.5	Salassapitoon ja eettisyyteen liittyvät tekijät	10
1.5.1	Salassapitoon liittyvät tekijät	11
1.5.2	Eettisyyteen liittyvät tekijät	11
2	Tutkimuksen toteutus	11
2.1	Otanta	11
2.2	Tutkimusmenetelmä.....	11
2.3	Aineiston kerääminen	12
2.4	Kysymyslomakkeen suunnittelu.....	13
2.5	Saatekirje.....	14
3	Tutkimuksen tulokset	14
3.1	Kysymykset	14
3.2	Yhteenveto	24
4	Kehittämisehdotukset	25
4.1	Äänen tai kuvan suoratoisto.....	25
4.2	Ulkoiset tallennusvälineet	25
4.3	Vierailijat yrityksen tiloissa	26
4.4	Tietoturvaongelmien ilmoitusvelvollisuus	26
4.5	Mistä voi epäillä tietokoneen saaneen haittaohjelmatartunnan.....	26
4.6	Tietoturvakäytännön suomentaminen	26
4.7	Henkilöstön lisäkoulutus	26
4.8	Tietoturvaohjeistuksen rinnalle lisäohjeistus	27
4.9	Muistilista tietoturvasta.....	27
4.10	Lyhyet tietoiskut tietoturvasta.....	28
4.10.1	Mitä tarkoittaa tietoturvallisuus?.....	28
4.10.2	Miksi tietoturva on tärkeää?.....	29
4.11	Uusia tutkimuksia	29
5	Tutkimuksen luotettavuus	29
6	Johtopäätökset	30
6.1	Uudet tutkimukset	31
	Lähteet	32
	Liitteet.....	34
	Liite 1: Kysymykset	34
	Liite 2: Tietoisku Internet-radiolähetysten kuuntelusta	36

1 Johdanto

Tietotekniikka on iso osa yrityksen liiketoimintaa, ja tiedon turvaaminen onkin nykypäivänä kiinteä osa monen yrityksen strategiaa. Tätä varten yritykset ovat laatineet omia tietoturvakäytäntöjä sekä -ohjeistuksia. Henkilöstön tietoturvaohjeistuksen tietämyksen tason selvittäminen onkin monelle yritykselle olennaista ja antaa paljon lisätietoja siitä, miten kehittää yrityksen tietoturvaa paremmaksi.

CSI Computer Crime & Security Surveyn mukaan vuonna 2008 jopa 44 prosenttia yritysten tietoturvaongelmista koostui yrityksen oman henkilöstön väärinkäytöksistä (Richardson 2008). Tämä osoittaa, että yrityksen henkilökunnan kouluttaminen tietoturvan osalta on todella tärkeää. Pelkkä tekninen tietoturva ei riitä yrityksen turvaksi, vaan tarvitaan hyviä tietoturvaohjeita ja käytäntöjä. Ohjeiden myös täytyy olla sellaisia, joita henkilöstö noudattaa mielellään ja soveltaa työssään. Näin henkilöstön keskuudessa vahingossa tai huolimattomuuttaan tehtyjä tietoturvarikkomuksia vähennetään merkittävästi.

Henkilöstön tietoturvatietoisuus on tärkeä osa yrityksen kokonaistietoturvaa, koska isokin yritys koostuu yksittäisistä työntekijöistä. Tietoturvatietoinen työntekijä on tietoinen roolistaan osana yrityksen tietoturvaa ja näin oppii olemaan osana tietoturvallista työympäristöä. Tietoturvatietoinen työntekijä myös raportoi tietoturvaongelmista asiaankuuluville tahoille. (Puhakainen 2006.)

Työn tavoitteena oli selvittää yrityksen henkilöstön tietoturvaohjeistuksen tietämyksen tasoa ja tehdä tulosten pohjalta parannusehdotus yrityksen tietoturvaohjeistukseen ja tietoturvallisuuden yleensä. Opinnäytetyön aiheen sain suoraan kohdeyritykseltä, joka tarvitsi tutkittuja tuloksia henkilöstönsä tietoturvaohjeistuksen tietämyksen tasosta.

Tutkimuksen teoreettinen viitekehys perustuu tietoturvallisuutta käsittelevään kirjallisuuteen ja dokumentteihin. Näitä ovat muun muassa Valtionvarainministeriön VAHTI-tietoturvaohjeet, Laaksosen, Nevasalon ja Tomulan Yrityksen Tietoturvakäsikirja sekä IT-Grundschutz Manual 2005. Teoriaa käytettiin tutkimuksen ohjaamisessa ja tavoitteiden täsmentämisessä.

Tämä opinnäytetyö jakaantuu johdantoon, jossa kerrotaan tutkimuksen taustat, tutkimusongelma sekä keskeiset käsitteet. Tämän jälkeen luvussa kaksi kerrotaan miten opinnäytetyö on toteutettu sekä minkälaisia menetelmiä tässä opinnäytetyössä on käytetty. Luvussa kolme käydään läpi tutkimuksen tulokset ja tehdään niistä yhteenveto. Luvussa neljä teen kehitysehdotuksia liittyen tietoturvaohjeistukseen sekä yrityksen yleiseen tietoturvallisuuteen. Luku

viisi käsittelee tämän tutkimuksen luotettavuutta. Viimeisessä luvussa teen johtopäätöksiä tästä tutkimuksesta ja summaan tutkimuksen tulokset.

1.1 Tutkimusongelma

Tutkimusongelmana oli yritys X:n henkilöstön tietoturvaohjeistuksen tietämyksen tason selvittäminen. Aihe rajattiin koskemaan vain tietoturvaohjeistusta, koska yleisen tietoturvatietoisuuden kartoitus olisi ollut liian laaja alue tälle opinnäytetyölle. Tutkimuksella haluttiin selvittää henkilöstön tietämyksen tasoa liittyen yrityksen tietoturvaohjeistukseen.

Tutkimuksen tarve juontuu yrityksessä tehdystä laatuauditoinnista, joka tehtiin elokuussa 2010. Laatuauditoinnista syntyneestä arviointiraportista käy selkeästi ilmi tarve tällaiselle tutkimukselle. Raportissa mainitaan, että henkilöstön tietoturvaohjeistuksen tietoisuudesta ei ole tehty kartoitusta. Myös tämän opinnäytetyön toimeksiantaja piti tätä tutkimusta tärkeänä, jotta henkilöstön tietoturvaohjeistuksen tietämyksestä saataisiin tutkittua tietoa.

Yrityksen henkilöstön tietoturvatietoisuutta on tähän asti pidetty yllä vaatimalla jokaista työntekijää lukemaan tietoturvaohjeistus läpi sekä erilaisilla tietoisuuksilla. Tietoisuuksia ovat esimerkiksi yrityksen seinillä olevat taulut ja julisteet, jotka antavat tietoa tietoturvariskeitä.

Yrityksellä on tietoturvaohjeistus sisäverkossa kaikkien työntekijöiden nähtävillä sekä tietoturvakäytäntöjä yrityksen verkossa. Suomenkielinen versio tietoturvaohjeistuksesta on ollut saatavilla syksystä 2009. Siihen asti kaikki tietoturvaohjeistukset ovat olleet englanniksi. Tälläkin hetkellä osa tietoturvakäytännöistä on englanniksi. Tämä on osasyynä tutkimuksen tarpeellisuudelle.

Valmista tutkimusta voidaan hyödyntää kohdeyrityksen tietoturvan kehittämisessä.

1.2 Yritys X

Yritys X on suuri kansainvälinen yritys, joka on perustettu vuonna 1937. Yritys tuottaa yritysratkaisuja sekä kuluttajatuotteita. Suomessa yrityksellä on noin 397 työntekijää. Suomen pääkonttori sijaitsee Helsingissä, Suomessa toimipisteitä on yhteensä 35 kpl. Yrityksellä on maailmanlaajuisesti toimipisteitä 50 eri maassa. Yrityksen liikevaihto on noin 164 miljoonaa euroa.

Opinnäytetyön tarkoituksena oli tutkia Helsingin toimipisteen henkilöstön tietoturvaohjeistuksen tietämystä. Tutkittavien henkilöiden lukumäärä oli 295.

Yrityksen tietoturvaohjeistus on kuusisivuinen dokumentti, joka käsittelee yrityksen verkon ja laitteiden käyttöä. Dokumentissa kerrotaan mitkä asiat ovat kiellettyjä sekä miten ohjeistuk-

sen noudattamista voidaan valvoa. Dokumentissa kerrotaan myös, mitä seurauksia tietoturvaohjeiden noudattamista jättämisellä on.

1.3 Keskeiset käsitteet

Tietoturva

Tietoturvallisuuden tarkoituksena on taata tiedon, tietojärjestelmien, ja palveluiden asianmukainen suojaus. Suojaus tapahtuu käytännössä teknisillä, hallinnollisilla ja muilla toimenpiteillä. Riskit, jotka liittyvät niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen täytyvät olla asianmukaisesti hallinnassa. Näitä riskejä ovat luonnonmullistukset, laitteistoviat, ohjelmistoviat, tahalliset teot tai tapaturmaiset teot.

Tietoturvallisuus tarkoittaa myös, että tieto ja tietojärjestelmät ovat vain niiden henkilöiden saatavilla, jotka ovat valtuutettuja käyttämään niitä. (VAHTI 5/2003, 8; VAHTI 4/2009, 8-9.)

Tietoturvallisuus on pieniä tekoja osana jokapäiväistä toimintaa. Toimiva tietoturva on osa yrityksen kulttuuria, jolloin kaikilla on ymmärrys tietoturvasta ja kaikki työskentelevät sen mahdollistamiseksi ja ylläpitämiseksi. (Laaksonen, Nevasalo & Tomula 2006, 17.)

Tietoturvakäytännöt

Tietoturvakäytännöt ovat lakien, sääntöjen ja käytäntöjen kokonaisuus. Ne määrittävät miten organisaatio ylläpitää, suojaa ja levittää yrityksen sisäistä arkaluontoista tietoa (Slade 2006, 202.)

Tietoturvaohjeistus

Tietoturvaohjeistus on dokumentti, joka sisältää tietoturvaan liittyviä ohjeita yrityksen tai yhteisön työntekijöille. Tietoturvaohjeistus voi sisältää ohjeita liittyen työaseman, yrityksen sisäverkon, Internetin, ulkoisten tallennusvälineiden ja tulostimien käyttöön. Ohjeistuksessa voi olla myös ohjeita sisäverkon salasanan käyttöön ja laatimiseen, virustorjuntaan, luottamuksellisten dokumenttien tuhoamiseen ja jakamiseen ynnä muihin.

Tietoturvaohjeistus on tavallisesti osa tietoturvakäytäntöä. Se on kirjallinen käytäntö, joka käsittelee tietokoneiden ja verkkoresurssien käyttöä.

(Slade 2006, 123; 37.)

Tietoturvatietoisuus

Tietoturvatietoisuus on yrityksen henkilöstön ymmärrystä tietoturvan tärkeydestä ja säännöistä. Tietoturvatietoinen työntekijä on tietoinen roolistaan osana yrityksen tietoturvaa ja näin oppii olemaan osana tietoturvallista ympäristöä.

Tietoturvatietoisuudella tarkoitetaan tietoturvapoliittikan ja ohjeiden noudattamista mikä näkyy henkilöstön toimintatavoissa. Tietoturvatietoinen työntekijä myös raportoi tietoturvaongelmista asiaankuuluville tahoille. (Puhakainen 2006).

1.4 Tietoturvatietoisuuden kohottaminen henkilöstön keskuudessa

Voidakseen toteuttaa hyvää tietoturvallisuutta, on yrityksen tehtävä tietoturvasta osa yrityksen strategiaa ja pyrkiä kohottamaan henkilöstön tietoturvatietoisuutta. Koko henkilöstö pitää vakuuttaa siitä, että tietoturva on tärkeä väline yrityksen toiminnan takaamiseksi. Henkilöstön kanssa täytyy käydä läpi kaikki tärkeät tietoturvallisuutta koskevat säännöt ja ohjeet. Henkilöstölle pitää myös ilmoittaa mitä heiltä vaaditaan tietoturvallisen työympäristön aikaansaamiseksi ja mitä heidän täytyy tehdä, jos he kohtaavat tietoturvaongelmia. Tietoturvatietoisten työntekijöiden aikaansaamiseksi vaaditaan yleensä pitkäaikaista ja jatkuvaa toimintaa. Pelkät yksittäiset tietoturvakurssit eivät yksin riitä. (IT-Grundschutz Manual 2005, 86.)

Tietoturvatietoiset työntekijät ovat todella suuri apua yrityksen tietoturvallisuuden kohottamisessa. Työntekijöitä kouluttamalla saadaan henkilöstö arviomaan omia tekojaan tietoturvallisuuden kannalta, niin työpaikalla kuin yksityiselämässäänkin. (IT-Grundschutz Manual 2005, 86.) Oikeanlaisella kouluttamisella ja tiedottamisella tietoturvallinen käyttäminen siis kasvaa osaksi henkilöstön identiteettiä.

Jotta tietoturvallisuuden koulutusta ja tiedottamista tuettaisiin tarvittavissa määrin, on todella tärkeää että yrityksen johto ja hallitus ovat tietoisia tietoturvallisuuden tärkeydestä yrityksen menestykselle (IT-Grundschutz Manual 2005, 86).

1.5 Salassapitoon ja eettisyyteen liittyvät tekijät

Salassapitoon kiinnitettiin tässä opinnäytetyössä erityistä huomiota, koska aihe on arka ja vastauksista haluttiin saada mahdollisimman luotettavia.

1.5.1 Salassapitoon liittyvät tekijät

Opinnäytetyöni toimeksiantaja ei halunnut nimeään opinnäytetyöhöni. Viittaankin yritykseen vain nimellä Yritys tai Yritys X. Opinnäytetyössäni ei mainita yrityksen nimeä tai yrityksessä työskenteleviä henkilöitä nimeltä.

Kyselylomakkeessa ei kysytty vastaajien henkilötietoja tai muitakaan tietoja, joilla vastaajat voisi tunnistaa. Kyselyyn vastaaminen oli siis täysin anonyymiä, pois lukien kuuluminen juuri tämän yrityksen henkilöstöön.

1.5.2 Eettisyyteen liittyvät tekijät

Kyselytutkimus suunniteltiin niin, että kenenkään ei ollut pakko vastata siihen. Tutkimuksesta myös tiedotettiin etukäteen saatekirjeen muodossa. Saatekirjeessä kerrottiin tutkimuksen taustat, kuka tutkimuksen tekee sekä mihin vastauksia käytetään.

2 Tutkimuksen toteutus

2.1 Otanta

Otantana käytettiin harkinnanvaraista otantaa, jossa vastaajiksi valittiin Helsingin toimipisteiden henkilöstö. Tämä toimipiste valittiin, koska minulla on omakohtaista kokemusta juuri tästä toimipisteestä ja yleisimmät tietoturvarikkomukset ja ongelmat olivat jo tiedossani. Tutkittavien henkilöiden lukumäärä oli 295.

2.2 Tutkimusmenetelmä

Kvantitatiivista tutkimusmenetelmää käytetään melko runsaasti sosiaali- ja yhteiskuntatieteissä. Kvantitatiivisen tutkimuksen perusta on luonnontieteessä ja useat menetelmät ovat samoja näillä tieteenoilla. (Hirsjärvi, Remes & Sajavaara 2009, 139.)

Kvantitatiivisen tutkimuksen kohteina ovat usein fyysiset esineet ja ilmiöt sekä ihmiset. Kvantitatiivista tutkimusta käytetään yleensä suuren joukon tutkimukseen ja tutkimuskohteita tarkastellaan yleisellä tasolla. (Empiiriset aineistot ja analysoinnin kysymykset 1999.)

Kvalitatiivisessa menetelmässä tutkittavan ja tutkijan suhde on yleensä hyvin läheinen, joka tarkoittaa käytännössä yksilö- tai ryhmähaastatteluja. Tästä syystä vastaajamäärät ovat usein kvalitatiivisessa tutkimuksessa melko pieniä. Kvalitatiivinen tutkimus on yleensä myös teoriaa luovaa kun taas kvantitatiivinen tutkimus pyrkii varmistamaan jo olemassa olevaa teoriaa. (Saukkonen.)

Tähän opinnäytetyöhön valittiinkin tutkimusmenetelmäksi kvantitatiivinen tutkimus. Tämä menetelmä valittiin, koska se sopii hyvin laajojen vastaajamäärien tutkimiseen.

Kvantitatiivisen tutkimuksen tuloksena käytetään numeroita, ja vastaukset perustuvat yleensä aina numeroihin. Esimerkiksi kvalitatiivisen tutkimuksen tulokset ovat yleensä aina tekstimuodossa, mikä ei olisi sopinut näin laajan tutkimuksen kanssa käytettäväksi. Tässä tutkimuksessa kysymykset lähetettiin 295 henkilölle, joten kvantitatiivinen menetelmä koettiin ainoaksi järkeväksi vaihtoehdoksi vastausten keräämiseen. Näin suuren henkilömäärän läpikäyminen yksilö tai ryhmähaastatteluilla olisi ollut todella työlästä ja aikaa olisi kulunut huomattava määrä, joten tässä työssä haastattelujen käyttö ei ollut mahdollista.

Kvalitatiivisessa tutkimuksessa vastauksista olisi saatu paljon yksityiskohtaisempia ja tarkempia, mutta näin laajassa tutkimuksessa ei kvalitatiivisen tutkimuksen tekemiseen olisi ollut aikaa eikä voimavaroja. Kvantitatiivinen tutkimus on vaivattomampi sekä nopeampi suorittaa. Toisaalta kvantitatiivinen tutkimus ei kuvaa tutkimuskohteita kovin tarkasti, vaan lähinnä pintapuolisesti. Tässä tutkimuksessa ei tosin ole tarvettakaan saada kovin yksityiskohtaisia vastauksia, vaan lähinnä yleistettäviä tuloksia.

2.3 Aineiston kerääminen

Tässä opinnäytetyössä käytettiin aineiston keräämiseen kyselytutkimusta, joka sopii hyvin yhteen kvantitatiivisen tutkimusmenetelmän kanssa käytettäväksi.

Kyselytutkimus valittiin, koska kyselylomake haluttiin lähettää laajalle joukolle. Kyselylomakkeen analysointi on helppoa suurien vastaajamäärien tutkimuksissa sekä se koettiin nopeimmaksi tavaksi kerätä suuri määrä vastauksia.

Kyselytutkimuksen periaate on koota tietyin kriteerein tutkimukseen tarvittavalta joukolta vastauksia selkeisiin kysymyksiin. (Kyselyyn perustuvan tutkimuksen suorittaminen 2007). Kyselytutkimuksen hyvänä puolena on, että sen avulla voidaan kerätä suuria tutkimusaineistoja tutkimuksessa voi olla paljon kysymyksiä ja kohdehenkilöitä. Kyselylomakkeella tutkimuksen tekeminen on myös helppoa ja aikaa säästävää. Lomake voidaan lähettää suurella vastaajajoukolle ja aineisto on helppo käsitellä tietokoneella. (Hirsjärvi, Remes & Sajavaara 2009, 195.)

Kyselytutkimus suoritettiin sähköisesti, yrityksen omaa kyselyohjelmaa käyttäen. Ohjelman avulla voitiin lähettää jokaiselle työntekijälle kysely sähköpostitse. Sähköpostikysely oli mielestäni hyvä vaihtoehto, koska jokainen yrityksen työntekijä käyttää sähköpostia joka päivä

työssään. Yrityksen omaa kysymyslomake-ohjelmaa apuna käyttäen, voidaan kyselytutkimuksen tulokset viedä suoraan esimerkiksi Exceliin.












2.4 Kysymyslomakkeen suunnittelu

Suurin osa kysymyksistä on suoraan johdettu tietoturvaohjeistuksesta. Kuten edellisessä luvussa mainitsin, käytettiin kysymyslomakkeena yrityksen omaa lomaketta. Tällä toivottiin olevan positiivinen vaikutus vastausprosenttiin.

Lomakkeen suurin mahdollinen kysymysmäärä oli 10 kysymystä, joten se aiheutti pientä karsimista ja kysymyksiä piti miettiä tarkemmin. Kyselomakkeen laatimisen jälkeen tehtiin pilot-tikysely pienelle joukolle yrityksen henkilöstöä. Pilottikyselyn jälkeen kysymyslomake todettiin toimivaksi ja sillä päätettiin suorittaa varsinainen kysely. Vastausajaksi päätettiin laittaa yksi viikko, koska tutkimuksella oli tässä vaiheessa hieman kiire ja toisaalta vastauksia ajateltiin kuitenkin tulevan riittävästi.

Survey Results
Please answer the following questions, then click on 'Save & Close' above.

Survey Code	Tietoturva 2010
Description	Verkon, internetin ja ICT-laitteiden käyttöä koskevat yhteiseurooppalaiset toimintaohjeiden itsearviointikysely
Comments	Kiitos ajastasi
Answers From	

Item	Answer
	If an answer field has this symbol  , you can click on this to select from a list of possible answers
Oman organisaatiosi päätaso	
Onko vertaisverkkosovellusten lataaminen Internetistä hyväksyttävää yrityksenomistamalla ICT-laitteella?	
Voiko Internetistä lataamieni ohjelmien mukana tulla haittaohjelmia yrityksen laitteille?	
Voiko asentamieni sovellusten ansiosta joku ulkopuolinen murtautua yrityksen verkkoon?	
Onko sallittua luovuttaa oma käyttäjätunnus ja salasana toiselle työntekijälle?	
Voivatko toiselle työntekijälle luovutetut tunnukset päätyä myös ulkopuolisille henkilöille?	
Työasema täytyy aina lukita, kun poistun sen luota	
Voiko lukitsemattoman työaseman kautta joku ulkopuolinen saada käsiinsä arkaluontoista tietoa?	
Saan kuunnella Internet-radiolähetyksiä yrityksen verkossa	
Internet-radiolähetyksien kuuntelu hidastaa yrityksen verkkoa	

Kuvio 1: Kysymyslomake

2.5 Saatekirje

Ennen varsinaisen kyselyn suorittamista lähetettiin kohderyhmälle saatekirje. Saatekirjeessä kerrottiin, että teen opinnäytetyötä henkilöstön tietoturvaohjeistuksen tietämyksen tasosta ja olen opiskelijana Laurea-ammattikorkeakoulussa. Saatekirjeessä sanottiin myös, että tutkimuksen tuloksia tullaan hyödyntämään tietoturvan parantamisessa ja vastaukset ovat täysin anonyymejä. Saatekirjeen tavoitteena oli saada henkilöstö vastaamaan kyselytutkimukseen ja tiedottaa henkilöstölle kyselytutkimuksen taustoista.

Saatekirjeen kirjoitti yrityksen edustaja, mutta myös minä vaikutin sen sisältöön.

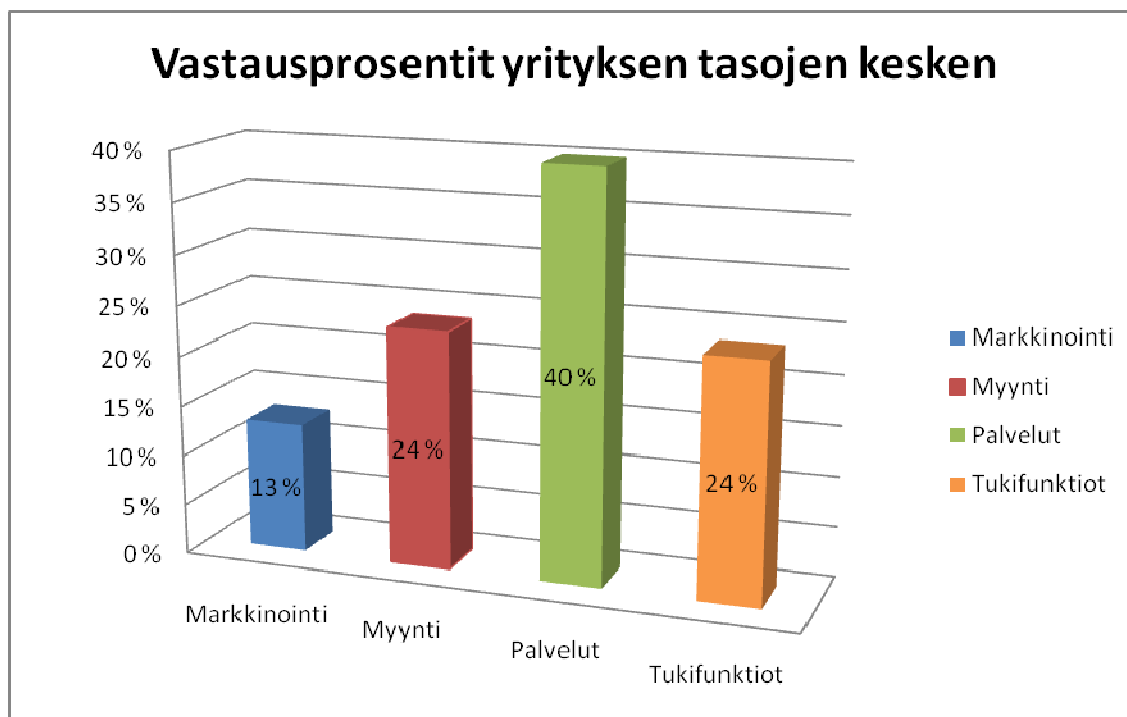
3 Tutkimuksen tulokset

Kyselylomake lähetettiin 295 työntekijälle ja vastaukset saatiin 85 työntekijältä. Vastausprosentiksi saatiin siis 29 %. Vastausprosentti jäi kaikesta huolimatta melko pieneksi. Tähän oli luultavasti osasyynä suhteellisen lyhyt vastausaika, joka oli vain yhden viikon pituinen. Seuraavissa luvuissa käyn läpi vastaukset ja kerron tarkemmin kysymyksien taustat.

3.1 Kysymykset

Vastausprosentit yrityksen toimintojen kesken

Suurin osa vastauksista tuli yrityksen palvelutasolta, heidän yhteenlaskettu vastausmääränsä oli 34 kpl (40 %). Toisena tulivat Myynti sekä Tukifunktiot, joiden kummankin vastausmäärä oli tasan 20 kpl (24 %). Viimeisenä oli Markkinointi, jonka vastausmääräksi jäi 11 kpl (13 %).



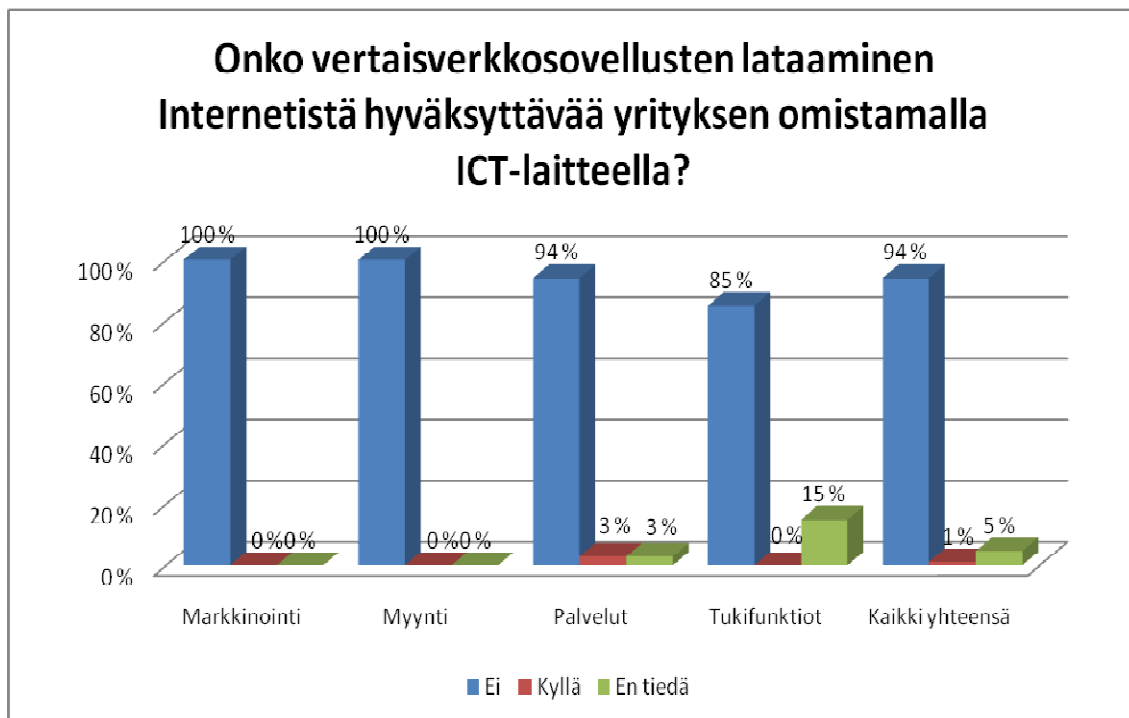
Kuvio 2: Vastausprosentit yrityksen toimintojen kesken

Onko vertaisverkkosovellusten lataaminen Internetistä hyväksyttävää yrityksen omistamalla ICT-laitteella?

Tämä kysymys käsitteli tietoturvaohjeistuksen kohtaa, jossa kielletään sovellusten lataaminen työasemalle ilman erillistä lupaa. Kohdassa kielletään erityisesti vertaisverkkosovellusten lataaminen työasemalle sekä niiden käyttäminen. Kysymys oli ajankohtainen, koska yrityksen ICT-laitteilta on löytynyt vertaisverkkosovelluksia aikaisemmin. Tästä huolimatta suurin osa vastanneista tiesi, että vertaisverkkosovellusten lataaminen ei tietoturvaohjeistuksen mukaan ole hyväksyttävää.

Kaikki markkinoinnin 11 vastaajaa vastasivat tähän kysymykseen ”Ei”. Samoin tekivät myynnin 20 vastaajaa. (Kuvio 3). Palveluiden vastaajista 32 (94 %) vastasi ”Ei”, yksi (3 %) ”Kyllä” sekä yksi (3 %) ”En tiedä”. Tukifunktioiden vastaajista 17 (85 %) vastasi ”Ei” ja kolme (15 %) vastasi ”En tiedä”.

Kaikkien toimintojen vastaukset yhteenlaskettuna vastasi 80 (94 %) ”Ei”, yksi (1 %) ”Kyllä” ja neljä (5 %) ”En tiedä”.



Kuvio 3: Vertaisverkkosovellusten lataaminen Internetistä

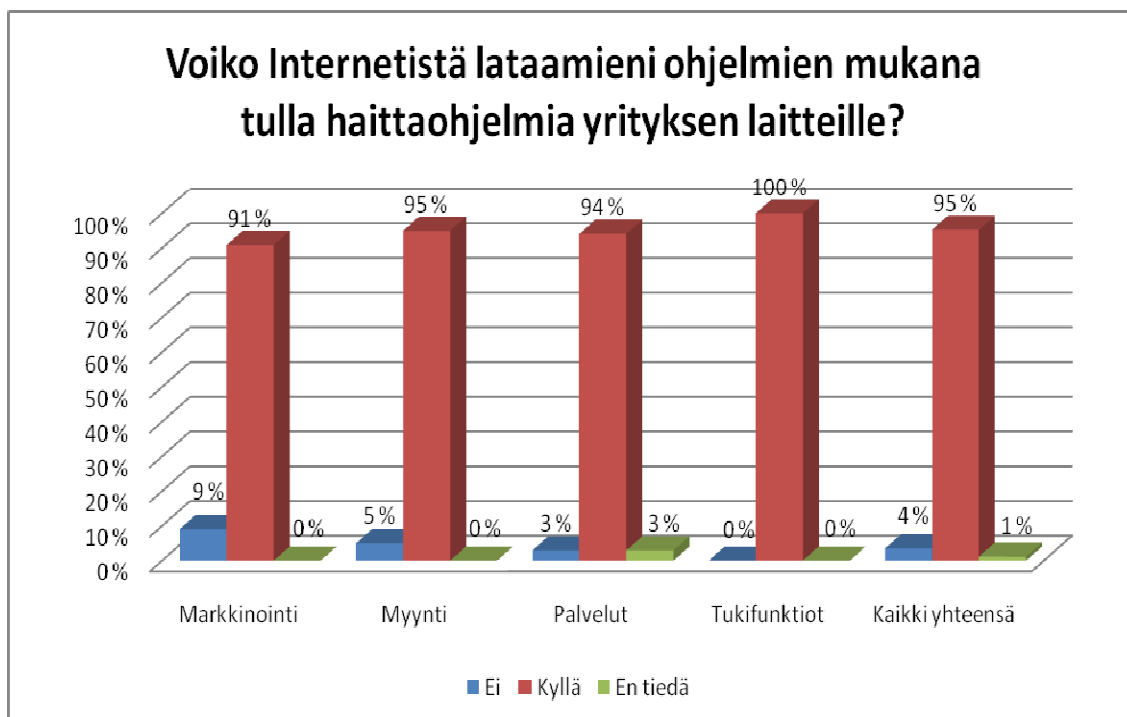
Voiko Internetistä lataamieni ohjelmien mukana tulla haittaohjelmia yrityksen laitteille?

Kysymys käsitteli pääpiirteissään samaa kohtaa tietoturvaohjeistuksesta, kuin edellinenkin kysymys. Tämä kysymys oli vain yleisluonteisempi ja pohjautui enemmän vastaajan omaan tietämykseen tietoturvasta. Vastauksista näkee, että yrityksen henkilöstöllä on hyvin tiedossa Internetistä haettujen ohjelmien mahdolliset vaarat.

Markkinoinnin vastaajista vastasi tähän kysymykseen 10 (91 %) ”Kyllä” ja yksi (9 %) ”Ei”.

Myyntin puolelta vastasi 19 (95 %) ”Kyllä” ja yksi (5 %) ”Ei”. Palveluiden vastaajista 32 (94 %) vastasi ”Kyllä”, yksi (3 %) ”Ei” ja yksi (3 %) ”En tiedä”. Tukifunktioiden kaikki 20 vastaajaa vastasit ”Kyllä”.

Kaikkien toimintojen vastaukset yhteenlaskettuna vastasi 81 (95 %) ”Kyllä”, kolme (4 %) ”Ei” ja yksi (1 %) ”En tiedä”.



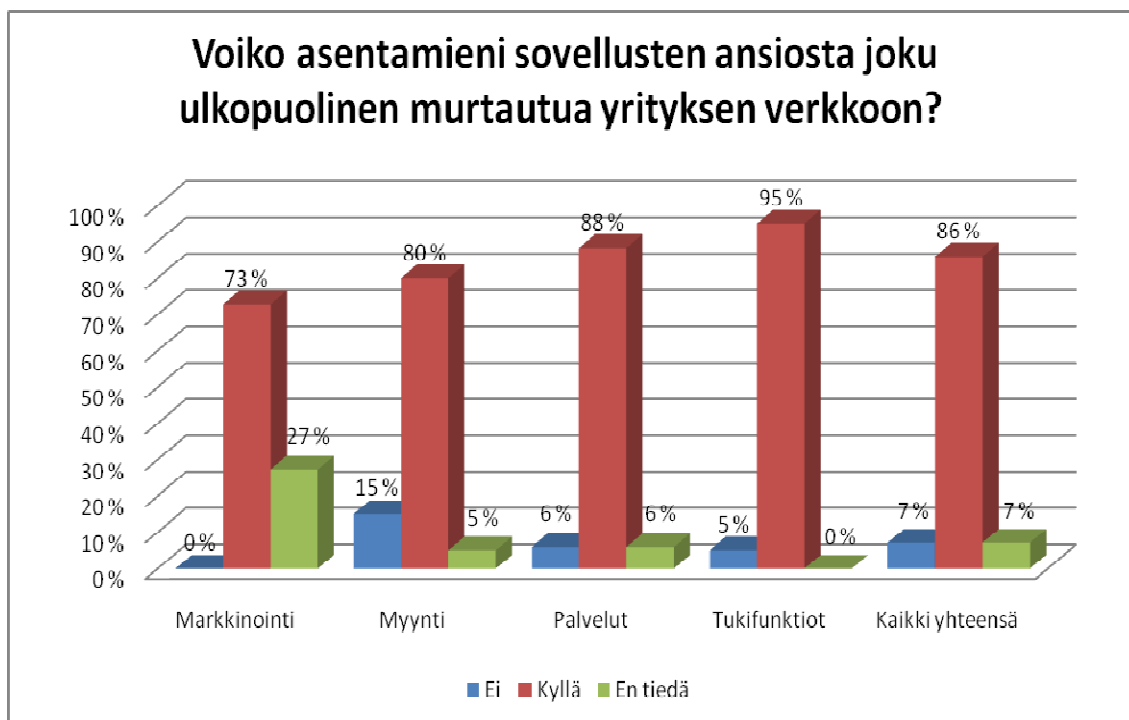
Kuvio 4: Haittaohjelmat Internetistä ladatuista ohjelmista

Voiko asentamieni sovellusten ansiosta joku ulkopuolinen murtautua yrityksen verkkoon?

Tämä kysymys käsitteli myös ulkopuolisten sovelluksien vaaroja, kuten kaksi edellistäkin kysymystä. Kysymyksen tarkoituksena oli laittaa vastaajat miettimään itse työasemalle ladattujen ja asennettujen ohjelmien turvallisuutta sekä minkälaista vahinkoa ne voisivat tuottaa yritykselle. Tämä kysymys käsitteli myös samaa kohtaa tietoturvaohjeistuksessa, kuin kaksi edellistäkin kysymystä. Tässä kysymyksessä on enemmän hajontaa vastausten välillä, kuin kahdessa edellisessä. Vastaajat eivät nähtävästi ole olleet niin tietoisia tässä kysymyksessä käsiteltävästä uhkatekijästä samalla tavalla kuin edellisissä kysymyksissä.

Markkinoinnin vastaajista 8 (73 %) vastasi tähän kysymykseen ”Kyllä” ja kolme (27 %) vastasi ”En tiedä”. Myynnin henkilöstöstä vastasi 16 (80 %) ”Kyllä”, kaksi (15 %) ”Ei” ja yksi (5 %) ”En tiedä”. Palveluiden vastaajista 30 (88 %) vastasi ”Kyllä”, kaksi (6 %) ”Ei” ja kaksi (6 %) ”En tiedä”. Tukifunktioiden vastaukset olivat 19 (95 %) ”Kyllä” ja yksi (5 %) ”Ei”.

Kaikkien toimintojen vastaukset olivat yhteensä 73 (86 %) ”Kyllä”, 6 (7 %) ”Ei” ja 6 (7 %) ”En tiedä”.

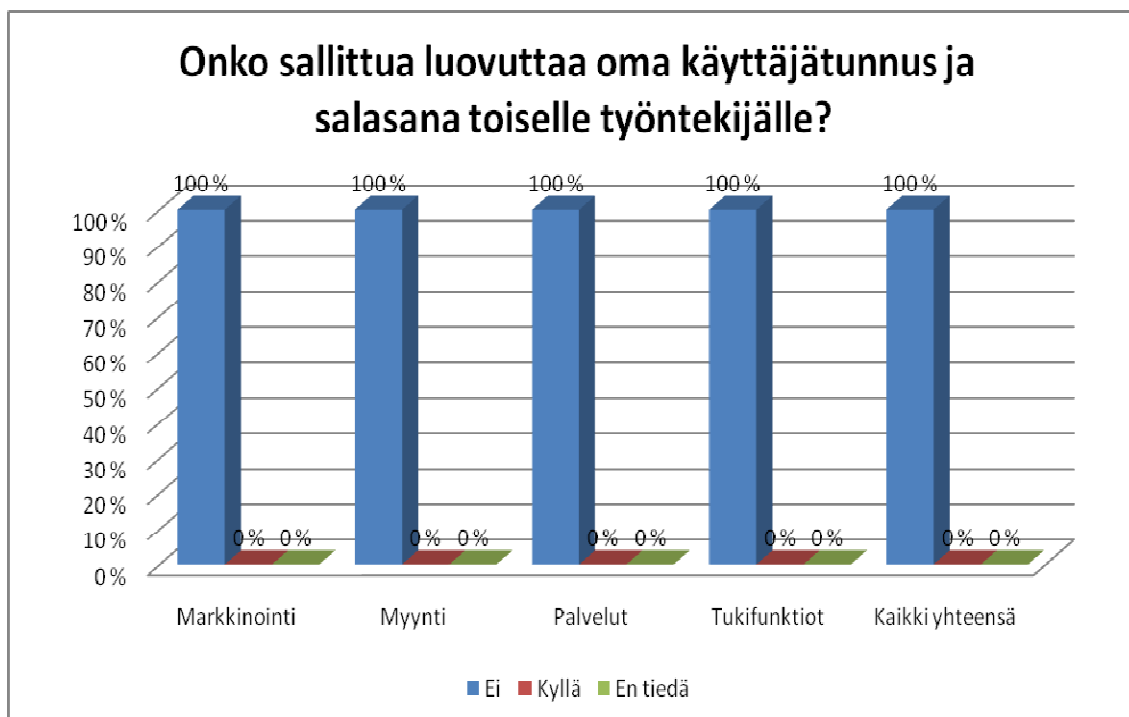


Kuvio 5: Yrityksen verkkoon murtautuminen asennettujen ohjelmien avulla

Onko sallittua luovuttaa oma käyttäjätunnus ja salasana toiselle työntekijälle?

Kysymys käsittelee tietoturvaohjeistuksen kohtaa, missä kielletään käyttäjätunnuksen ja salasanan luovuttaminen toisille henkilöille ilman kirjallista lupaa. Kuten vastauksista näkee, tästä ei ollut vastaajilla minkäänlaista epäselvyyttä.

Kaikki 85 vastaajaa vastasivat tähän kysymykseen ”Ei”.



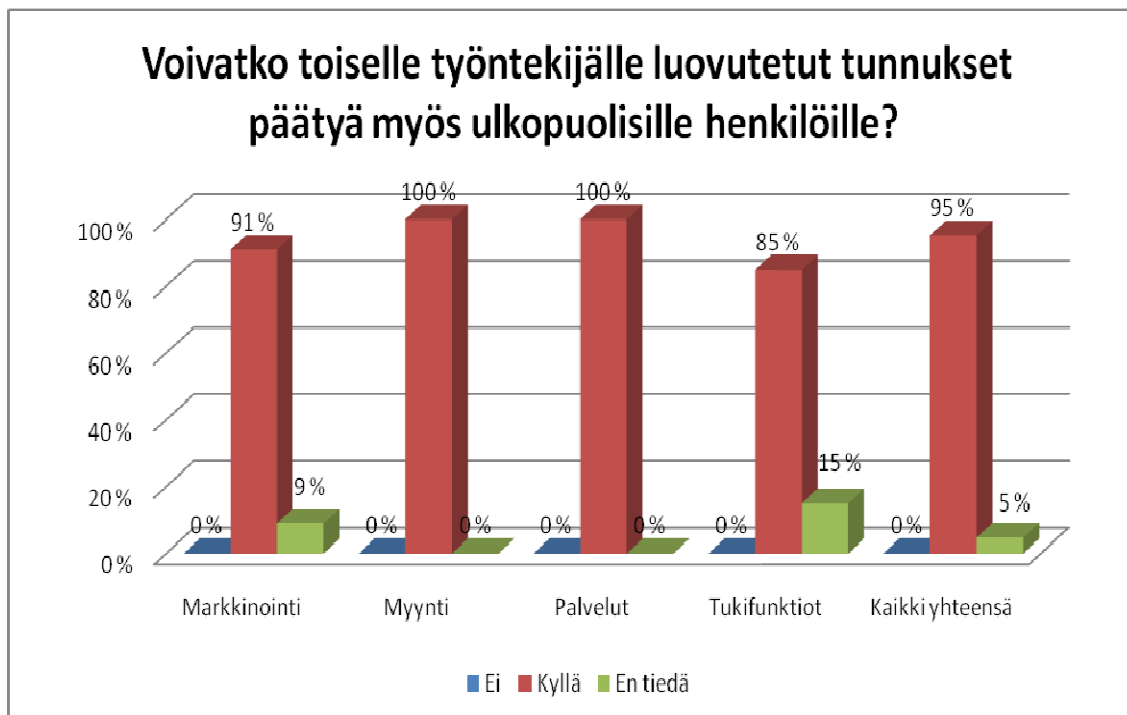
Kuvio 6: Salasanan luovutus

Voivatko toiselle työntekijälle luovutetut tunnukset päätyä myös ulkopuolisille henkilöille?

Tämä kysymys liittyy samaan osioon tietoturvaohjeistuksessa kuin edellinenkin kysymys. Tällä kysymyksellä haluttiin tietää vastaajien tietoturvatietämyksestä yleisemmällä tasolla. Jos omat käyttäjätunnuksensa luovuttaa toiselle työntekijälle, voivat ne päätyä mihin vain. Kaikki vastaajat olivat suurimmaksi osaksi samaa mieltä asiasta, lukuun ottamatta muutamaa ”En tiedä” -vastausta.

Markkinoinnin vastaajista 10 (91 %) vastasi ”Kyllä” ja yksi (9 %) ”En tiedä”. Myynnin kaikki 20 vastaajaa vastasivat ”Kyllä”. Samoin palveluiden 34 vastaajaa vastasivat kaikki tähän kysymykseen ”Kyllä”. Tukifunktioiden vastaajista 17 (85 %) vastasivat ”Kyllä” ja kolme (15 %) vastasi ”En tiedä”.

Kaikista vastaajista yhteensä 81 (95 %) vastasi ”Kyllä” ja neljä (5 %) vastasi ”En tiedä”.



Kuvio 7: Tunnuksien päätyminen ulkopuolisille

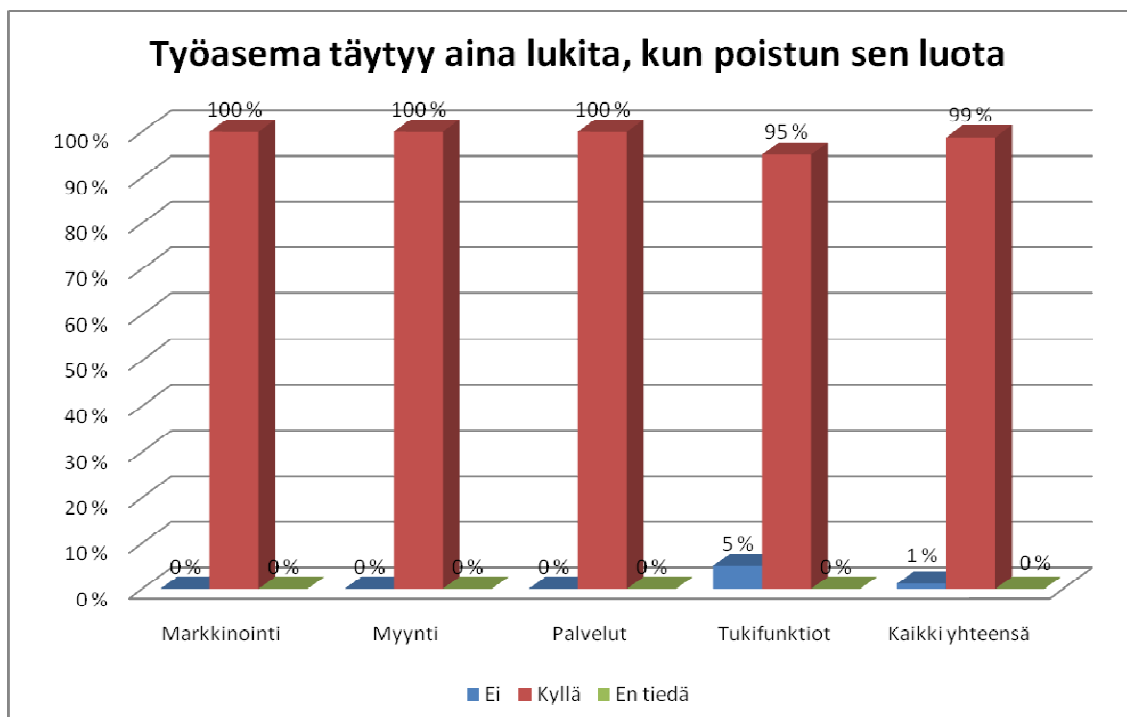
Työasema täytyy aina lukita, kun poistun sen luota

Tämä kysymys koskee tietoturvaohjeistuksen kohtaa, jossa määrätään lukitsemaan työasema aina kun se jätetään valvontaa vaille. Käytännössä siis aina, kun työntekijä poistuu työasemaltaan. Kohdassa mainitaan myös, että työasemaa ei saa säilyttää huolimattomasti. Kysymyksellä haluttiin selvittää vastaajien tietämystä tästä tietoturvaohjeistuksen kohdasta. Kuten vastauksista näkee, lähes jokainen vastaaja tiedostaa tämän osan ohjeistuksesta.

Kaikki markkinoinnin 11 vastaajaa vastasivat tähän kysymykseen ”Kyllä” ja niin tekivät myös myynnin 20 vastaajaa. Myös palveluiden kaikki 34 vastaajaa vastasivat ”Kyllä”.

Tukifunktioiden vastaajista 19 (95 %) vastasi tähän kysymykseen ”Kyllä” ja yksi (5 %) vastasi ”Ei”.

Kaikilta tasoilta yhteensä 84 (99 %) vastasi ”Kyllä” ja yksi (1 %) ”Ei”.



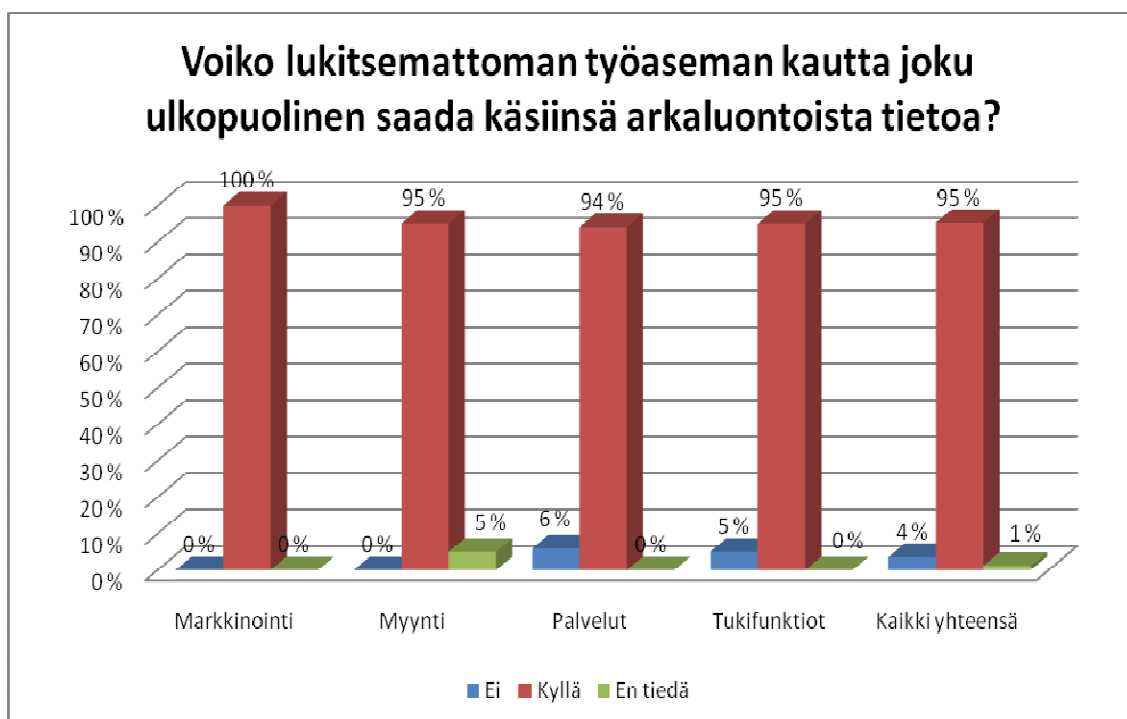
Kuvio 8: Työaseman lukitseminen kun poistun sen luota

Voiko lukitsemattoman työaseman kautta joku ulkopuolinen saada käsiinsä arkaluontoista tietoa?

Kysymys käsitteli pääpiirteissään samaa kohtaa, kuin edellinenkin kysymys. Tällä kysymyksellä haluttiin herättää vastaajaan oma tietoturvatietoisuus liittyen tietoturvaohjeistuksen tärkeyteen ja sen noudattamiseen. Yrityksen tiloissa käy jonkin verran myös ulkopuolisia henkilöitä ja he voisivat melko helposti päästä käsiksi lukitsemattomiin työasemiin ja niiden tietoihin. Vastauksista näkee, että suurin osa vastanneista pitää kysymyksessä käsiteltyä asiaa mahdollisena.

Kaikki markkinoinnin 11 vastaajaa olivat samaa mieltä ja he vastasivat ”Kyllä”. Myynnin vastaajista 19 (95 %) vastasi ”Kyllä” ja yksi (5 %) ”En tiedä”. Palveluiden vastaajista vastasi 32 (94 %) ”Kyllä” ja kaksi (6 %) ”Ei”. Tukifunktioiden vastaajista 19 (95 %) vastasi ”Kyllä” ja yksi (5 %) ”Ei”.

Kaikista toiminnoista vastasi yhteensä 81 (95 %) ”Kyllä”, kolme (4 %) ”Ei” ja yksi (1 %) ”En tiedä”



Kuvio 9: Voiko ulkopuolinen saada tietoa lukitsemattoman työaseman kautta

Saan kuunnella Internet-radiolähetystä yrityksen verkossa

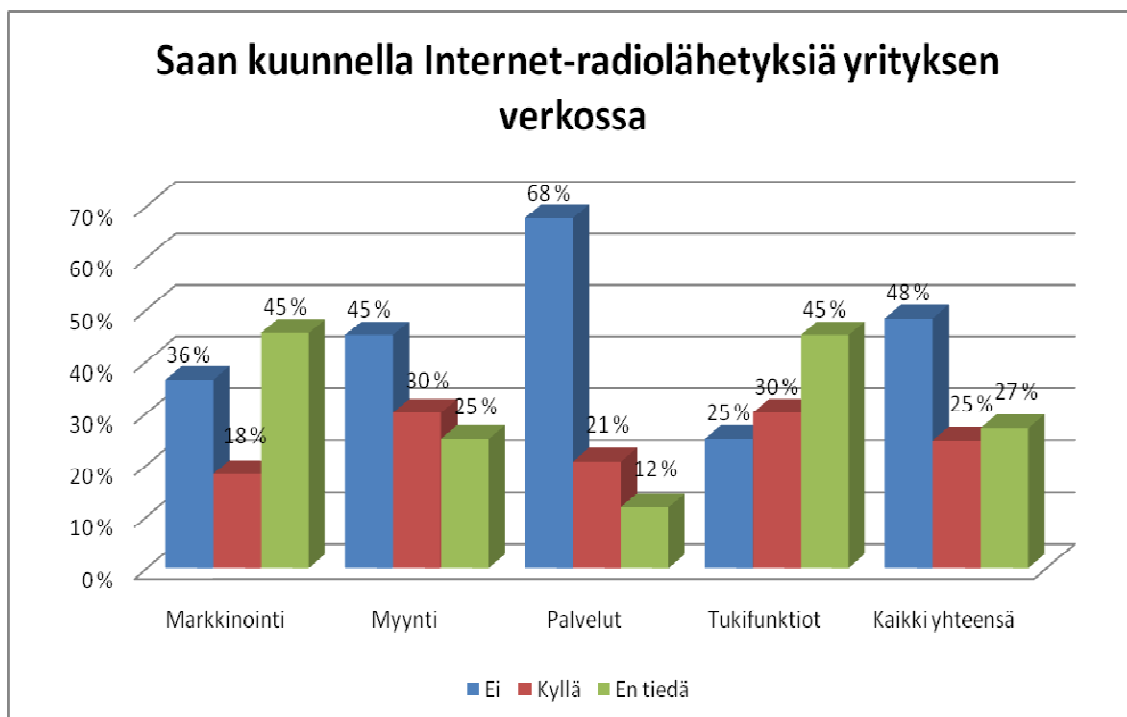
Kysymys käsitteli tietoturvaohjeistuksen kohtaa, jossa kielletään yrityksen verkon ylikuormittaminen tai suurien liiketoimintaan kuulumattomien tiedostomäärien siirtäminen. Esimerkkinä kerrotaan äänen tai kuvan suoratoisto. Käytännössä tämä tarkoittaa Internet-radiolähetysten kuuntelua tai suorien tv-lähetysten katselua yrityksen verkossa.

Kysymys oli ajankohtainen myös siksi, koska Internet-radiolähetystä on kuunneltu yrityksen verkossa aikaisemminkin.

Kuten vastauksista näkee, ei vastaajilla ollut aivan selkeää tietoa tästä asiasta. Suurin osa vastanneista kyllä näyttää tietävän tämän, mutta epätietoisuuttakin on paljon.

Markkinoinnin vastaajista neljä (36 %) vastasi ”Ei”, kaksi (18 %) ”Kyllä” ja 5 (45 %) ”En tiedä”. Myynnin puolelta 9 (45 %) vastasi ”Ei”, 6 (30 %) vastasi ”Kyllä” ja 5 (25 %) ”En tiedä”. Palveluiden vastaajista 23 (68 %) vastasi ”Ei”, 7 (21 %) ”Kyllä” ja neljä (12 %) ”En tiedä”. Tukifunktioiden puolelta 5 (25 %) vastasi ”Ei”, 6 (30 %) ”Kyllä” ja 9 (45 %) ”En tiedä”.

Kaikki toiminnot yhteenlaskettuna vastasi 41 (48 %) ”Ei”, 21 (25 %) ”Kyllä” ja 23 (27 %) ”En tiedä”.



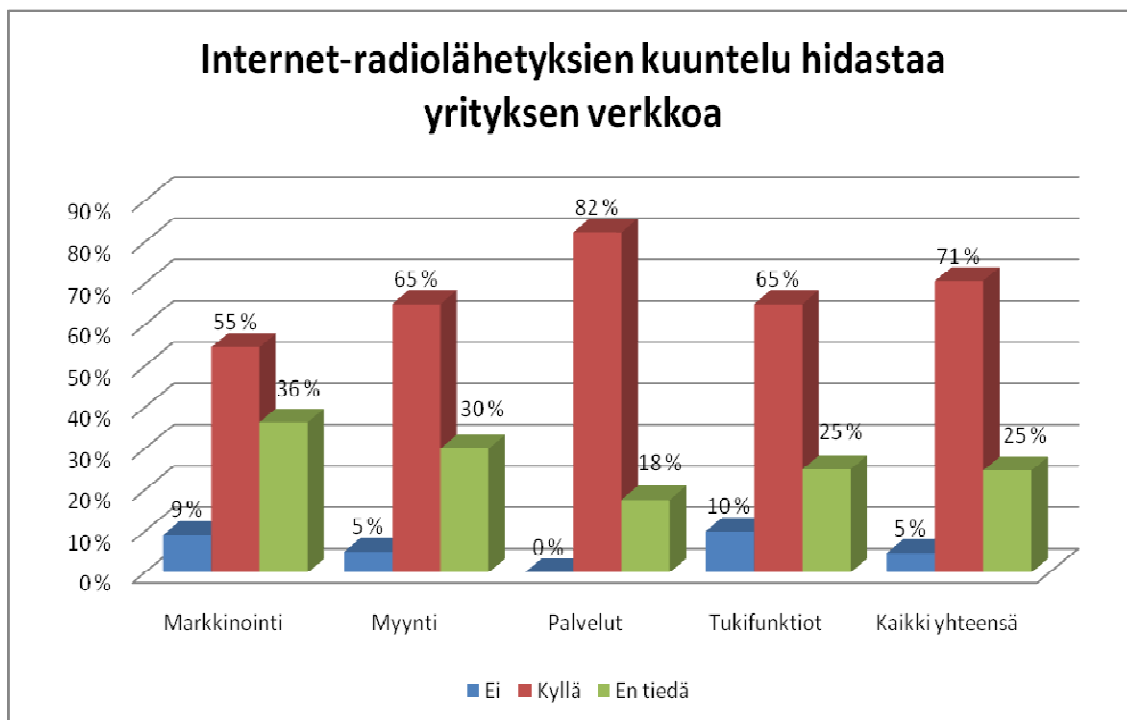
Kuvio 10: Internet-radiolähetysten kuuntelu

Internet-radiolähetysten kuuntelu hidastaa yrityksen verkkoa

Tämä kysymys käsitteli samaa kohtaa tietoturvaohjeistuksessa, kuin edellinenkin kysymys. Kysymyksellä pyrittiin selvittämään vastaajien tietämystä Internet-radiolähetysten kuuntelun vaikutuksista yrityksen verkkoliikenteen sujuvuuteen. Kysymys viittaa Internet-radiolähetysten kuuntelun haittavaikutuksiin ja verkkoliikenteen hidastumiseen kuuntelemisen myötä. Internet-radiolähetykset hidastavat yrityksen verkkoliikennettä paljon ja niiden kuuntelu onkin tämän takia usein kiellettyjä tietoturva- tai muissa ohjeistuksissa. Vastauksista näkee, että asia ei ole ollut aivan yksiselitteinen.

Markkinoinnin puolelta vastasi yksi (9 %) ”Ei”, 6 (55 %) ”Kyllä” ja neljä (36 %) ”En tiedä”. Myynnin vastaajista yksi (5 %) vastasi ”Ei”, 13 (65 %) ”Kyllä” ja 6 (30 %) ”En tiedä”. Palveluiden puolelta vastasi 28 (82 %) ”Kyllä” ja 6 (18 %) ”En tiedä”. Tukifunktioiden vastaajista kaksi (10 %) ”Ei”, 13 (65 %) ”Kyllä” ja 5 (25 %) ”En tiedä”.

Kaikista vastauksista yhteensä neljä (5 %) vastasi ”Ei”, 60 (71 %) ”Kyllä” ja 21 (25 %) ”En tiedä”.



Kuvio 11: Internet-radiolähetykset hidastavat yrityksen verkkoa

3.2 Yhteenveto

Kaiken kaikkiaan yrityksen henkilöstö näyttää tuntevan tietoturvaohjeistuksen sisällön melko hyvin. Suurimmat epätietoisuudet liittyvät Internet-radiolähetysten kuunteluun. Vastausmääräksi tuli lopulta 85 vastaajaa ja kysymykset lähetettiin 295 henkilölle, joten vastausprosentiksi muodostui 29 %. Tämä oli vähemmän kuin oli odotettu, mutta siihen oltiin kuitenkin tyytyväisiä. Kohderyhmäksi valittiin Helsingin toimipisteen henkilöstö, joka osoittautui toimivaksi vaihtoehdoksi. Koko yrityksen henkilöstön valinta olisi ollut turhaa, koska tutkittava joukko olisi kasvanut todella suureksi ja työlääksi tutkia.

Yritys X ei ollut ennen tehnyt vastaavanlaisia tutkimuksia, joten tälle tutkimukselle oli tarvetta yrityksen sisällä. Tutkimus tehtiin kvantitatiivisella menetelmällä sekä kyselylomakkeella, joka lähetettiin jokaiselle kohderyhmään kuuluvalle työntekijälle. Kyselylomakkeella oli tarkoitus selvittää henkilöstön tietoturvaohjeistuksen tietämyksen tasoa. Kysymysten analysoinnin jälkeen tehtiin kehitysehdotuksia liittyen tietoturvaohjeistukseen sekä yrityksen tietoturvaan yleisemmällä tasolla.

Yritys suhtautui tähän tutkimukseen hyvin ja tarvittaviin kysymyksiin sai helposti vastaukset. Yhteistyö sujui siis mainiosti, niiltä osin kuin sitä tarvittiin. Myös yrityksen edustajalta saatiin aina tarpeen vaatiessa apua sekä tarvittavia tietoja.

4 Kehittämissuhteet

Tutkimuksen mukaan yrityksen henkilöstö on suurimmaksi osaksi tietoinen yrityksen tietoturvaohjeistuksen sisällöstä. Suurimmat epävarmuudet löytyvät Internet-radiolähetysten kuuntelusta. Tämä oli ennalta-arvattavaa, koska yrityksessä on ollut tapauksia joissa Internet-radiolähetystä on kuunneltu koko työpäivän ja näin ylikuormitettu yrityksen sisäistä verkkoa. Seuraavissa kappaleissa kerron omia kehittämissuhteitani liittyen yrityksen tietoturvaohjeistukseen sekä tietoturvallisuuteen yleensä.

4.1 Äänen tai kuvan suoratoisto

Ensimmäinen kehittämissuhteitani koskee tietoturvaohjeistuksen kohtaa, jossa kielletään äänen ja kuvan suoratoisto. Tällä hetkellä kohdassa kielletään yrityksen verkon ylikuormittaminen tai suurien liiketoimintaan kuulumattomien tiedostojen siirtäminen. Esimerkkinä mainitaan äänen tai kuvan suoratoisto.

Mielestäni tähän esimerkki kohtaan voisi lisätä Internet-radiolähetysten kuuntelun, suorien tv-lähetysten katselun ja erilaisten suorien lähetysten katsomisen tai kuuntelun.

Lisäksi erityisesti Internet-radiolähetysten kuuntelun kiellosta voisi tehdä julisteen tai vastaavan tietoisuuden ja lisätä muutenkin yleistä tietoisuutta asiasta.

4.2 Ulkoiset tallennusvälineet

Tietoturvaohjeistukseen voisi lisätä kohdan, jossa kerrotaan miten ulkoisten tallennusvälineiden, kuten MP3-soittimien, ulkoisten kovalevyjen ja USB-muistitikkujen kanssa pitäisi toimia. Tietoturvaohjeistuksessa kyllä mainitaan ulkoiset tallennusvälineet, mutta niiden käytöstä ei kerrota sen enempää.

Tähän kohtaan voisi laittaa jonkin esimerkin. Esimerkki voisi olla vaikkapa seuraavanlainen: ”Muita kuin yrityksen omistuksessa olevia ulkoisia tallennusvälineitä ei saa liittää yrityksen verkkoon tai ICT-laitteisiin. Tämä tarkoittaa omia henkilökohtaisia ulkoisia tallennusvälineitä”

4.3 Vierailijat yrityksen tiloissa

Vierailijoihin suhtautumisesta yrityksen tiloissa ei ole minkäänlaista ohjetta yrityksen tietoturvaohjeistuksessa. Ohjeistukseen voisi lisätä kohdan joka käsittelee tätä aihetta.

Esimerkkinä vaikkapa:

”Kun tuot vieraita yrityksen tiloihin, varmistu aina että vierailija oleilee vain hänelle sallituissa tiloissa. Muista että sinä vastaat yrityksen sisälle päästämistäsi vierailijoista.

Jos näet yrityksen sisällä eksyneen vierailijan, ohjaa hänet oikeaan paikkaan.”

4.4 Tietoturvaongelmien ilmoitusvelvollisuus

Tietoturvaohjeistukseen voisi myös lisätä kohdan, jossa kehoitetaan työntekijöitä aina ilmoittamaan mahdollisista ongelmista tietoturvallisuudessa. Ilmoituksen tarvitsevia asioita voisivat olla tietokoneelta löytyneet virukset, haittaohjelmat, vakoiluohjelmat tai epäily edellä mainittujen tartumisesta tietokoneelle. Myös muista tietoturvallisuusongelmista ja rikkomuksista voitaisiin kehottaa ilmoittamaan.

4.5 Mistä voi epäillä tietokoneen saaneen haittaohjelmatartunnan

Tästä asiasta voisi tehdä kokonaan oman ohjeen tai sen voisi suoraan lisätä tietoturvaohjeistukseen. Tämä ohje voisi sisältää myös, että mitä täytyy tehdä jos epäilee haittaohjelmatartuntaa. Ohje voisi sisältää seuraavaa: Tartunnan oireet voivat olla tietokoneen äkillinen hidastuminen tai outojen varoitusten ilmestyminen tietokoneen näytölle. Jos epäilee tartuntaa, ei pidä hätiköidä. Tietokonetta ei myöskään täydy sulkea. Jos tietokoneen näytölle on ilmestynyt varoituksia, pitää kirjata ylös mitä niissä lukee. Ota tämän jälkeen yhteyttä ICT-osastoon. (VAHTI 5/2003, 20).

4.6 Tietoturvakäytännön suomentaminen

Yrityksellä on tietoturvakäytäntö, mutta vain osa siitä on suomeksi ja helposti löydettävissä. Ehdotukseni onkin suomentamattomien tietoturvakäytäntöjen kääntäminen suomeksi ja niiden siirtäminen sellaiseen paikkaan yrityksen sisäverkossa, josta ne voi jokainen työntekijä helposti löytää. Myös nykyinen tietoturvaohjeistus voisi olla helpommin saatavilla.

4.7 Henkilöstön lisäkoulutus

Henkilöstön lisäkoulutus tietoturvan saralla on aina kannattavaa. Olipa tietoturvaohjeistus tai tietoturvakäytäntö miten hyvä tahansa, se ei korvaa henkilöstön koulutusta. Hyvä tietoturvakoulutus tekee henkilöstöstä tietoisempaa tietoturvan saralla ja näin edesauttaa tietoturvaoh-

jeistuksen ja tietoturvapoliittikan noudattamista sekä parantaa yrityksen yleistä tietoturvaa suuresti.

4.8 Tietoturvaohjeistuksen rinnalle lisäohjeistus

Nykyisen tietoturvaohjeistuksen rinnalle voisi laatia ytimekkään, vain pääkohdat sisältävän ohjeistuksen tai julisteen tyyppisen tietoiskun. Näin tärkeimmät kohdat tietoturvaohjeistuksesta tulisivat selville. Näitä julisteita tai tietoiskuja laitettaisiin jokaiseen kerrokseen, josta ne olisivat helposti nähtävissä. Tällä tavalla ei välttämättä tarvitsisi joka kerta avata koko tietoturvaohjeistusta, vaan työntekijä voisi katsoa mieltä askarruttavasta asiasta suoraan julisteesta tai taulusta.

Yrityksessä on kyllä nykyisin julisteita ja tauluja seinillä muistuttamassa tietoturvasta, mutta ne tulevat suoraan ulkomaisten toimipisteistä. Tämä juliste tai ohjeistus voisi olla laadittu vain Suomen toimipisteille ja näin siihen saataisiin ajankohtaisempia aiheita sekä omakohtaisempia käsitteitä. Alla olevissa luvuissa kerron tämän tyyppistä ytimekkäistä tavoista kertoa tietoturvasta.

4.9 Muistilista tietoturvasta

Tietoturvasta yleisemmällä tasolla voisi tehdä pienen muistilistan, jossa kerrotaan tietoturvasta ja listataan hyviä käytäntöjä liittyen tietoturvaan. Tämän tyyppinen muistilista löytyy muun muassa VAHTI Käyttäjän tietoturvaohjeesta 5/2003.

Lista voisi olla tälle yritykselle esimerkiksi seuraavanlainen:

1. Vastuu tietoturvalisesta työympäristöstä kuuluu kaikille yrityksessä työskenteleville
2. Seuraa tietoturvatiedotteita, tutustu tietoturvaohjeistukseen ja osallistu tietoturvakoulutuksiin. Näin parannat omalta osaltasi koko yrityksen tietoturvalisuu
3. Älä luovuta henkilökohtaista käyttäjätunnusta ja salasanaasi kenellekään
4. Vaihda salasanasasi riittävän usein ja varsinkin silloin, jos luulet sen päätyneen jonkun muun henkilön tietoon
5. Älä asenna ohjelmistoja tai muuta ohjelmistojen asetuksia, jos se ei kuulu työnkuvaasi
6. Kun käytät yrityksen sähköpostia tai olet verkossa yrityksen ICT-laitteella, muista aina että edustat yritystä

7. Lukitse aina työasemasi, kun poistut sen luota

8. Ilmoita aina huomaamistasi tietoturvaongelmista ja rikkomuksista ICT-osastolle

9. Älä aiheuta turhaa kuormitusta yrityksen verkkoliikenteeseen esimerkiksi Internet-radiolähetyksien kuuntelulla tai suurien liiketoimintaan kuulumattomien tiedostojen siirrolla

4.10 Lyhyet tietoiskut tietoturvasta

Tietoturvasta ja sen tarpeellisuudesta voisi tehdä omat dokumenttinsa, josta ne olisivat helpposti ja nopeasti luettavissa. Dokumentit voisivat olla yrityksen sisäverkossa ja julisteena käytävillä. Dokumentit voisivat kertoa mitä tietoturva on ja miksi tietoturva on tärkeää. Alla muutama esimerkki tietoiskuista.

4.10.1 Mitä tarkoittaa tietoturvallisuus?

Tietoturvallisuus on pieniä tekoja osana jokapäiväistä toimintaa. Toimiva tietoturva on osa yrityksen kulttuuria, jolloin kaikilla on ymmärrys tietoturvasta ja kaikki työskentelevät sen mahdollistamiseksi ja ylläpitämiseksi. (Laaksonen, Nevasalo & Tomula 2006, 17.)

Tietoturvallisuuden tarkoituksena on taata tiedon, tietojärjestelmien, ja palveluiden asianmukainen suojaus. Suojaus tapahtuu käytännössä teknisillä, hallinnollisilla ja muilla toimenpiteillä. Riskit jotka liittyvät niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen täytyvät olla asianmukaisesti hallinnassa. Näitä riskejä ovat mm. luonnonmullistukset, laitteistoviat, ohjelmistoviat, tahalliset teot tai tapaturmaiset teot. Tietoturvallisuus tarkoittaa myös, että tieto ja tietojärjestelmät ovat vain niiden henkilöiden saatavilla, jotka ovat valtuutettuja käyttämään niitä. (VAHTI 5/2003, 8; VAHTI 4/2009, 8-9.)

Tietoturvalla on kolme pääkäsitettä, jotka ovat seuraavanlaisia:

1. Luottamuksellisuus tarkoittaa että tiedot ovat vain niiden henkilöiden käytössä, joilla niihin on oikeus. Ulkopuoliset eivät saa käsiinsä tietoja.
2. Eheyys tarkoittaa että tiedot ovat luotettavia ja niitä eivät ole ulkopuoliset päässeet muokkaamaan tai poistamaan.
3. Käytettävyys tarkoittaa että tiedot ovat oikeutettujen henkilöiden käytössä juuri tarvittavaan aikaan.

4.10.2 Miksi tietoturva on tärkeää?

Yrityksen toiminta edellyttää tietoa ja tietotekniikkaa. Valtaosa tiedoista on sähköisessä muodossa tietokoneilla tai tietoverkossa. Tietoturvallisuus suojaa näitä tietoja ja samalla yrityksen toiminnan jatkuvuutta. (VAHTI 5/2003, 9.)

Yrityksessä käsitellään paljon luottamuksellista materiaalia kuten taloustietoja, henkilötietoja ja julkaisemattomien tuotteiden tuotetietoja ja kuvia. Ilman tietoturvaa, nämä tiedot olisivat helposti saatavilla ulkopuolisille.

4.11 Uusia tutkimuksia

Tietoturvallisuuden tietoisuudesta voisi mielestäni tehdä yrityksen sisällä useampiakin tutkimuksia. Tulevat tutkimukset voisivat olla yksilöhaastatteluun tehtäviä kvalitatiivisia tutkimuksia sekä tämän tutkimuksen tyyppisiä kvantitatiivisia kyselylomaketutkimuksia. Esimerkiksi yksilöhaastatteluun voitaisiin aina valita jonkin osaston esimiesasemassa oleva työntekijä tai vastaava henkilö joka tietäisi juuri sen osaston asioista. Näin saataisiin paljon tarkempaa tietoa tietoturvallisuuden tietoisuudesta ja ohjeiden noudattamisesta.

Kvantitatiiviset tutkimukset voisivat olla vaikkapa kerran vuodessa toistettavia samankaltaisia tutkimuksia kuin tämä tutkimus.

Tällaisten tutkimusten avulla saataisiin henkilöstön tietoturvatietoisuutta paremmaksi, sekä saataisiin selville yleisimmät yrityksen tietoturvaongelmat.

5 Tutkimuksen luotettavuus

Tutkimuksen luotettavuudella tarkoitetaan tutkimusmenetelmän kykyä selvittää, mitä sillä oli tarkoitus selvittää. (Tutkimuksen validiteetti 2007). Luotettavuus tarkoittaa myös, että tutkimuksen tulokset ovat toistettavissa. Tutkimuksen luotettavuutta voi haitata huolimattomuudesta johtuneet virheet, joita voi tapahtua aineiston keruussa, otannan määrittämisessä, mittauksen ajankohdassa tai analysoinnissa. (Saukkonen; Paasonen 2008.)

Kun aiheena on tietoturva tai jokin muu melko arka aihe, ei edes anonymiteetin lupaaminen välttämättä takaa totuudenmukaisia vastauksia. Vastajaat voivat luulla, että vastaukset voidaan kuitenkin jollain tavalla yksilöidä ja jäljittää tiettyyn henkilöön. Myös ihmisten miellyttämishalu voi väärentää vastauksia ja vastaja voi helposti valita sellaisen vaihtoehdon, jonka luulee miellyttävän tutkimuksen tekijää. Myös kysymysten väärinymmärtämisellä on suuri rooli tutkimuksen luotettavuuden arvioinnissa. Näistä asioista huolimatta, voidaan kuitenkin olettaa, että tähän tutkimukseen vastanneet henkilöt antoivat totuudenmukaisia vastauksia.

Oletus johtuu siitä, että tutkimus oli täysin anonyymi ja kaikki vastanneet pystyivät vastaamaan tutkimukseen nimettömästi. Tutkimukseen vastaaminen oli täysin vapaaehtoista ja mitään pakotteita vastaamiseen ei ollut, tämä osaltaan auttoi tutkimuksen luotettavuuden parantamisessa. Vastajille myös tiedotettiin tutkimuksen tarkoituksesta ja mihin heidän vastauksiaan käytetään. (Saukkonen.)

Vastausvaihtoehdoiksi annettiin Kyllä, Ei tai En tiedä. ”En tiedä” -vaihtoehdon kohdalla piti miettiä tuloksien oikeellisuutta. Jos ”En tiedä” -vaihtoehto olisi jätetty pois, olisivat vastauksien tulokset oletettavasti vääristyneet huomattavasti tai vastausprosentti tippunut reilusti. ”En tiedä” -vastausvaihtoehdon lisäämiseen päädyttiin yhdessä yrityksen edustajan kanssa.

Kyselylomakkeen luotettavuus pyrittiin saamaan mahdollisimman korkeaksi. Apuna käytettiin yrityksen edustajaa konsultoimassa sekä vastajille mahdollisimman tuttua kieltä. Myös lomakkeen rakenne laitettiin sellaiseen muotoon, että vastaaminen oli helppoa ja nopeaa. Luotettavuutta pyrittiin nostamaan myös siten, että yhdessä kysymyksessä kysyttiin kerralla vain yhtä asiaa. Ainoastaan vastauslomakkeen kysymysten väärinymmärtämistä ei pystytty ennalta koimaan tai ennaltaehkäisemään. Lomaketta myös muokattiin yrityksen edustajan sekä ohjaajien avustuksella ja näin sen luotettavuutta pyrittiin parantamaan.

Tutkimuksessa käsiteltiin tietoturvaohjeistuksen tietämystä ja kysymykset laadittiin sen pohjalta. Vastajien melko suuresta määrästä johtuen tutkimuksen tuloksia tietoturvaohjeistuksen tietämyksen tasosta voidaan pitää melko luotettavina ja suuntaa antavina.

Tämän tutkimuksen avulla voi yritys kehittää tietoturvaohjeistusta ja yleistä tietoturvaa paremmaksi. Olen myös itse ehdottanut joitain tärkeimpiä muutoksia ja parannusehdotuksia yrityksen tietoturvaan.

6 Johtopäätökset

Tutkimuksen perusteella voidaan todeta, että yrityksen henkilöstö tuntee tietoturvaohjeistuksen melko hyvin. Tämä ei kuitenkaan tarkoita, ettei tietoturvaohjeistusta voisi parantaa ja muutenkin tietoturvasuutta kohentaa yrityksen sisällä. Suurimmat epätietoisuudet vastajien joukossa liittyvät Internet-radiolähetysten kuunteluun. Kaikki muut tietoturvaohjeistuksen kohdat näyttävät olevan melko hyvin tiedossa.

Mielestäni yrityksen tietoturvaohjeistus on tällä hetkellä suhteellisen hyvä ja tarvitsisi vain muutamia muutoksia. Ohjeistukseen voisi lisätä tarkempia kuvauksia jo käsitellyistä aiheista, esimerkkinä vaikkapa Internet-radiolähetysten kuuntelun kiellon ja tarkempia ohjeita muistitikkujen ja ulkoisten kovalevyjen käyttöön. Myös tällä hetkellä englanniksi olevat tietoturva-

käytännöt olisi hyvä suomentaa ja laittaa helpommin saataville. Myös tietoturvaohjeistuksen aihealueita olisi hyvä selkeyttää ja tehdä helpommin tulkittaviksi sekä ymmärrettäviksi. Varsinkin Internet-radiolähetyksien kuuntelun kiellosta voisi viestittää paremmin, kuten tutkimuksen tuloksista käy ilmi.

Kaiken kaikkiaan tutkimus onnistui suhteellisen hyvin. Vastauksia olisi voinut tulla enemmän, mutta sähköpostikyselyissä tällainen vastausmäärä on melko normaali. Olen kuitenkin tyytyväinen näinkin moneen vastaukseen. Tutkimus sujui myös melko lailla suunnitelmien mukaan, tosin vastausten lähettämisen aikataulu hieman venyi ja vastausaikaa jouduttiin tästä syystä lyhentämään.

6.1 Uudet tutkimukset

Suosittelen että yritys tekisi tietoturvaan liittyviä tutkimuksia jatkossakin. Tästä olisi yritykselle paljon hyötyä ja se parantaisi yrityksen tietoturvaa huomattavasti. Yritys voisi tehdä joka vuosi tämän tutkimuksen tyyppisen tietoturvakyselyn, jolla seurattaisiin henkilöstön tietoturvaohjeistuksen tietoisuuden tasoa. Myös tarkempia tutkimuksia olisi hyvä tehdä, jossa tiettyä osaa henkilökunnasta haastateltaisiin tutkimukseen. Haastateltavat henkilöt voitaisiin valita jokaiselta osastolta, näin saataisiin hyvä kuva yrityksen jokaisen osaston tietoturvatietämyksestä. Kyseiset henkilöt olisi hyvä valita tarkkaan ja kysyä heiltä esimerkiksi kehitysehdotuksia yrityksen tietoturvallisuuteen sekä sen toimivuuteen liittyen.

Tutkimukset voitaisiin tehdä joka vuosi tai joka toinen vuosi, riippuen yrityksen yksilöllisistä tarpeista ja mahdollisista muutoksista tietoturvaohjeistuksiin ja politiikkoihin.

Tietoturvatietoisuuden tutkimisesta on hyötyä yrityksille, koska näin saadaan selville henkilöstön tietoisuutta tietoturvaohjeistuksista ja politiikoista. Tutkimukset ovatkin tarpeellinen osa hyvää tietoturvaa. Säännöllisesti tehtynä tutkimukset myös viestittävät henkilöstölle tietoturvallisuuden tärkeydestä ja ne antavat heille vaikutusmahdollisuuksia siihen. Yrityksen hyvä tietoturvallisuus käsittääkin säännölliset tutkimukset liittyen tietoturvatietoisuuteen.

Lähteet

Empiiriset aineistot ja analysoinnin kysymykset. Tampereen yliopisto. Viitattu 04.11.2010
<http://www.uta.fi/laitokset/hoito/wwwoppimateriaali/luku5a.html>

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Uudistettu painos.
Helsinki: Tammi.

IT-Grundschutz Manual 2005. Federal Office for Information Security. Viitattu 15.01.2011
https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutz/catalogues_node.html

Laaksonen, M., Nevasalo, T., & Tomula, K. 2006. Yrityksen Tietoturvakäsikirja.
Helsinki: Oy Nordprint Ab.

Paasonen E. 2008. Mittaaminen: Mittarin Luotettavuus. Viitattu 12.01.2011
<http://www.fsd.uta.fi/metelmaopetus/mittaaminen/luotettavuus.html>

Puhakainen, P. 2006. Tietoturvaohjeet paperipinosta käytännöksi. Viitattu 17.10.2010
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20061215Valtio/04_Puhakainen_15.12.2006.pdf

Richardson, R. 2008. Computer Crime and Security Survey. Viitattu 01.11.2010
<http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf>

Saukkonen P. Tutkielmanteon tukisivut. Viitattu 12.01.2011
http://www.valt.helsinki.fi/staff/psaukkon/tutkielma/Tutkimusasetelma.html#Kvalitatiivinen_ja_kvantitatiivinen

Saukkonen P. Tutkielmanteon tukisivut. Viitattu 12.01.2011
http://www.valt.helsinki.fi/staff/psaukkon/tutkielma/Tutkimusmenetelmat.html#Validius_ja_reliaabelius

Slade, R. 2006. Dictionary of Information Security.
Rockland, MA, USA: Syngress.

VAHTI 4/2009. Information Security Instructions For Personnel. Ministry of finance.
Helsinki: Edita Prima Plc.

VAHTI 5/2003. Käyttäjän tietoturvaohje. Valtionvarainministeriö.
Helsinki: Edita Prima Oy.

VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. Valtionvarainministeriö.
Helsinki: Edita Prima Oy.

Virtuaaliammattikorkeakoulu. Kyselyyn perustuvan tutkimuksen suorittaminen. Viitattu 4.11.2010
<http://www.amk.fi/opintojaksot/0709019/1193463890749/1193464131489/1194289345955/1194290010211.html>

Virtuaaliammattikorkeakoulu. Tutkimuksen validiteetti. Viitattu 13.12.2010
<http://www.amk.fi/opintojaksot/0709019/1193463890749/1193464185783/1194413809750/1194415367669.html>

Kuvat ja Kuviot

Kuvio 1: Kysymyslomake	13
Kuvio 2: Vastausprosentit yrityksen toimintojen kesken.....	15
Kuvio 3: Vertaisverkkosovellusten lataaminen Internetistä	16
Kuvio 4: Haittaohjelmat Internetistä ladatuista ohjelmista.....	17
Kuvio 5: Yrityksen verkkoon murtautuminen asennettujen ohjelmien avulla.....	18
Kuvio 6: Salasanan luovutus	19
Kuvio 7: Tunnuksien päätyminen ulkopuolisille	20
Kuvio 8: Työaseman lukitseminen kun poistun sen luota	21
Kuvio 9: Voiko ulkopuolinen saada tietoa lukitsemattoman työaseman kautta.....	22
Kuvio 10: Internet-radiolähetysten kuuntelu	23
Kuvio 11: Internet-radiolähetykset hidastavat yrityksen verkkoa	24

Liitteet

Liite 1: Kysymykset

1. Oman organisaatiosi päätaso?

Myynti, Markkinointi, Pavelut, Tukifunktiot

2. Onko vertaisverkkosovellusten lataaminen Internetistä hyväksyttävää yrityksen omistamalla ICT-laitteella?

Kyllä - Ei - En tiedä

3. Voiko Internetistä lataamieni ohjelmien mukana tulla haittaohjelmia yrityksen laitteille?

Kyllä - Ei - En tiedä

4. Voiko asentamieni sovellusten ansiosta joku ulkopuolinen murtautua yrityksen verkkoon?

Kyllä - Ei - En tiedä

5. Onko sallittua luovuttaa oma käyttäjätunnus ja salasana toiselle työntekijälle?

Kyllä - Ei - En tiedä

6. Voivatko toiselle työntekijälle luovutetut tunnukset päätyä myös ulkopuolisille henkilöille?

Kyllä - Ei - En tiedä

7. Työasema täytyy aina lukita, kun poistun sen luota

Kyllä - Ei - En tiedä

8. Voiko lukitsemattoman työaseman kautta joku ulkopuolinen saada käsiinsä arkaluontoista tietoa?

Kyllä - Ei - En tiedä

9. Saan kuunnella Internet-radiolähetyksiä yrityksen verkossa

Kyllä - Ei - En tiedä

10. Internet-radiolähetyksien kuuntelu hidastaa yrityksen verkkoa

Kyllä - Ei - En tiedä

Liite 2: Tietoisku Internet-radiolähetyksien kuuntelusta

Tiesitkö, että...

Internet-radiolähetyksien
kuuntelu ei ole sallittua
yrityksen verkossa

Internet-radiolähetyksien kuuntelu
hidastaa huomattavasti yrityksen
verkkoliikennettä

Hidastunut verkkoliikenne haittaa
yrityksen liiketoiminnan sujuvuutta

Älä siis kuuntele Internet-radiolähetyksiä
työpaikalla