LAUREA

Tietoturvatietoisuuden kartoitus yrityksen eri-koisosastoilla

. . . . . .

Piirainen, Henrik

2013 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvatietoisuuden kartoitus yrityksen erikois-osastoilla

Piirainen, Henrik
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2013

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

Piirainen, Henrik

Tietoturvatietoisuuden kartoitus yrityksen erikoisosastoilla

Vuosi 2013 Sivumäärä 56

Tämän opinnäyte työn tarkoituksena oli tutkia tietoturvallisuuden tilaa kohdeorganisaatiossa sekä löytää menetelmiä, joilla tietoturvallisuutta voidaan kehittää. Kohdeorganisaatio on Danske Bankin asiakas- ja tekninen tuki, mikä sijaitsee Pohjois-Haagassa Helsingissä. Tavoitteena oli löytää tekijät, jotka ovat tärkeimpiä kohdeorganisaation työntekijöiden tietoturvatietoisuuden kannalta. Aihe rajattiin käsittelemään tiedon, työssä käytettävien laitteiden sekä salasanojen ja käyttäjäoikeuksien hallintaa ja käyttöä.

Teoriaosuudessa kartoitetaan tekijät, joista tietoturvatietoisuus muodostuu. Teoriaosuus koostuu työn kannalta tärkeimmistä käsitteistä, kuinka tietoturva toteutetaan kohdeorganisaatiossa sekä tietoturvauhista ja -riskeistä. Kohdeorganisaation tietoturvatietoisuutta käsitellään teorian sekä organisaation tietoturvapolitiikan pohjalta.

Tutkimuksen tiedonkeruumenetelmänä käytettiin kyselytutkimusta. Kyselytutkimuksen tarkoitus oli kartoittaa vastaajien tietoturvatietoisuuden nykytilaa, sekä kerätä näkökulmia sen kehittämiseen. Kyselytutkimus sopi hyvin tähän tutkimukseen, sillä menetelmällä voitiin kysyä kohderyhmältä monia asioita koskien tietoturvallisuutta.

Tutkimuksessa löydettiin paljon kohderyhmän tietoturvatietoisuuteen liittyviä puutteita ja epäkohtia sekä kehittämisideoita, joita voidaan helposti omaksua päivittäisessä työskentelyssä. Tutkimuksesta saadut tiedot tarjoavat toimeksiantajalle ajatuksia tietoturvallisuuden kehittämiseksi.

Asiasanat tietoturva, tietoturvatietoisuus, tietoturvapolitiikka, tietoturvaohje, tietoturvakartoitus

LaureaUniversity of Applied Sciences **Abstract**
Laurea Leppävaara
Business Information Technology Program

Piirainen, Henrik

Information security awareness survey in companies special units

Year 2012 Pages 56

The purpose of this was to study the state of information security in the target organization and find ways to improve information security. The target organization is Danske Bank customer and technical support, which are located in Northern Haaga in Helsinki. The goal was to pinpoint the factors, which are most important to target organization's employee awareness of information security. This thesis focused on handling and usage of information, equipment and programs, passwords and user rights that are used in daily tasks.

The theoretical part describes the essential factors that contribute information security awareness. The theoretical part consists of most important terms, how information security is implemented in target group and about threats and risks of information security. Target group's information security awareness is discussed from the theory and organization's information security policy.

The data for this study was collected by poll survey. The purpose of this poll survey was to examine the current state of target group's information security awareness and collect perspectives to improve it. Poll survey is suitable with this survey, because this method allows collecting large amount of data concerning information security awareness.

The survey brought up many lacks and faults in target group's information security awareness and development ideas, which can be easily implemented in daily tasks. The results offer valuable information for the client on how to develop information security.

Key words information security, information security awareness, information security policy, information security guide, information security survey

Sisällys

1 Johdanto

Tietoturvallisuus on osa organisaation liiketoimintaa. Organisaatiolle tiedon turvaaminen on yksi menestymisen edellytys. Tietoturvassa ei ole kyse vain tietotekniikasta, vaan henkilöstön työskentelytavoista. Kaikkien tulee tietää, kuinka tietoturvallisuus voidaan taata yrityksessä. Yrityksellä on myös velvollisuus osan tiedon turvallisuus. Hyvä tietoturva ei välttämättä vaadi isoja investointeja, vaan pienikin parannus ja panostus voi hyödyntää liiketoimintaa. (Yrityksen tietoturvaopas 2012)

Kiireisessä ja tuottavuutta tavoittelevassa työmaailmassa helposti unohtuu tietoturvallisuuden tärkeys ja näin tietoturvatietoisuus ei välttämättä ole tarvittavalla tasolla yrityksen henkilöstön keskuudessa. Tässä opinnäytetyössä aioin keskittyä tietoturvallisuuteen vaikuttaviin asioihin ja tarkastelen näiden asioiden yhteyttä henkilöstön tietoturvatietoisuuteen. Uskon vahvasti, että tietoturvallisuuden merkitys sähköisessä viestinnässä ja yritysmaailmassa korostuu merkittävästi tulevaisuudessa.

Valtiovarainministeriön henkilöstön tietoturvaohjeen mukaan tietoturvallisuus perustuu normiohjaukseen ja lainsäädäntöön. Vastuu tietoturvallisuudesta ja siihen liittyvä osaaminen kuuluu jokaiselle organisaation henkilöstölle.(VAHTI 10/2006, 9.)

Toimeksiantajanani toimi Danske Bankin verkkopankin asiakastuki ja tekninen tuki, joka sijaitsee Pohjois-Haagassa. Kohde on erittäin suotuisa, koska työskentelen organisaatiossa ja tunnen hyvin organisaation toimintatavat ja käytänteet. Näen verkkopankin asiakastuen ja teknisen tuen olevan hyvä ja mielenkiintoinen kohde tietoturvatietoisuustutkimukselle, koska osastoilla käytetään eniten tietosuojaa vaativia teknillisiä laitteita ja ohjelmia kuin missään muualla organisaatiossa. Osastoilla käsitellään myös paljon pankkisalaisuuden alaista tietoa.

1.1 Tavoite

Tämän opinnäytetyön tavoite on kartoittaa tietoturvatietoisuuden tilaa kohdeorganisaation verkkopankin asiakas- ja teknisessä tuessa. Työn tarkoitus on kartoittaa miten työntekijät ovat omaksuneet organisaation tietoturvapolitiikan sekä -ohjeistuksen ja kuinka tietoturvaa sovelletaan omissa työtehtävissä. Tässä työssä keskitytään niihin tietoturvan osa-alueisiin, jotka ovat kohderyhmän kannalta oleellisempia. On havaittu, että tietoturvapolitiikka ja sen käytänteet eivät ole näkyvissä päivittäisessä työskentelyssä. Hyvänä esimerkkinä tästä, toimeksiantajani ei edes itse tiennyt missä organisaation tietoturvapolitiikka sijaitsee. Alustavien kyselyiden perusteella moni työntekijä ei tiennyt että yrityksellä on tietoturvapolitiikka tai

erillistä ohjeistusta asiaan. Tiimin esimiehellä ei usein riitä aikaa työkiireiden ja osaston johtamisen lomassa tarkastella työntekijöiden tietoturvatietoisuuden tilaa. Työn tavoitteisiin on päästy, jos pystyn tutkimieni asioiden perusteella tekemään sellaisia havaintoja, joista on hyötyä kohdeorganisaatiolle ja niiden perusteella pystyn suunnitella ehdotuksia turvallisuuden kehittämiseksi. Aiheen tutkiminen mahdollistaa työntekijän kuulemista tietoturvallisuudesta ja pystyn pohtimaan kohderyhmän tietoturvatietoisuutta.

1.2 Aiheen rajaus

Työn aiheeksi rajattiin organisaation tietoturvaohjeistusta ja -politiikkaa koskevat alueet. Keskustelimme toimeksiantajan kanssa, mitkä alueet olisi tärkeä kartoittaa ja mihin tietoturvallisuuden alueisiin kohderyhmän työtekijät voivat vaikuttaa työpaikalla. Työn rajaukseen käytin pohjana myös Valtionvarainministeriön VAHTI -henkilöstön tietoturvaohjetta. Työssä keskityn seuraaviin osa-alueisiin:

- Tiedon käyttö, säilyttäminen sekä tuhoaminen
- Tietokoneiden ja mobiili -laitteiden käyttö sekä siirrettävät mediat
- Salasanat ja käyttöoikeudet
- Internet ja sähköposti

Rajaus perustuu tulkintaan tietoturvallisuudesta, jonka toimeksiantaja kokee tärkeimpänä. Toimeksiantaja halusi myös käsityksen siitä, mihin tietoturva-asioihin organisaatiossa keskitytään ja mitkä asiat ovat tärkeitä huomioida ja korostaa. Rajaukseen vaikutti myös se, että uskon saavani selkeitä vastauksia ja mielipiteitä kohderyhmän työntekijöiltä tutkimustyötä tehdessäni.

Opinnäytetyö on rajattu koskemaan Danske Bankin verkkopankin asiakas- ja teknistä tukea, jossa työskentelee yhteensä 20 henkilöä. Kohde sopii mainiosti, koska työskentelen itse asiakastuessa ja tiedän hyvin teknisentuen työnkuvan ja työtavat. Kohde on myös otollinen, sillä näillä osastoilla käytetään enemmän erilaisia IT-laitteistoja, järjestelmiä ja tietoverkkoja kuin muualla organisaatiossa.

Opinnäytetyön alussa käsittelen keskeisiä käsitteitä, joista tietoturva ja tietoturvatietoisuus muodostuu. Tutkimuksen teoreettinen viitekehys pohjautuu Valtionvarainministeriön VAHTI ohjeistuksiin, IT-Grundschutz-Catalogues 2005:teen sekä Mika Laaksosen Yrityksen tietoturvakäsikirjaan. Teoriaosuuden jälkeen kartoitin kohderyhmän tietoturvariskit, joiden pohjalta tein kvantitatiivisen tutkimuskyselyn työntekijöille.

1.3 Tutkimusongelma

Tutkimusongelmani on selvittää Danske Bankin verkkopankin tukiosastojen työntekijöiden tietoturvallisuustietoisuuden taso. Osastojen uusille työntekijöille ja osalle osastoilla pidempään työssä olleille ei ole ehditty järjestää erillistä koulutusta organisaation tietoturvallisuudesta. Alustavan kyselyn perusteella monikaan työntekijä ei tiennyt mistä organisaation tietoturvaohjeet löytyvät tai olisi lukenut ohjeistusta. Tämä luo tarpeen kartoittaa työntekijöiden tietämyksen aiheesta.

Tutkimusongelmani on kartoittaa ja selvittää seuraavia asioita:

- Mitkä ovat tutkimuksen kannalta tärkeimmät käsitteet?
- Mitkä tekijät vaikuttavat tietoturvallisuuden omaksumiseen?
- Mikä on työntekijöiden tietoturvallisuuden tietämyksen tila?
- Miten työntekijöiden tietoturvallisuuden tietämystä voidaan tulevaisuudessa parantaa?

Nämä tutkimusongelmat muodostavat tämän opinnäytetyön perustan. Pyrin löytämään vastauksia näihin ongelmiin tutkimuskyselyn sekä teorian kautta. Tätä tutkimusta voidaan hyödyntää kohderyhmän työntekijöiden tietoturvatietoisuuden kehittämisessä.

1.4 Tärkeimmät käsitteet

Tietoturvallisuus

Tietoturva ja tietoturvallisuus ovat järjestelyjä, joilla pyritään varmistamaan tiedon eheys, luottamuksellisuus ja käytettävyys. Tietoturvaan kuuluu muun muassa laitteistojen, ohjelmistojen, tietoaineistojen, tietoliikenteen ja toiminnan turvaaminen. (Sanastokeskus TSK 2004, 13.)

Tietoturva ei ole itseisarvo vaan se on jotain, jolla on tarkoitus. Tämä tarkoitus organisaatiossa on liiketoiminnan tarpeiden tukeminen sekä sisäisten ja ulkoisten vaatimusten toteuttaminen. Tietoturva tarjoaa erilaisia ratkaisuja ja toimintamalleja tietosuojan ylläpitämiseen. Sillä ikään kuin rakennetaan muuri suojattavan tiedon ympärille. (Laaksonen, Navasalo & tomula 2006, 17.)

Tietoturvallisuus on pieniä tekoja osana henkilöstön jokapäiväistä toimintaa. Hyvä tietoturvallisuus on osa yrityksen kulttuuria, jolloin kaikki tiedostavat tietoturvallisuuden merkityksen ja työskentelevät sen saavuttamiseksi ja ylläpitämiseksi. Tietoturvallisuus on hallinnollisia ja

teknisiä toimia, jotka tulee suunnitella tarkasti, toteuttaa lainsäädännön rajoitukset ja vaatimukset huomioon otten ja joiden vaikutuksia tulee seurata organisaation toiminnan kehittämiseksi. (Laaksonen, Navasalo & tomula 2006, 17.)

Nykymaailmassa tuskin mikään yritys tai julkinen virasto voi toimia ilman toimivaa tietoturvajärjestelyjä. Nämä järjestelyt täytyy myös toteuttaa turvallisesti ja huolellisesti. Tänä päivänä lähes kaikki liiketoiminnan prosessit ja toimeksiannot tehdään sähköisesti. Suurin osa tiedosta on tallennettu digitaalisesti. tietoa myös käsitellään sähköisesti yleisissä verkossa sekä yksityisessä salatussa verkossa. Niinpä organisaatio on täysin riippuvainen moitteettomasta IT-järjestelmistä ja niiden toimivuudesta. (IT-Grundschutz Catalogues 2005, 11.)

Tietoturvatoimenpiteillä turvataan työntekijän, yhteisön ja työpaikan etuja. Verkottuneessa maailmassa harva yritys on enää vastuussa yksinomaan omasta tietoturvallisuudestaan. Tietoturvallisuudesta huolehtiminen on jokaisen työntekijän velvollisuus. Suurimmat tietoturvaongelmat liittyvät yleisesti huolimattomuuteen, kiireeseen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön tekijöihin. Kehittämällä tietoturvallisuutta parannetaan toimintojen jatkuvuutta ja luotettavuutta. (Vahti 10/2006, 11.)

Henkilöstötietoturvallisuus

Henkilöstöturvallisuudella tarkoitetaan yrityksen henkilöstöstä aiheutuvien riskien ehkäisyä ja hallintaa. Tietoturvallisuuden alaterminä henkilöstöturvallisuudella tarkoitetaan myös henkilöstään liittyvien käytettävyys- ja salassapitoriskien hallintaa tietojärjestelmiä ja tietoja käytettäessä. Henkilöstöturvallisuuden merkitys tietojärjestelmien ja tietojen suojaamiselle on keskeinen. Henkilöstöturvallisuuden haasteena on ihminen. Henkilöstö käsittelee tietoja tallentamalla, vastaanottamalla, muokkaamalla, välittämällä ja tuhoamalla niitä. Lisäksi henkilöstöllä on tärkeä rooli järjestelmien ja tietovarastojen ylläpidossa.

Henkilöstöturvallisuus sisältää kaksi vaatimusta, jotka eivät ole riippuvaisia toisistaan:

- Tietojen eheysvaatimus ja käytettävyysvaatimus
- Salassapitovaatimus

(VAHTI 2/2008, 11-12.)

Tietojenkäsittely tulee suojata henkilöstön aiheuttamilta tahattomilta virheiltä ja väärinkäytöksiltä, jotta organisaation toiminnalle ei aiheudu ongelmia ja haittaa. Tietoturvariskejä henkilöturvallisuudelle aiheuttavat muun muassa organisaation kilpailutilanteen kiristyminen, muutokset yhteiskunnassa sekä tietojenkäsittelyyn osallistuvan henkilöstön suuri määrä yrityksen sisällä ja sen ulkopuolella. (Laaksonen, Navasalo & tomula 2006, 138.)

Henkilöturvallisuutta voidaan tarkastella erilaisista näkökulmista. Työkuvan kannalta oleellisia asioita ovat työntekijän nuhteettomuus ja luotettavuus. Työtehtävien kannalta oleellisia asioita ovat työtehtävien eriyttäminen siten, että vastuut ovat rajattu turvallisiksi ja toimenkuvat ovat selkeitä. (Laaksonen, Navasalo & tomula 2006, 138.)

Tietoturva yrityksen näkulmasta

Tieto on yrityksen keskeinen voimavara ja tekijä menestykseen. Siksi sitä on myös suojattava samalla tavalla kuin yrityksen brändiä, työntekijöitä ja fyysistä omaisuutta. (Petteri Järvinen 2002, 111.)

Tietoturva on verkostoituneessa maailmassa suorastaan liiketoiminnan edellytys. Yrityksen tietoturvalta edellytetään laatu- ja sisältövaatimuksia, jotta yritys pääsisi mukaan alihankinta- ja yhteistyösopimuksiin. Elleivät edellä mainitut asiat ole kunnossa, sopimuksia ei voi tehdä. Vajaa ja huono tietoturva voi kostautua vahingonkorvauksina ja sopimussakkoina, jotka rasittava liiketulosta ja yrityksen julkista imagoa.
(Petteri Järvinen 2002, 111.)

Tipton ja Krause ovat Information Security Management handbook kirjassaan samaa mieltä. Heidän mielestään tietoisuus ja koulutus eivät ole vain avain tietoturvan onnistumiseen, vaan myös välttämätöntä yrityksen menestykselle. On ainakin seitsemän syytä miksi parhaat liikejohtajat tukevat koko yrityksen kattavaa tietoturva- ja yksityisyyskoulutusta:

- Koulutuksen avulla turvatoimet saadaan käytäntöön
- Koulutus luo vastuullisuutta
- koulutus on välttämätöntä jotta voidaan noudattaa lainsäädännöllisiä vaatimuksia
- Koulutus on välttämätöntä jotta voidaan noudattaa annettua politiikkaa
- Koulutus osoittaa ahkeruutta
- Koulutus tekee tietoturvasta osan joka päivästä työskentelyä
- Koulutus parantaa asiakassuhteita

Henkilöstön tietoturvakoulutus auttaa henkilöstöä ymmärtämään tiedon suojaamisen tärkeyden ja auttaa heitä keskustelemaan järkevästi asiakkaiden kanssa jos heillä on kysyttävää asiasta. (Tipton & Krause 2009, 91-92.)

Ohjeiden laatiminen on tietoturvan helpoin osa-alue ja se jää usein IT-osaston vastuulle. Vaikeinta on saada tietoturvaohjeet toimimaan myös käytännössä. Tietoturvaa lisäävien sääntöjen noudattaminen helpottuu, kun henkilöstö ymmärtävät, miksi rajoituksia asetetaan ja mi-

ten heidän oma etunsa voi olla vaarassa, jos tietoturva pettää. Työntekijän pitäisi hahmottaa asemansa osana yritystä ja sen julkista kuvaa sekä koko laajassa tietoturvan käsitteessä.Tietoturvan huolehtiminen on viime kädessä yrityksen johdon vastuulla, onhan tietoturva yritystoiminnan perusedellytys. (Petteri Järvinen 2002, 111-112.)

Tietoturvapolitiikka

Organisaation hyväksymä näkemys organisaation tietoturvan toteutuksesta, periaatteista ja päämääristä. (Sanastokeskus TSK 2004, 15.)

Tietoturvapolitiikka ja sen menetelmät muodostavat pääosan organisaation turvallisuudesta. Tietoturvallisuuden valtuutus ja vastuiden jakaminen ovat välttämättömiä tietoturvallisuuden kannalta. Sääntöjen asettaminen työntekijöille ja turvallisuutta vastaaville henkilölle kuuluu tietoturvapolitiikkaan. Politiikka tulisi olla yleisesti sovittu organisaatiossa ja sillä tulisi olla korkeimman johdon hyväksyntä. (John R. Vacca 2009, 261.)

Tietoturvapolitiikka on organisaation tietoturvallisuusprosessia ja tietoturvakäytäntöjä ohjaava dokumentti. Hyvä tietoturvapolitiikka sisältää ainakin nämä osa-alueet:

- organisaation tietoturvallisuuden määritelmät ja keskeiset kohteet
- johdon ilmaus ja tuki tietoturvan tavoitteiden ja periaatteiden noudattaminen
- rakenteet joiden avulla tietoturvallisuus tunnistetaan ja hallitaan
- yhteenveto tietoturvakäytännöistä
- yhteenveto lainsäädännön vaatimuksista
- yhteenveto turvallisuuskoulutuksen järjestämisestä
- määritelmät tietoturvallisuuden vastuualueista
- seuraukset ja käytännöt turvallisuuspolitiikan rikkomisesta
- luettelo politiikkaa tarkentavista standardeista ja tietoturvaohjeista.

Tietoturvapolitiikka tulisi kirjoittaa sellaiseen muotoon, että myös muut kuin hallinnon ja tietojenkäsittelyn ammattilaiset ymmärtävät sen sisällön. (Hakala, Vainio & Vuorinen 2006, 8-9.)

1.5 Kohdeorganisaatio

Danske Bank tarjoaa monipuolisia pankkipalveluja henkilö-, -yritys ja yhteisö- asiakkaille. Pankkituotteiden lisäksi pankki tarjoaa palveluja ja osaamista säästämiseen ja sijoittamiseen, vakuutuksiin, kiinteistövälitykseen ja omaisuudenhoitoon. Danske Bankilla on yli miljoona henkilöasiakasta ja noin 100 000 yritysasiakasta. 15.11.2012 konserni vaihtoi nimensä Danske Bankiksi kaikissa konsernimaissa. Ennen tätä Danske Bank tunnettiin nimellä Sampo Pankki. Suomen maajohtajana toimii Ilkka Hallavo, joka on myös Danske Bank –konsernin laajennetun johtoryhmän jäsen.

Danske Bank suomessa kuuluu Danske Bank –konserniin, joka tarjoaa palveluja yli viidelle miljoonalle asiakkaalle viidessätoista maassa. Konsernissa työskentelee noin 22 000 pankinalan osaajaa ja ammattilaista.

Danske Bank konserni maat ovat Suomi, Ruotsi, Tanska, Norja, Viro, Latvia, Liettua, Irlanti, Pohjois-Irlanti, Iso-Britannia, Saksa, Puola, Luxemburg, Yhdysvallat ja Venäjä. Konttoreita on yli 600 ympäri konsernimaita ja Suomessa konttoreita on yli 100. Suomen pohjoisin konttori sijaitsee Sodankylässä. Konttoreiden lisäksi organisaatioon kuuluu Finanssikeskukset, Contact Center, Instituutio–yksikkö, Sampo Rahoitus, Palvelukeskus sekä Kiinteistömaailma. Konsernin pääkonttori sijaitsee Kööpenhaminassa.

Sampo Pankin toiminta käynnistyi vuonna 1887 Suomen valtion omistaman Postisäästöpankin toimesta. Postisäästöpankki otti vastaan asiakkaiden talletuksia postikonttoreissa. Vuonna 1997 valtion omistama Postipankki ja suomen Vientiluotto yhdistyivät uudeksi yhtiöksi, joka nimettiin Leonia-konserniksi. Vuonna 2000 Vakuutusyhtiö Sampo ja Suomen valtio yhdistivät Sammon ja Leonian uudeksi täyden palvelun finanssikonserniksi. Postipankin ajoilta peritty yhteistyö Postin kanssa päättyi myös vuonna 2000. Helmikuussa 2001 konserniin yhdistyi Mandatum Pankki. Se oli aloittanut toimintansa vuonna 1998 Interbank Osakepankin ja Mandatum & CO:n fuusiosta. Sampo aloitti pankkiliiketoimintansa Virossa, kun se osti kesällä 200 Optiva -pankin Viton keskuspankilta. Tanskalainen Danske Bank ilmoitti marraskuussa 2006 ostavansa Sampo Pankin Sampo osakeyhtiöltä. Kauppa vahvistettiin helmikuussa 2007. Sampo Pankki on Suomen kolmanneksi suurin pankki. Marraskuussa 2012 Sampo Pankin nimi muuttui Danske Bankiksi.

Danske Bank –Konserninkonsepti perustuu vahvasti siihen, että tuotekehitys, tuotteet ja tietojärjestelmät ovat lähes identtiset joka maassa. Danske Bankin ajattelu maailmaan kuuluu yhteiset tekniset ratkaisut ja toimintatavat, jotka mahdollistavat tehokkuuden koko konsernissa. Yhteiset tekniset ratkaisut ja toimitavat mahdollistavat tehokkuuden, sillä yksi kokonaisuus on paljon taloudellisempi kuin monta pientä. Yhteiset ratkaisut mahdollistavat sen, että

resurssit voidaan ohjata tehokkaasti kehitys- ja asiakastyöhön. Yhteinen toimintamalli tarjoaa suurta etua ja hyötyä erityisesti suomalaisyrityksille, jotka toimivat kansainvälisillä markkinoilla.

Danske Bankin tärkeimpiin palveluihin kuuluu:

- Asiakaspalvelu konttoreissa, puhelimitse ja viesteillä
- Asiakastuki puhelimitse
- Automaattinen puhelinpalvelu
- Tekstiviesti- ja sähköpostiviestipalvelut
- Verkkopalvelut joihin kuuluu verkkopankki ja miniverkkopankki
- Pankkipalvelut älypuhelimessa
- Pankkipalvelut iPadissä ja Android -tableteissa
- E-pisteet konttoreissa
- Yksityispankkipalvelut Private Banking asiakkaille

1.5.1 Verkkopankin asiakas- ja tekninen tuki

Tämä opinnäytetyön tutkimuskohteena on Danske Bankin Contact Centerissä sijaitseva Verkkopankin asiakastuki ja tekninen tuki. Kaikki Suomessa tapahtuva Verkkopankin asiakasneuvonta tapahtuu näiden kahden osaston kautta. Nämä kaksi osastoa toimii läheisessä yhteistyössä verkkopankin kehitystiimin kanssa, koska kehityksen on tiedettävä tarkkaan miten verkkopankki toimii käytännössä.

Verkkopankin asiakastuen työ koostuu hyvin monipuolisista tukitehtävistä. Työhön kuuluu henkilö- ja yritysasiakkaiden käytön neuvontaa sähköisten palveluiden käytössä ensisijaisesti verkkopankkiympäristössä. Lisäksi osastolla ratkaistaan verkkopankkiasiakkaiden teknisiä ongelmatilanteita. Asiakastuessa neuvotaan myös asiakkaita Mobiili- ja Tabletpankin käytössä ja sovellusten teknisten ongelmien ratkaisemisessa. Työtehtäviin kuuluu myös vastata asiakasviesteihin, jotka tulevat osastolle eri kanavia pitkin. Teknisellä puolella ratkaistaan ja raportoidaan eteenpäin ongelmat, mitä ei saada ratkaistua asiakastuessa. Sähköpostin käyttö on suuressa roolissa osastojen työskentelyssä.

Osastoilla käytetään työskentelyyn kahta tietokonetta oheislaitteineen, puhelinta, headsettiä ja useita ohjelmia tietokoneilla, jotka mahdollistavat asiakkaiden ongelmatilanteiden selvittämistä ja ongelmien ratkaisemisen. Toinen tietokoneista on pankin sisäisessä verkossa ja

toinen koneista on ulkoisessa verkossa. Sisäisenverkon tietokoneella on kaikki oleelliset työkaluohjelmat, joilla pystyttään selvittämään asiakkaan ongelmatilanteet. Ulkoisenverkon koneella taas pystyy tekemään samoja toimenpiteitä mitä asiakas tekee. Näin on helppo neuvoa asiakasta ohjelmien asentamisessa ja poistamisessa, sekä ohjeistaa asiakasta palvelujen käytössä. Osastoilla on myös Mac OSX eri versioilla varustettuja kannettavia tietokoneita, jotka ovat liitetty langattomaan verkkoon. Käytössä on myös Ipad -tabletti ja eri merkkisiä älypuhelimia joihin on asennettu verkkopankki- sovellus. Mac- kannettavat tietokoneet, älypuhelimet ja Ipad ovat yhteisessä käytössä osastoilla.

Normaalin työpäivän aikana työntekijä vastaa noin 35 asiakaspuheluun päivässä. Viestivuorossa asiakasviesteihin vastataan noin kahteenkymmeneen. Työssä täytyy olla erittäin tarkkana, koska usein käsitellään pankkisalaisuuden alaista tietoa.

2 Tutkimuksen toteutus ja tutkimusmenetelmät

Tutkimuksellinen kehittämistyö voi saada alkunsa erilaisista lähtökohdista. Työn lähtökohta voi löytyä organisaation kehittämistarpeista tai halusta saada aikaan muutoksia. Tutkimukselliseen kehittämistyöhön kuuluu yleensä käytännön ongelmien ratkaisua ja uusien käytäntöjen ideoiden, tuotteiden tai palvelujen tuottamista ja toteuttamista. Työn tarkoituksena on tyypillisesti luonnostella, kehitellä ja ottaa käyttöön ratkaisuja. (Ojasalo, Moilanen & Ritalahti 2009, 19.)

Tutkimuksella normaalisti tavoitellaan tietoa. Kehittämisen määränpäänä on saada aikaan parannettuja tuloksia. Tutkimus- kehittämistoiminta yhdistää nämä molemmat tehtävät. Kehittämistöitä suunnitellaan ja toteutetaan hyvin monenlaisina. Kehittämistöiden luonne vaihtelee, mutta niille on kuitenkin luonteenomaista innovatiivisuus, käytännönläheisyys, hyödynnettävyys ja arvioitavuus. (Anttila 2007, 9-13.)

2.1 Kehittämistyön prosessin eteneminen

Käytännössä prosessi ei ole usein jaettavissa eri vaiheisiin, ja vaiheiden eroa voi olla vaikea nähdä. Usein prosessia myös palataan taaksepäin, sekä edetään edestakaisin eri vaiheiden välillä. Ei siis pidä huolestua, vaikka oma prosessi ei etenisi kuvatavan prosessin mukaisesti.

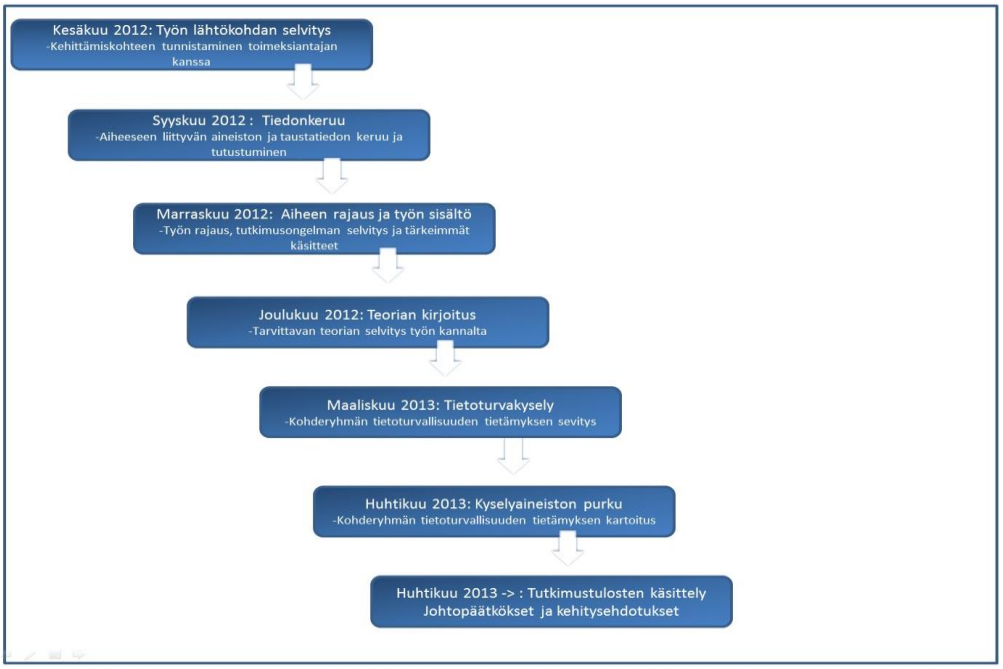
Tutkimuksellisen kehittämishankkeen lähtökohtana ovat kehittämiskohteen ymmärtäminen ja tunnistaminen. Kehittämishanke kohdentuu työelämän kehittämiseen, ja tarkoituksena on saada aikaan jonkinlainen muutos. (Ojasalo, Moilanen & Ritalahti 2009, 24-25.)

Kehittämiskohteen tunnistamisen jälkeen haetaan aiheeseen liittyvää tietoa. Tietoa haetaan sekä käytännöstä että perehtymällä olemassa olevaan teoreettiseen ja muuhun kirjoitettuun aineistoon. (Ojasalo, Moilanen & Ritalahti 2009, 25.)

Kohdeorganisaatiosta ja toimintaympäristöstä kootun taustatiedon sekä tutkimustiedon avulla määritellään tarkempi kehittämistehtävä ja rajataan kehittämisen kohde. Vasta tämän jälkeen voidaan kuvata kehittämistyöhön liittyvät prosessit ja suunnitella oma lähestymistapa ja menetelmät. (Ojasalo, Moilanen & Ritalahti 2009, 25.)

Kehittämistyön prosessin muutoksen toteuttamiseen eli implementointiin tulee sisällyttää paljon aikaa, koska tavoitteena on tuottaa hyödyllisiä muutoksia työelämään. Tulosten jakaminen kirjallisena on myös keskeinen osa tutkimuksellista kehittämistyötä.
Kehittämistyön arviointi on työn viimeinen vaihe, vaikka arviointia tehdään koko prosessin ajan. Arviointi kohdistuu sekä kehittämisprosessiin sekä sen tuotoksiin. (Ojasalo, Moilanen & Ritalahti 2009, 26.)

Alla olevassa kuviossa (kuvio 2) on havainnollistettu tämän tutkimustyön eteneminen



Kuvio 1: Tutkimuksen eteneminen.

2.2 Tutkimusmenetelmä

Kvantitatiivinen eli määrällinen menetelmä on tyypillisesti lomakekysely tai strukturoitu lomakehaastattelu, jossa kysytään samoja kysymyksiä samassa muodossa isolta joukolta vastaajia. Tämä ryhmä muodostaa otoksen tietystä kohteen olevasta perusryhmästä. Kvantitatiiviset menetelmät sopivat hyvin tutkimuksiin, jossa halutaan testata, pitääkö jokin teoria paikkansa. Teoriasta tehdään usein väittämiä ja oletuksia, joilla kyselyllä testataan. (Ojasalo, Moilanen & Ritalahti 2009, 93-94.)

Kvalitatiivisia eli laadullisia menetelmiä ovat ryhmä-, teema- ja avoinhaastattelu sekä osallistuva havainnointi. Kvalitatiivisia menetelmiä on käytetty sellaisten aiheiden tutkimiseen, joita ei tunneta entuudestaan hyvin ja aiheita joita halutaan ymmärtää paremmin. Kvalitatiivisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen. (Ojasalo, Moilanen & Ritalahti 2009, 94.)

Tämän opinnäytetyön tukimusmenetelmäksi valittiin kvantitatiinen eli määrällinen menetelmä. Kvantitatiivinen tutkimusmenetelmä sopii hyvin työn menetelmäksi, koska työssä tutkitaan miten tutkimuksen perusjoukko on omaksunut yrityksen tietoturvapolitiikan ja ohjeistuksen. Koska kyseinen menetelmä valitttiin, tuli aihepiiriin liittyvä teoria tuntea hyvin, ennen kuin sitä alettiin tutkia. Tämä tarkoittaa, että tutkimuksen kysymyseten avulla mitattiin teorian paikkaansapitävyyttä eikä tutkimuksen kysymyksiä keksitä omasta päästä.

2.3 Otanta

Kyselyn vastaajiksi valittiin Pohjois-Haagan Contact Centerin verkkopankin asiakas- ja tekinen tuki. Valinta perustui siihen, että osastoilla käytetään eniten erilaisia järjestelmiä, verkkoja ja laitteita koko organisaatiossa, sekä pystyin olemaan päivittäisessä yhteydessä kohderyhmään. Tällä otannalla varmistettiin, että vastausprosentti on erittäin korkea. Tutkittavien työntekijöiden lukumäärä oli 20.

2.4 Tiedonkeruun menetelmä

Tutkimuksen tietonkeruuseen käytettiin kyselytutkimusta, jossa voitiin kysyä kohderyhmältä monia asioita koskien tietoturvallisuutta. Kyselytukimus valittiin, koska menetelmä on nopea ja tehokas.

Kyselytutkimuksen etuna on, että sen avulla voidaan kerätä laaja tutkimusaineisto. Kyselyt tuottavat tyypillisesti suurimmaksi osaksi numeroihin perustuvia tuloksia, joita voidaankäsitellä tilastollisesti. (Ojasalo, Moilanen & Ritalahti 2009, 108.)

Kyselytutkimus suoritettiin paperisella kyselylomakkeella, jonka jaoin vastaajille osastojen aamupalaverissa. Ennen kyselylomakkeen jakamista kerroin, mistä kyselyssä on kysymys ja vastasin aiheeseen koskeviin kysymyksiin, joita kohdejoukko esitti minulle. Tällä tavalla sain vakuutettua kyselyn vastaamisen tärkeyden, joka käy ilmi kyselyn korkeasta vastusprosentista. Kysymyslomakkeen jaon jälkeen pyysin vastaajia palauttamaan kyselyn takaisin saman viikon aikana henkilökohtaisesti. Muistutin myös, että vastaisin mielelläni mahdollisiin lisäkysymyksiin.

Paperista kyselylomaketta käyttäessä kyselytutkimuksen tulokset joudutaan viemään käsin syöttämällä analysoitavaksi esimerkiksi Exceliin. Sähköisen kyselyn etu olisi ollut, että sen olisi voinut suoraan siirtää analysointiohjelmaan.

2.5 Kysymysten valinta ja lomakkeen suunnittelu

Tämän tutkimuksen kysymykset ovat johdettu tämän opinnäytetyön teorista sekä kohdeorganisaation tietoturvapolitiikasta ja ohjeistuksesta. Kyselylomake toteutettiin paperisena kyselynä, joka jaettiin vastaajille henkilökohtaisesti. Tällä haluttiin mahdollistaa nopea ja vaivaton vastaaminen kyselyyn.

Kyselylomakkeelle valittiin lopulta 30 väittämää ja yksi avoin kysymys (liite 1). Väittämät jaettiin neljään opinnäytetyön osa-alueeseen sekä väittämiin koskien yrityksen tietoturvapolitiikkaa ja ohjeistusta. Väittämät ovat jaettu seuraavasti:

Tietoturvaohjeet ja politiikka (väittämät 1-3)
Tiedon käsittely ja säilytys (väittämät 4-9)
Salasanat ja käyttöoikeudet (väittämät 10-14)
Internet ja sähköposti (väittämät 15-25)
Tietokoneenkäyttö ja mobiililaitteet (väittämät 26-30)

Väittämiin vastattiin viisiportaisella asteikolla:

Täysin samaa mieltä
Melkein samaa mieltä
Hieman eri mieltä
Täysin samaa mieltä

En osaa sanoa

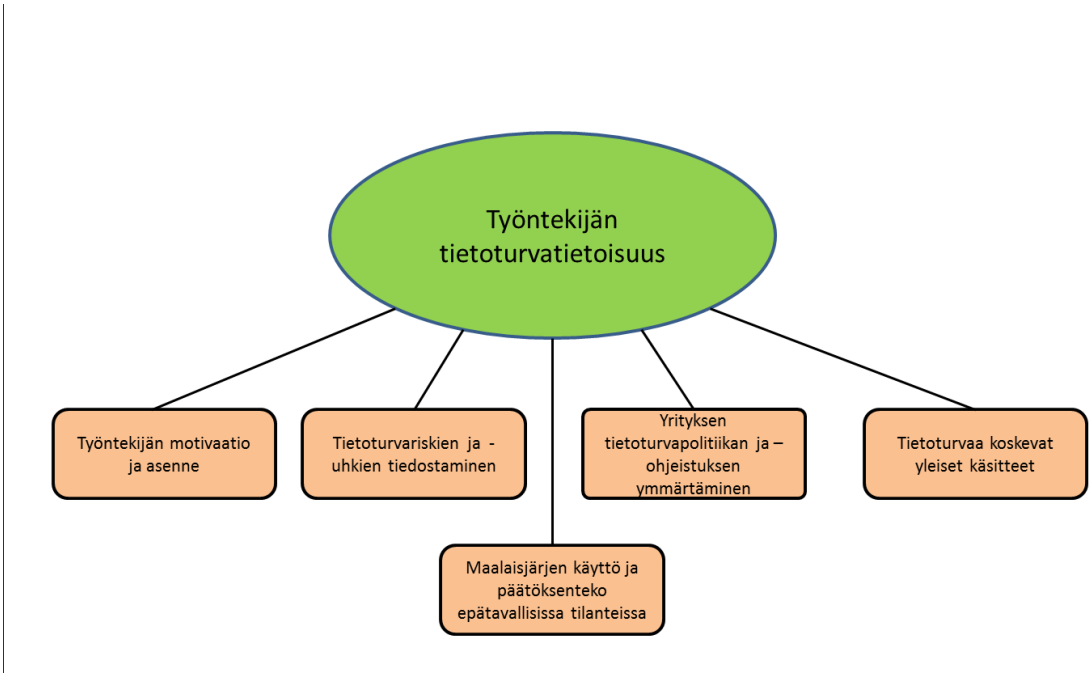
Ennen lopullista kyselylomakkeen jakamista kohderyhmälle kysely testattiin kahdella työntekijällä. Testipalautteen perusteella kyselylomakkeeseen tehtiin pieniä muutoksia ja joitakin kysymyksiä jätettiin pois. Vastausaikaa kyselylle annettiin yksi viikko.

3 Tietoturvan toteutuminen kohderyhmässä

Jokaisen työntekijän tulee huolehtia omalta osaltaan tietoturvaohjeistuksen ja tietoturvapolitiikan tavoitteiden saavuttamisesta. Jotta työntekijä voi toimia organisaation tietoturvavaatimusten mukaisesti, on hänen osallistuttava tietoturvakoulutuksiin sekä soveltaa tietoturvaohjeita ja toimintatapoja käytännön työtehtäviin. (Laaksonen, Nevasalo & Tomula 2006, 107.)

Tietoturvariskien ja tietojenkäsittelyn hallinta vaatii organisaation kulttuurin ja luonteen ymmärtämistä sekä näkemystä siitä miten toimintamallit ja -tavat voivat vaikuttaa henkilöstön käyttäytymiseen. Tarvittava ymmärrys koostuu kahdesta asiasta; miten työntekijä ymmärtää ja sisäistää yrityksen toimintatavat ja miten työntekijät haluavat noudattaa niitä. (Laaksonen, Nevasalo & Tomula 2006, 248.)

Alla olevassa kuviossa (kuvio 1) on havainnollistettu mistä työntekijän tietoturvatietoisuus koostuu.



Kuvio 2: Työntekijän tietoturvatietoisuus

3.1 Työntekijän motivoiminen tietoturvallisuuteen

Useimmat asiantuntijat ovat todenneet työntekijöiden huomion kiinnittämisen tietoturvallisuuteen vaikeaksi. On selvää, että tietoturvallisuustason kohottaminen vaatii muutosta työntekijän käyttäytymisessä. Työntekijän käyttäytymisen ennustaminen ja ymmärtäminen on tärkeää tietoturvallisuuden kehittämisessä. (Laaksonen, Nevasalo & Tomula 2006, 252-253.)

Jotkut tutkijat uskovat, että tietoturvallisuutta voidaan parantaa antamalla henkilöstölle myönteisiä kannustimia ohjeiden ja määräysten noudattamiseksi. Yrityksen soveltaessa tietoturvapolitiikkaansa ja -ohjeita käytäntöön keskitytään kuitenkin helposti tarkkailemaan vain ohjeiden laiminlyöntiä tai rikkomista. (Laaksonen, Nevasalo & Tomula 2006, 252-253.)

3.2 Tietoturvauhat ja -riskit

Jotta organisaation tietoja voidaan suojella, on tunnettava suojattava tieto sekä järjestelmät, jotka käsittelevät, säilyttävät ja siirtävät niitä. Järkevien päätösten tekeminen tietoturvallisuudesta johdolle tulee selvittää organisaation henkilöstön, sovellusten, järjestelmien ja tiedon uhat. (Michael E. Whitman & Herbert J. Mattord 2012, 42.)

Jotta voi tutkia laajoja riski- ja uhka-alueita verkottuneessa maailmassa, tutkijan täytyy haastatella tietoturvahenkilöstöä ja tutkia tietoturvallisuuskirjallisuutta. Vaikka uhkien aihealueet voivat vaihdella paljon, ovat uhat suhteellisen hyvin tutkittu ja ymmärretty. (Michael E. Whitman & Herbert J. Mattord 2012, 43.)

Henkilöstöstä johtuvat tietoturvatekijät ovat mahdollisesti tietojen eheyden, luottamuksellisuuden ja käytettävyyden uhkia. Uhkana pidetään usein työntekijöiden aiheuttamia vahinkoja niin tahallisia kuin myös tahattomia, mutta myös organisaation rakenteella ja sen panostuksella tietotekniikkaan on merkitystä. .(VAHTI 2/2008, 19.)

3.2.1 Tiedon luottamuksellisuuden menetys työntekijän virheestä

Työntekijän sopimaton käytös voi aiheuttaa tiedon luottamuksellisuuden tai eheyden menetyksen. Vahingon laajuus ja luonne riippuu tiedon herkkyydestä. Tässä joitain esimerkkejä työntekijän sopimattomista käytöksistä:

- Arkaluonteista materiaalia sisältäviä monisteita jätetään vahingossa verkkotulostimeen
- Dokumentteja julkaistaan verkossa tarkastamatta saako niitä edes julkaista missään
- Ylläpitäjä on laittanut väärät oikeudet tiedostolle ja työntekijä pääsee muuttamaan tietoa huomaamatta sen seurauksia
- Uutta ohjelmistoa testataan ja näin antaa mahdollisuuden luvattomille työntekijöille mahdollisuuden päästä käsiksi suojattuihin tiedostoihin
- Ulkopuolinen henkilö pääsee käsiksi dokumenttiin jos testitulostusta ei ole käsitelty oikein
- Tiedosto voi päätyä vääriin käsiin jos kovalevy on irrotettu, lähetetty korjattavaksi tai poistettu käytöstä (IT-Grundschutz Catalogues 2005, 415.)

3.2.2 Tiedoston tai laitteiston huolimaton käyttö

Huolimaton tai harjaantumaton laitteiston käsittely voi johtaa laitteen tai datan tuhoutumiseen, joka voi vakavasti häiritä IT-järjestelmän käyttöä. Sama tulos voi syntyä ohjelmiston väärinkäytöstä, tiedoston muuttamisesta tai huolimattomasta poistosta. Yhden komennon huolimaton poistaminen voi poistaa koko tiedoston rakenteen. (IT-Grundschutz Catalogues 2005, 416.)

3.2.3 Tietoturvallisuusohjeiden laiminlyönti

On erittäin yleistä että työntekijät eivät toimi osittain tai kokonaan tietoturvallisuusohjeiden mukaisesti jotka heille on annettu tai suositeltu. Toiminta voi aiheuttaa vahinkoa joka muuten olisi voitu estää tai ainakin minimoida. Riippuen työntekijän tehtävistä ja suojauksen tärkeydestä voi aiheutuva vahinko olla erittäin vakavaa. Tietoturva suojausmenetelmiä usein laiminlyödään johtuen vähäisestä turvallisuustietämyksestä. Tässä pari esimerkkiä:

- Levykkeen, cd-levyn tai muistitikun pitäminen lukitussa pöytälaatikossa ei estä väärinkäyttöä jos avainta säilytetään pöydällä tai vastaavassa paikassa
- Salasanat säilytetään paperilapulla tietokoneen lähettyvillä. (IT-Grundschutz Catalogues 2005, 417.)

3.2.4 Tiedon huolimaton käyttö

On usein huomattu vaikka organisaatiossa on useita teknillisiä turvallisuusohjeita ovat ne sabotoitu tiedon huolimattomalla käytöllä. Tässä muutama esimerkki tiedon huolimattomasta käytöstä:

- Monitoriin kiinnitetty tarralappu johon on kirjattu kaikki salasanat
- Työmatkoille otetaan mukaan kannettavatietokone tai muistitikku, joka sisältää salaista tietoa
- Työntekijät puhuvat salaisesta tiedosta puhuessaan kännykkään julkisilla paikoilla

Lisäksi tauoilla kannettava tietokone jätetään kokoushuoneeseen tai työmatkalla se jätetään autoon tai junavaunuun. Usein muistitikuissa tai kannettavissa laitteissa oleva tieto ei ole tallennettu muualle. Jos kannettavalaite tai muistitikku varastetaan, tieto menetetään lopullisesti. Lisäksi varas saada hyvin rahaa myymällä tiedon eteenpäin, varsinkin jos tieto on salattu huonosti. (IT-Grundschutz Catalogues 2005, 461.)

3.2.5 Salasanojen ja käyttöoikeuksien riskit

Hyvin suunnitelluista ja toteutetuista todentamismenettelyistä ei ole juurikaan hyötyä, jos käyttäjät ovat huolimattomia käsittelemään salasanoja ja käyttöoikeuksia. Käytännössä käyttöoikeudet usein paljastetaan toiselle henkilölle tai niitä ei pidetä turvassa.(IT-Grundschutz Catalogues 2005, 460.)

Riittävän pitkä ja oikein valittu salasana antaa hyvän suojan monia hyökkäyksiä vastaan, mutta salasanoissa voi silti olla omat heikkoutensa. Pyrkimys liian pitkään ja monimutkaiseen salasanaan voi kääntyä käyttäjää vastaan. (Järvinen 2002, 343)

Salasanan unohtaminen

Silloin kun salasana on vain omassa muistissa, on aina olemassa vaara, että se unohtuu. Salasanojen ristiriita on siinä, että mitä mutkikkaampi ja pidempi se on, sitä helpommin käyttäjä sen myös unohtaa. Jos käyttäjä unohtaa salasanan, joutuu hän itse hyökkääjän osaan yrittäessään murtaa omaa salasanaansa. (Järvinen 2002, 344)

Salasanoja ei pitäisi koskaan kirjoittaa paperille, mutta jos kielto johtaa lyhyiden tai helposti arvattavien salasanojen käyttöön, on sittenkin parasta valita kahdesta pahasta pienempi. (Järvinen 2002, 344)

Salasanan kirjoittaminen

Paraskin salasana on vaarassa silloin, kun käyttäjä kirjoittaa sitä näppäimistöltä. Jos käyttäjä käyttää kahta sormea salasanan kirjoittamiseen, on ulkopuolisen helppo nähdä mitä koneelle kirjoitetaan. Kirjoittamisessa salasana osoittaa ristiriitaisen luoteensa. mutkikkaaseen ja pitkään salasanaan tulee helposti kirjoitusvirheitä. Kun käyttäjä joutuu syöttämään salasanan useaan kertaan, riski sen paljastumiseen kasvaa suuresti. Jotta urkkija ei näkisi ruudulle kirjoitettua salasanaa, se näytetään yleensä tähtinä. Toisaalta jo pelkkien tähtien määrä voi auttaa salasanan varastajaa merkittävästi. (Järvinen 2002, 344)

Liian helppo salasana

Käyttäjä usein keksii liian helpon salasanan. Salasana voi olla oma nimi ja syntymävuosi, mikä on helposti arvattavissa. Muita helppoja salasanoja voi olla ystävän, lemmikin tai helppo nu-

merosarja. Usein kun salasana vaihdetaan, käyttäjä vaihtaa vain yhden tai kaksi numero salasanasta ja pitää saman sanan, mikä oli vanhassa salasanassa. (Grundschutz Catalogues 2005, 460.)

Vakoojaohjelmat

Tietokoneelle ujutettu takaovi-haittaohjelma tai jokin muu vakoiluohjelma voi tallentaa kaikki näppäinpainallukset ja siten paljastaa salasanan, oli se miten mutkikas ja pitkä tahansa. Salasanan kirjoittamista kannattaa välttää vieraalla koneella tai jos epäilee ettei tietokone ole puhdas. (Järvinen 2002, 344)

Salasanan kysyminen

Viimeinen tapa saada käyttäjän salasana on saada käyttäjä itse kertomaan se. Murtautuja voi esiintyä puhelimessa tai sähköpostilla yrityksen uutena mikrotukihenkilönä tai operaattorina, joka korjaa jotakin vikaa ja tarvitsee siihen liittyen salasanan ja käyttäjätunnuksen. (Järvinen 2002, 345)

Käyttöoikeuksien väärinkäyttö

Jos peruskäyttäjä voi asentaa rajoitetusti ohjelmia tietokoneelle, on mahdollista, että koneelle tarttuu haittaohjelma. Haittaohjelma pystyy myös lisäämään itsensä myös järjestelmärekisteriin automaattisesti käynnistyvien ohjelmien listaan. Jos käyttöoikeuksia ei ole rajoitettu, käyttäjä voi helposti asentaa selainlaajennuksen, joka voi olla haittaohjelma tai muuten hidastaa internetin käyttöä. (Järvinen 2006, 211)

3.2.6 Internet- ja sähköpostiuhat

Internet ja sähköposti ovat hyviä työkaluja kommunikoida ja etsiä tietoa. Täytyy kuitenkin muistaa että sähköposti tai internet eivät sisällä itsessään mitään suojausta. Tieto kulkee salaamattomassa yleisissä verkossa missä vaanii monia vaaroja. Siksi internetiä ja sähköpostia tulisi käyttää huolellisesti. (VAHTI 4 2009, 16)

Internetin uhat

Internet-verkkoon pääsee kuka tahansa, eikä sieltä voi erottaa ketään. Vastuun kantaminen huolellisuudesta jää jokaisen käyttäjän tehtäväksi. Verkkokäyttäjien joukkoon mahtuu

huijareita, häiriköitä ja suoranaisia rikollisia. He eivät ota vastuuta mistään, vaan käyttävät törkeästi hyödykseen internetin heikkouksia. Mahdollisuus oman henkilöllisyyden salaamiseen ja kansainvälisyys voivat houkutella väärinkäytöksiin. Vaikka verkossa on vaaransa, varovaisuus ja maalaisjärjen käyttö riittävät yleensä niiden torjumiseen. (Järvinen 2002, 179.)

ActiveX-riskit

Useat haittaohjelmat tulevat ActiveX -moduuleina. Siksi käyttäjän kannattaa olla varovainen, kun selain kysyy lupaa ActiveX-ohjelman asentamiseen. Suurin osa ActiveX-ohjelmista on täysin vaarattomia, mutta joukkoon mahtuu myös erittäin vaarallisia ohjelmia. (Järvinen 2002, 198.)

Hakkerit voivat käyttää ActiveX oikeuksia levittämään haittaohjelmia koneellasi. He voivat vaarantaa käyttäjän lähettämät sähköpostit, lähettää viruksia, troijalaisia ja matoja jokaiselle henkilölle, jonka sähköpostiosoitteet käyttäjällä on. (Dangers of ActiveX and How to Disable It. 2006)

WWW-sivujen vaarat

Internet-sivujen tekijät sortuvat joskus epämiellyttäviin temppuihin. Sivuille upotetuilla skripteillä yritetään manipuloida käyttäjän selainta monin eri tavoin:

- Back-painikkeen esto estää back -painiketta toimimasta
- Sivulle piilotetulla ohjelmalla saadaan selain vaihtamaan aloitussivu siten, että haittaohjelman luojan oma sivu latautuu aina selaimen käynnistyessä
- Pop-up ikkunoiden avaaminen aiheuttaa sen, että yritys poistua sivuilta saattaa laukaista kokonaisen ikkunoiden sarjan, joista ei millään tahdo päästä eroon. Uusia ikkunoita aukeaa nopeammin kuin käyttäjä ehtii sulkea vanhoja ikkunoita
- Linkitys on koko www-järjestelmän infrastruktuuri, mutta linkeissäkin piilee vaaroja. Vaarallisimpia ovat kehyslinkit, jotka voivat tuoda toisen tekemän sisällön osaksi omia sivuja niin, ettei käyttäjä pysty tunnistamaan sisällön lähdettä. (Järvinen 2002, 199-203.)

Sähköpostin uhat

Moni sähköpostin käyttäjä uskoo, ettei omista viesteistä ole mitään sellaista, mikä kiinnostaa muita. Siitä emme voi kuitenkaan olla varmoja. Viestejä voi houkutella katsomaan pelkkä

uteliaisuus tai takana voi olla taloudellisen hyödyn hakeminen. Lähes aina sähköpostia koskevat tietoturvaongelmat tulevat uhreiksi joutuneelle täysin yllätyksenä. Käyttäjät, jotka osaavat epäillä, osaavat yleensä myös suojautua ongelmilta. (Järvinen 2003, 255.)

Sähköpostihuijauksia on kaikenlaisia. Vaarattomampia huijauksia ovat ketjukirjeet, joissa kehotetaan levittämään sähköpostia eteenpäin omille ystäville. Vaarallisimmat huijaukset ovat nigerialaiset kirjeet, joihin mukaan lähtevä voi menettää paljon rahaa. Jos lähtee selvittämään rahojensa kohtaloa, voi henki olla vaarassa. Näiden ääripäiden väliin mahtuu kaikenlasia haittaohjelmia. Huijausviesteissä saatetaan udella myös henkilöiden tai yritysten tilinumeroita erilaisilla verukkeilla. (Järvinen 2006, 52-53.)

Harhaanjohtava linkki

Uhrin huijaaminen on helpointa silloin, kun hänet saadaan painamaan annettua linkkiä sähköpostissa. Käyttäjä uskoo siirtyneensä juuri oikealle sivulle, vaikka todellisuudessa linkin tekstillä ei ole mitään tekemistä oikean osoitteen kanssa. Linkki voi itsessään sisältää jo haittaohjelman. (Järvinen 2006, 60.)

3.2.7 Tietokoneiden ja mobiililaitteiden käyttö sekä siirrettävät mediat

Tietotekniikkajärjestelmän virheellinen käyttö, joka johtuu piittaamattomuudesta tai huolimattomuudesta, vaarantaa IT-järjestelmien turvallisuuden. Tieto voi myös vanhingossa tuhoutua tai muuttua tietokoneen tai mobiililaitteen virheellisestä käytöstä. (IT-Grundschutz Catalogues 2005, 422.)

Tietokoneen käyttö

Jos useat käyttäjät työskentelevät yhdellä tietokoneella, on vaara, että edellinen käyttäjä ei kirjaudu ulos ja uusi käyttäjä ei kirjaudu oikein huolimattomuuden tai laiminlyönnin takia. Laiminlyönti perustellaan usein sillä, että käyttöjärjestelmän uudelleen käynnistäminen vie liikaa aikaa ja sitä ei pidetä hyväksyttävänä. Tämän virheellinen toiminta johtaa tilanteeseen, jossa käytönvalvonta menettää merkityksensä. Tallennettu tieto ei enää tarjoa luotettavaa tieto siitä, kuka käyttää tietokonetta tiettyinä ajankohtina. (IT-Grundschutz Catalogues 2005, 431.)

Kun käytetään tulostuksen hallintaa, jaettuja kansioita tai leikepöytää Windows-ympäristössä, ovat toiminnalliset virheet mahdollisia. Virheet voivat johtaa resurssien jakamiseen tahatto-

masti. Tarvittavat suojausmenetelmät voidaan soveltaa väärin, jos käyttäjällä ei ole tarpeeksi tietoa Windows käyttöjärjestelmistä. (IT-Grundschutz Catalogues 2005, 432.)

Kannettavien tietokoneiden turvallisuus

Kannettavat tietokoneet aiheuttavat haasteita yrityksen tietoturvalle. Kannettavaa tietokonetta käytetään sekä yrityksen sisäjärjestelmissä että ulkopuolisissa järjestelmissä. Tällöin on vaikea miettiä miten tietoa käsitellään. Jos tieto on tallennettu laitteeseen, pitää huolehtia siitä, ettei se joudu ulkopuolisen henkilön käsiin. On myös mahdollista, että laite on saanut tartunnan vieraasta verkosta. Jos kannettavalaite on pitempään poissa organisaation verkosta, on mahdollista, ettei virustietokantoja ole päivitetty asianmukaisesti. (Hakala, vainio & Vuorinen. 2006, 137.)

Mobiililaitteet ja siirrettävät mediat

Yrityksen työntekijöillä on nykyisin käytössä suuri joukko erilaisia mobiililaitteita ja tiedon tallennukseen sekä siirtoon käytettäviä laitteita. Yrityksen kannalta asian tekee hankalaksi se, että työntekijät voivat tuoda työpaikalle myös omia laitteitaan, joiden suojaaminen ja hallinta ovat yrityksen kontrollin ulkopuolella. (Laaksonen, Nevasalo & Tomula. 2006, 218.)

Lähes kaikki laitteet voidaan helposti liittää yrityksen työasemiin tai jopa palvelimiin käyttämällä USB -porttia. Laitteelle voi helposti ja nopeasti kopioida vaikka kaikki työaseman tiedot. Työntekijällä on näin mahdollisuus viedä kaikki haluamansa tiedot mukanaan vaikkapa siirtyessään toisen työnantajan palvelukseen. Muistivälineitä lukuun ottamatta lähes kaikki mobiililaitteilla on mahdollista mahdollista muodostaa erilaisia tiedonsiirtoyhteyksiä ja kytkeä laite suojaamattomaan verkkoon. Suojaamattomia laitteita on mahdollista käyttää hyväksi, tai niihin voi tartuttaa haittaohjelmia. Yrityksen luottamuksellisen tietojen menettämisen lisäksi laitteen käyttäjä voi joutua identiteettivarkauden uhriksi, joka on kasvava rikollisuuden muoto. (Laaksonen, Nevasalo & Tomula. 2006, 218-219.)

Laitteiden tiedot voivat vaarantua myös silloin, kun laitteita lähetetään huoltoon tai silloin, kun niitä jaetaan edelleen yrityksen sisällä tai myydään pois. (Laaksonen, Nevasalo & Tomula. 2006, 219.)

4 Tutkimustulokset

Kyselylomake jaettiin henkilökohtaisesti kaikille teknisen- ja asiakastuen työntekijöille, jotka olivat töissä vastausajan puitteissa. Yhdelle asiakastuen ja yhdelle teknisentuen työntekijälle ei kyselylomaketta voitu jakaa pitkän loman ja isyysvapaan vuoksi. Kyselyyn siis vastastasi 18 henkilöä, kun henkilöstön yhteismäärä on 20. Vastausprosentiksi saatiin siis 90%. Kyselyyn vastasi ensimmäisen päivän aikana 15 henkilöä ja loput 3 henkilöä vastasivat kyselyyn seuraavana päivänä. Vastausprosentti oli niin hyvä kuin sen hetkiset puitteet sallivat. Vastausprosentin hyvään tulokseen vaikutti luultavasti kyselylomakkeen antaminen henkilökohtaisesti vastaajalle sekä vastausten antamisen helppous ja nopeus. Vastaajista kaikki 18 henkilöä olivat vastanneet kaikkiin kolmeenkymmeneen väittämään ja 7 henkilöä vastasi avoimeen kysymykseen.

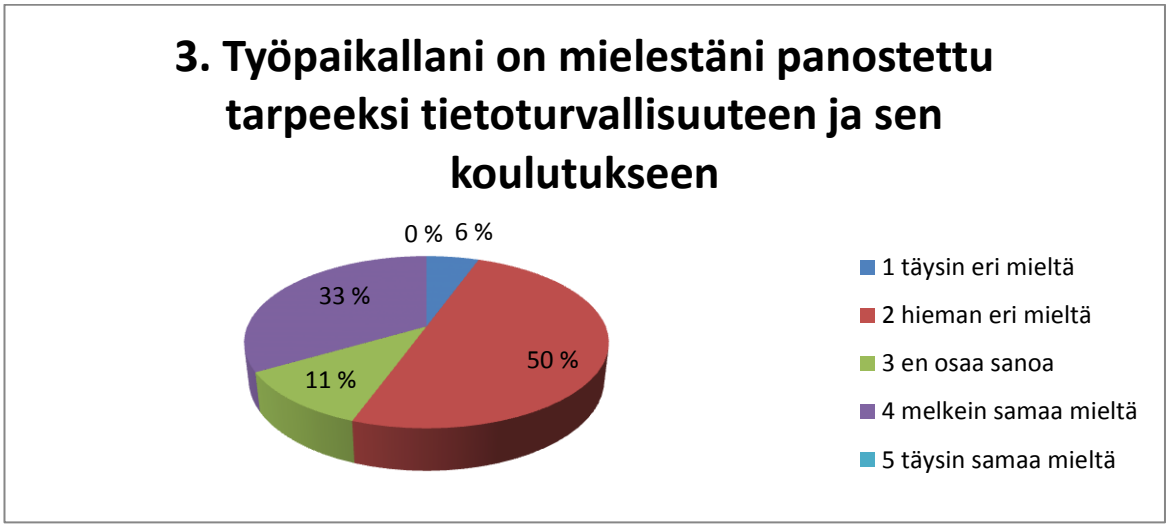
4.1 Tietoturvaohjeet ja -politiikka

Kuvio 3: Väittämän "1. Tiedän mistä yrityksen tietoturvaohjeet ja tietoturvapolitiikka löytyy" vastausjakauma.

Väitämmässä 1 tiedusteltiin, tietääkö vastaaja mistä yrityksen tietoturvaohjeet ja tietoturvapolitiikka löytyy. Vastaajista 7 henkilöä (39%) vastasi "täysin eri mieltä" ja 3 (17%) vastasi "hieman eri mieltä". Vastaajista 3 (17%) vastasi "täysin samaa mieltä" ja myös 3 (17%) vastasi "melkein samaa mieltä". Vastaajista 2 (11%) henkilöä vastasi "en osaa sanoa".

Kuvio 4: Väittämän "2. Olen ehtinyt huolellisesti tutustua yrityksen tietoturvaohjeisiin ja -politiikkaan" vastausjakauma.

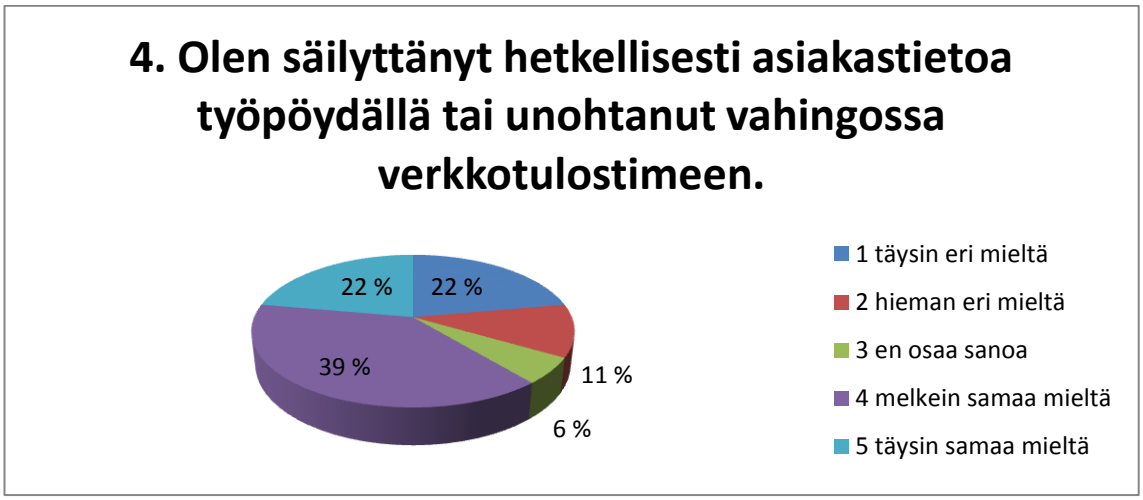
Väitämmässä 2 tiedusteltiin, onko vastaaja ehtinyt huolellisesti tutustua yrityksen tietoturva-ohjeisiin ja -politiikkaan. Vastaajista 6 henkilöä (33%) vastasi "täysin eri mieltä" ja 6 (33%) vastasi "hieman eri mieltä". Vastaajista 1 (6%) vastasi "täysin samaa mieltä" ja 3 (17%) vastasi "melkein samaa mieltä". Vastaajista 2 henkilöä (11%) vastasi "en osaa sanoa".



Kuvio 5: Väittämän "3. Työpaikallani on mielestäni panostettu tarpeeksi tietoturvallisuuteen ja sen koulutukseen" vastausjakauma.

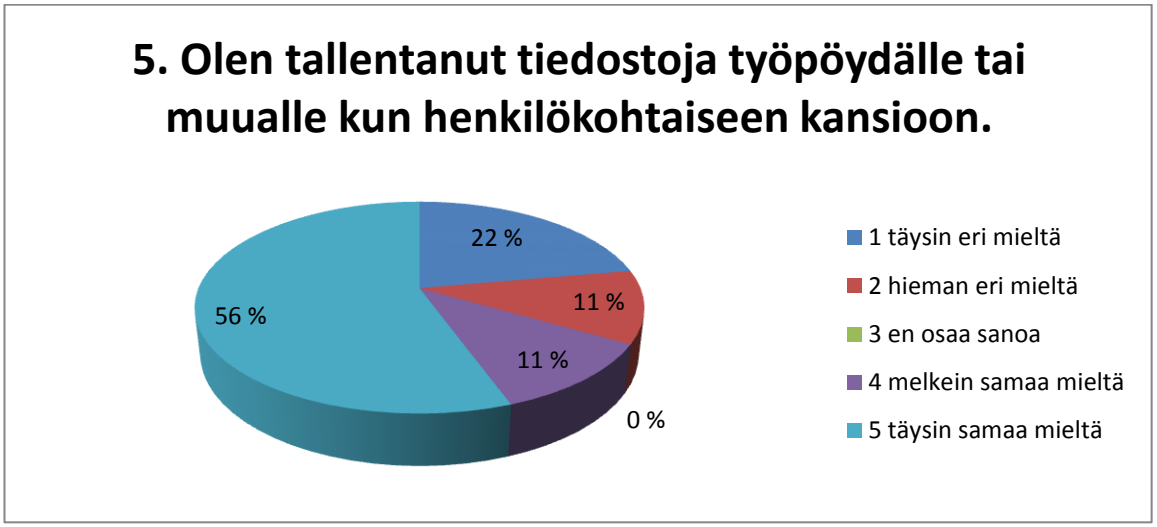
Väitämmässä 3 tiedusteltiin, onko työpaikalla panostettu tarpeeksi tietoturvallisuuteen ja sen koulutukseen. Vastaajista 1 henkilö (6%) vastasi "täysin eri mieltä" ja 9 (50%) vastasi "hieman eri mieltä". Vastaajista 0 (0%) vastasi "täysin samaa mieltä" ja 6 (33%) vastasi "melkein samaa mieltä". Vastaajista 2 henkilöä (11%) vastasi "en osaa sanoa".

4.2 Tiedon käsittely ja säilytys



Kuvio 6: Väittämän "4. Olen säilyttänyt hetkellisesti asiakastietoa työpöydällä tai unohtanut vahingossa verkkotulostimeen. " vastausjakauma.

Väitämmässä 4 tiedusteltiin, onko vastaaja säilyttänyt hetkellisesti asiakastietoa työpöydällä tai unohtanut vahingossa verkkotulostimeen. . Vastaajista 4 henkilöä (22%) vastasi "täysin eri mieltä" ja 2 (11%) vastasi "hieman eri mieltä". Vastaajista 4 (22%) vastasi "täysin samaa mieltä" ja 7 (39%) vastasi "melkein samaa mieltä". Vastaajista 1 henkilö (6%) vastasi "en osaa sanoa".



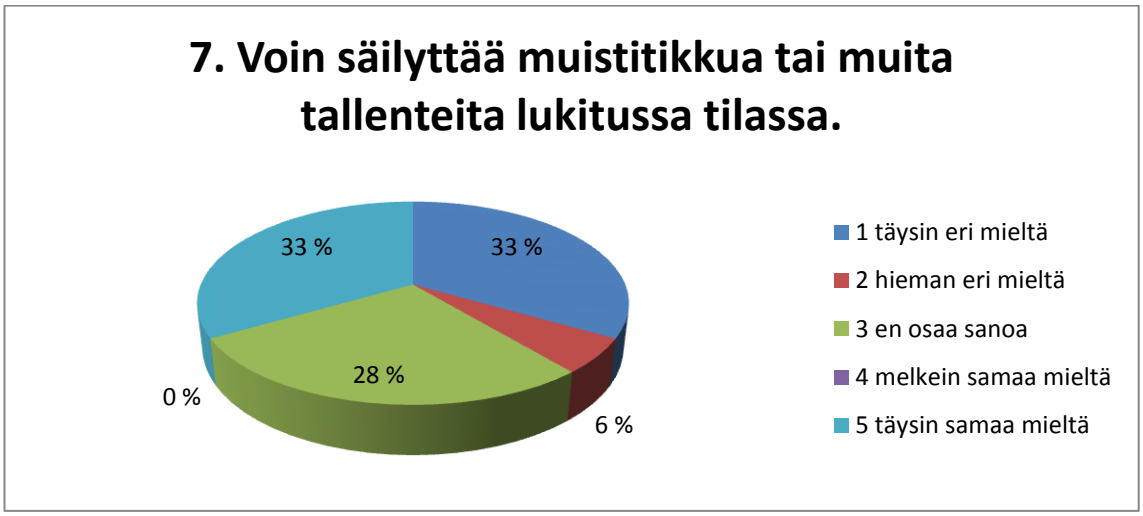
Kuvio 7: Väittämän "5. Olen tallentanut tiedostoja työpöydälle tai muualle kun henkilökohtaiseen kansioon. " vastausjakauma.

Väitämmässä 5 tiedusteltiin, onko vastaaja tallentanut tiedostoja työpöydälle tai muualle kun henkilökohtaiseen kansioon. Vastaajista 4 henkilöä (22%) vastasi "täysin eri mieltä" ja 2 (11%)

vastasi "hieman eri mieltä". Vastaajista 10 (56%) vastasi "täysin samaa mieltä" ja 2 (11%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".

Kuvio 8: Väittämän " 6. Tulostan ohjeistukset ja materiaalit mielummin paperille kuin katson ne tallennetuista kohteista. " vastausjakauma.

Väitämmässä 6 tiedusteltiin, tulostaako vastaaja ohjeistukset ja materiaalit mielummin paperille kuin katsoo ne tallennetuista kohteista. Vastaajista 7 henkilöä (39%) vastasi "täysin eri mieltä" ja 7 (39%) vastasi "hieman eri mieltä". Vastaajista 2 (11%) vastasi "täysin samaa mieltä" ja 0 (0%) vastasi "melkein samaa mieltä". Vastaajista 2 henkilöä (11%) vastasi "en osaa sanoa".

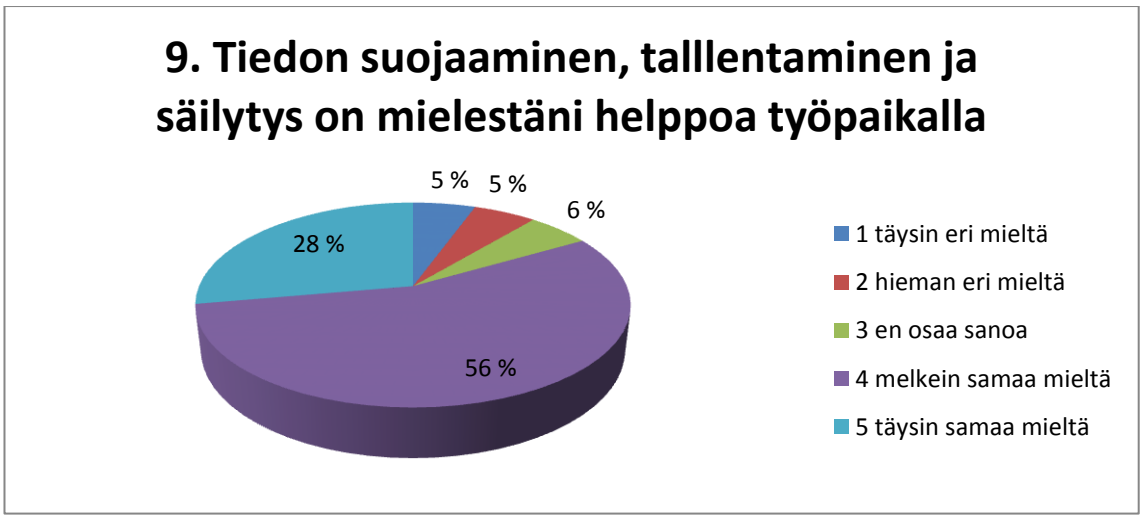


Kuvio 9: Väittämän "7. Voin säilyttää muistitikkua tai muita tallenteita lukitussa tilassa." vastausjakauma.

Väitämmässä 7 tiedusteltiin, voiko vastaaja säilyttää muistitikkua tai muita tallenteita lukitussa tilassa. Vastaajista 6 henkilöä (33%) vastasi "täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 6 (33%) vastasi "täysin samaa mieltä" ja 0 henkilöä (0%) vastasi "melkein samaa mieltä". Vastaajista 5 henkilöä (28%) vastasi "en osaa sanoa".

Kuvio 10: Väittämän "8. Olen käyttänyt henkilökohtaista muistitikkua työpaikalla." vastausjakauma.

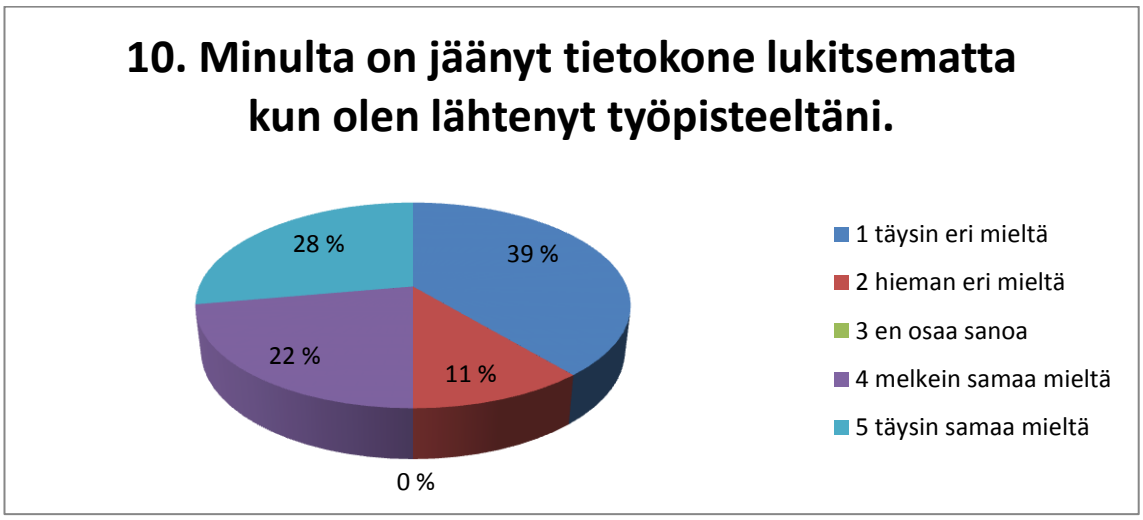
Väitämmässä 8 tiedusteltiin, onko vastaaja käyttänyt henkilökohtaista muistitikkua työpaikalla. Vastaajista 17 henkilöä (94%) vastasi "täysin eri mieltä" ja 0 (0%) vastasi "hieman eri mieltä". Vastaajista 1 (6%) vastasi "täysin samaa mieltä" ja 0 henkilöä (0%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".



Kuvio 11: Väittämän "9. Tiedon suojaaminen, talllentaminen ja säilytys on mielestäni helppoa työpaikalla" vastausjakauma.

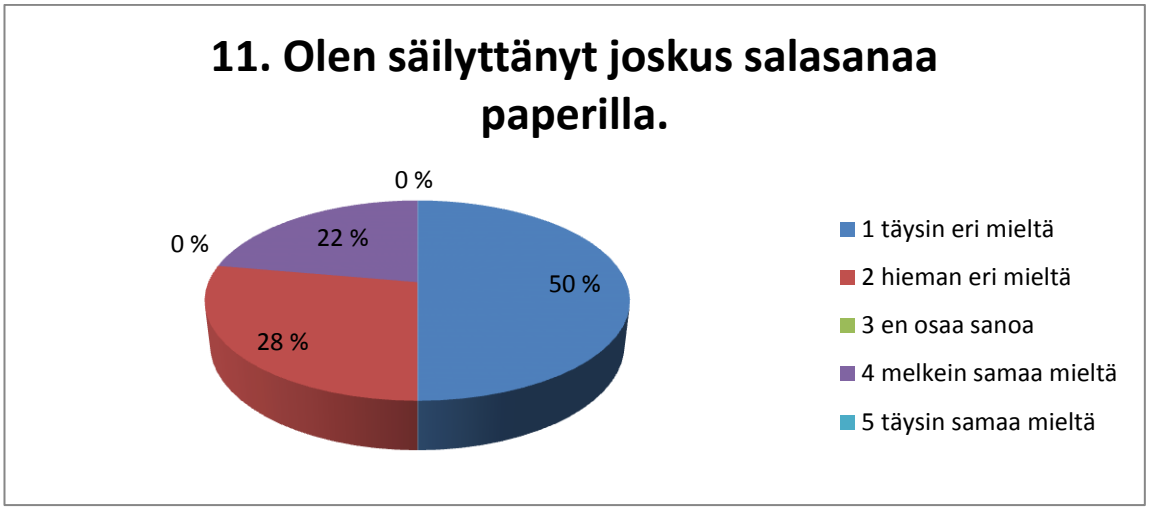
Väitämmässä 9 tiedusteltiin, onko vastaajan mielestä tiedon suojaaminen, talllentaminen ja säilytys helppoa työpaikalla. Vastaajista 1 henkilö (6%) vastasi "täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 5 (28%) vastasi "täysin samaa mieltä" ja 10 henkilöä (56%) vastasi "melkein samaa mieltä". Vastaajista 1 henkilö (6%) vastasi "en osaa sanoa".

4.3 Salasanat ja käyttöoikeudet



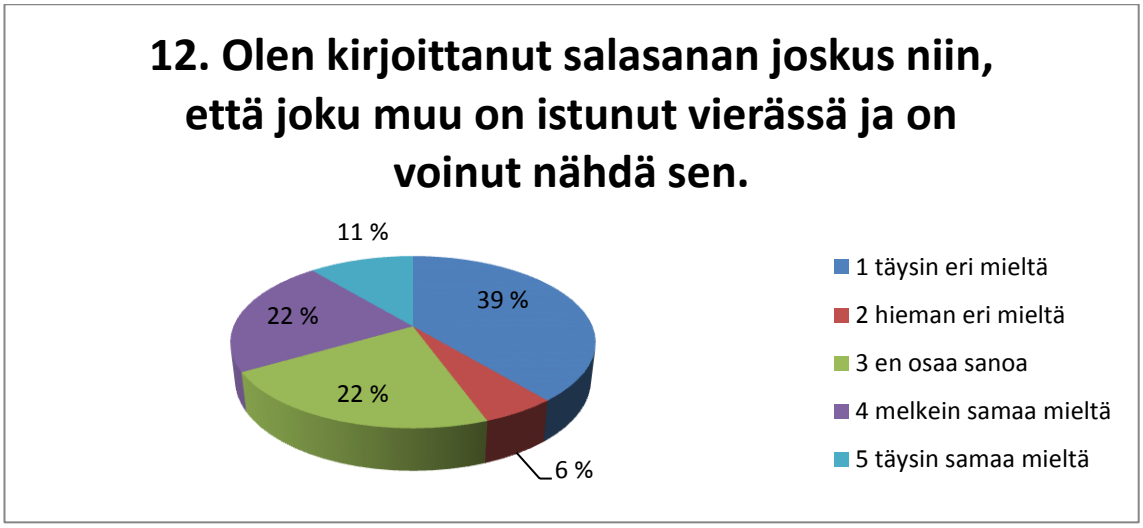
Kuvio 12: Väittämän "10. Minulta on jäänyt tietokone lukitsematta kun olen lähtenyt työpisteeltäni." vastausjakauma.

Väitämmässä 10 tiedusteltiin, onko vastaajalta jäänyt tietokone lukitsematta kun on lähtenyt työpisteeltä. Vastaajista 7 henkilöä (39%) vastasi "täysin eri mieltä" ja 2 (11%) vastasi "hieman eri mieltä". Vastaajista 5 (28%) vastasi "täysin samaa mieltä" ja 4 henkilöä (22%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".



Kuvio 13: Väittämän "11. Olen säilyttänyt joskus salasanaa paperilla." vastausjakauma

Väitämmässä 11 tiedusteltiin, onko vastaaja säilyttänyt joskus salasanaa paperilla. Vastaajista 9 henkilöä (50%) vastasi "täysin eri mieltä" ja 5 (28%) vastasi "hieman eri mieltä". Vastaajista 0 (0%) vastasi "täysin samaa mieltä" ja 4 henkilöä (22%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".

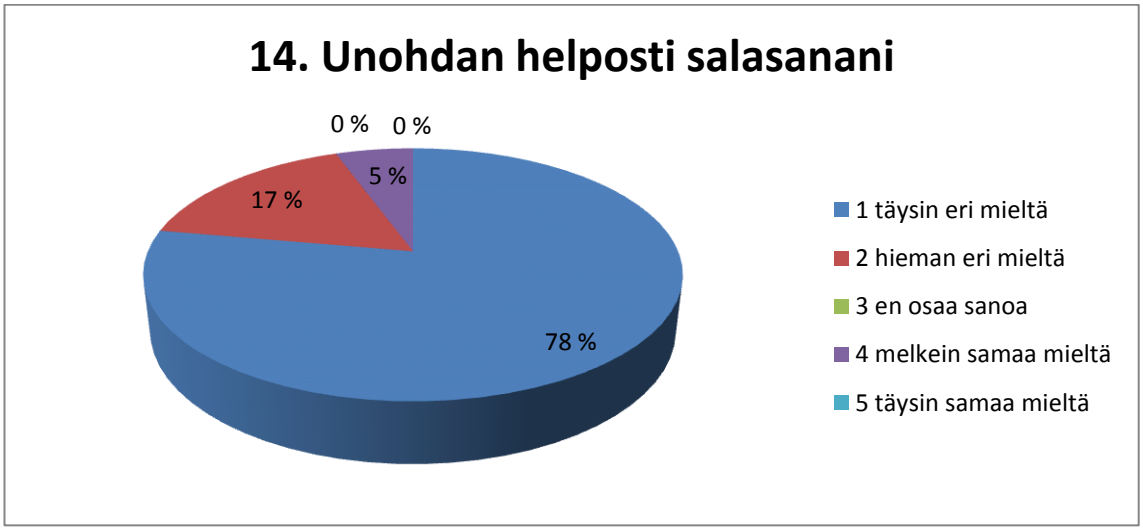


Kuvio 14: Väittämän "12. Olen kirjoittanut salasanan joskus niin, että joku muu on istunut vierässä ja on voinut nähdä sen." vastausjakauma.

Väitämmässä 12 tiedusteltiin, onko vastaaja kirjoittanut salasanan joskus niin, että joku muu on istunut vierässä ja on voinut nähdä sen. Vastaajista 7 henkilöä (39%) vastasi "täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 2 (11%) vastasi "täysin samaa mieltä" ja 4 henkilöä (22%) vastasi "melkein samaa mieltä". Vastaajista 4 henkilöä (22%) vastasi "en osaa sanoa".

Kuvio 15: Väittämän "13. Salasanani on sisältänyt oman nimeni, kaverini nimen, lemmikin nimen tai syntymävuoteni." vastausjakauma.

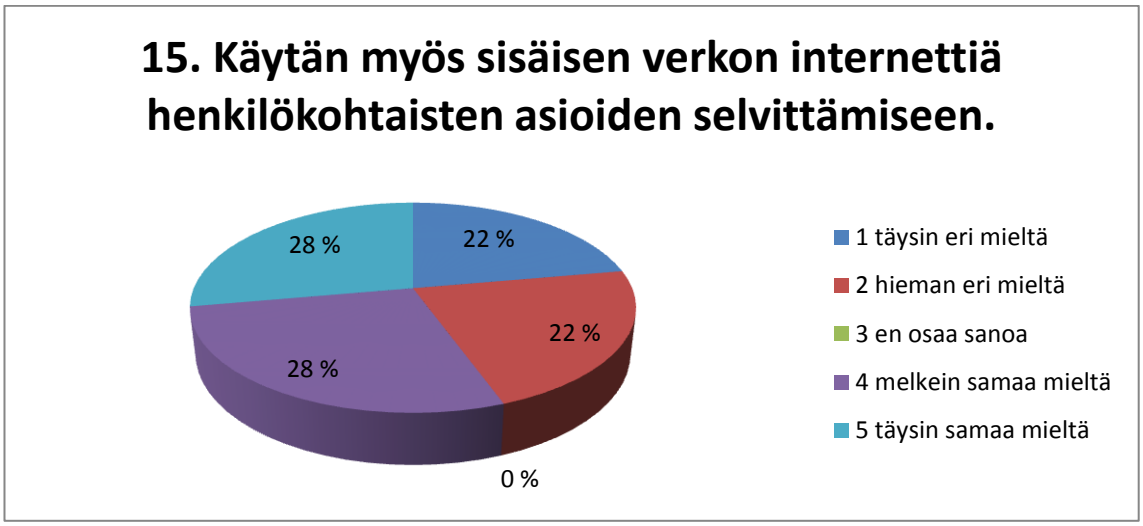
Väitämmässä 13 tiedusteltiin, onko vastaajan salasana sisältänyt oman nimen, kaverin nimen, lemmikin nimen tai syntymävuoden. Vastaajista 12 henkilöä (67%) vastasi "täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 3 (17%) vastasi "täysin samaa mieltä" ja 1 henkilö (6%) vastasi "melkein samaa mieltä". Vastaajista 1 henkilö (6%) vastasi "en osaa sanoa".



Kuvio 16: Väittämän "14. Unohdan helposti salasanani." vastausjakauma.

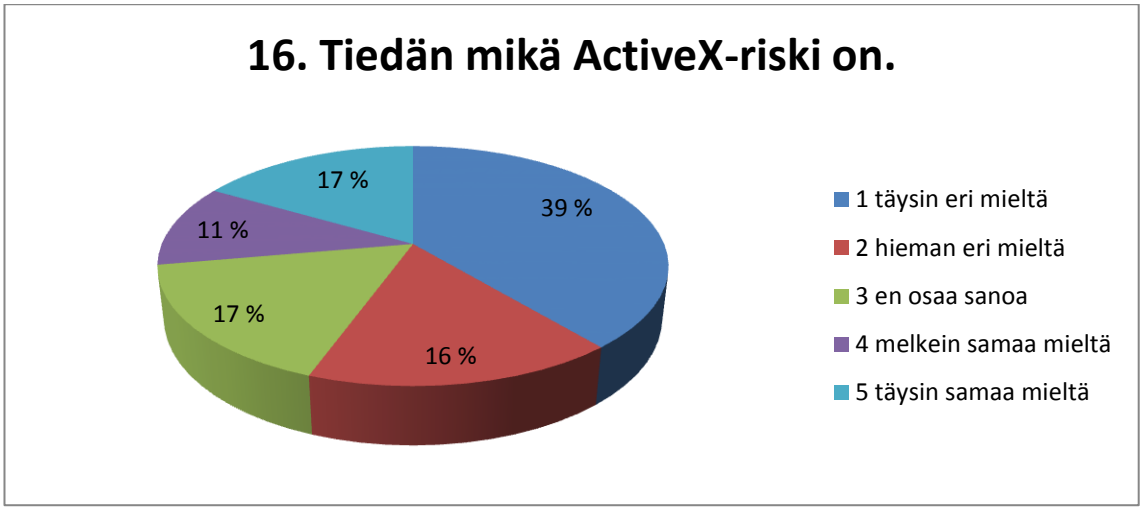
Väitämmässä 14 tiedusteltiin, unohtaako vastaaja helposti salanansa. Vastaajista 14 henkilöä (78%) vastasi"täysin eri mieltä" ja 3 (17%) vastasi "hieman eri mieltä". Vastaajista 0 (0%) vastasi "täysin samaa mieltä" ja 1 henkilö (6%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilö (0%) vastasi "en osaa sanoa".

4.4 Internet ja sähköposti



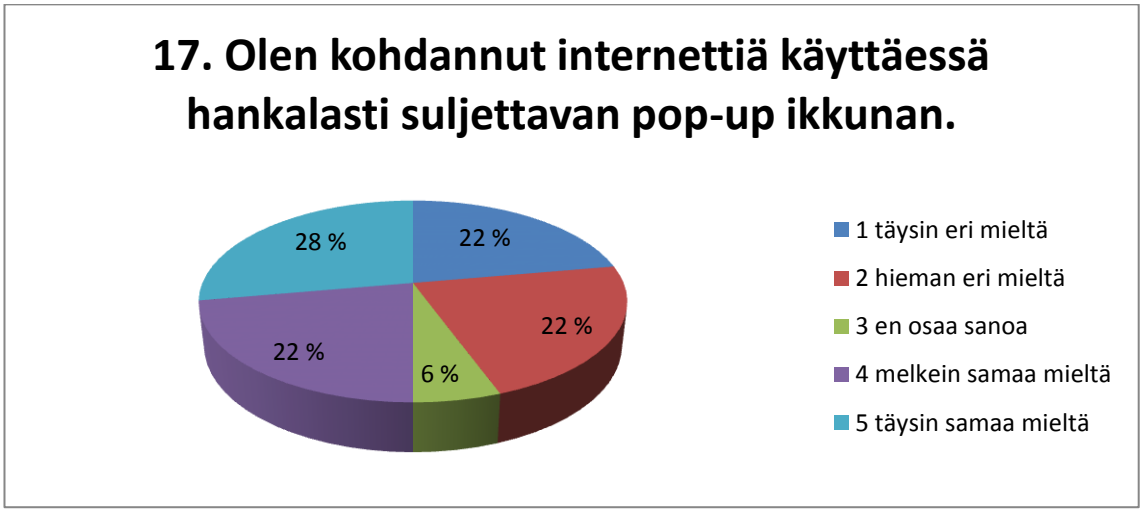
Kuvio 17: Väittämän "15. Käytän myös sisäisen verkon internettiä henkilökohtaisten asioiden selvittämiseen." vastausjakauma.

Väitämmässä 15 tiedusteltiin, käyttääkö vastaaja myös sisäisen verkon internettiä henkilökohtaisten asioiden selvittämiseen. Vastaajista 4 henkilöä (22%) vastasi "täysin eri mieltä" ja 4 (22%) vastasi "hieman eri mieltä". Vastaajista 5 (28%) vastasi "täysin samaa mieltä" ja 5 henkilöä (28%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".



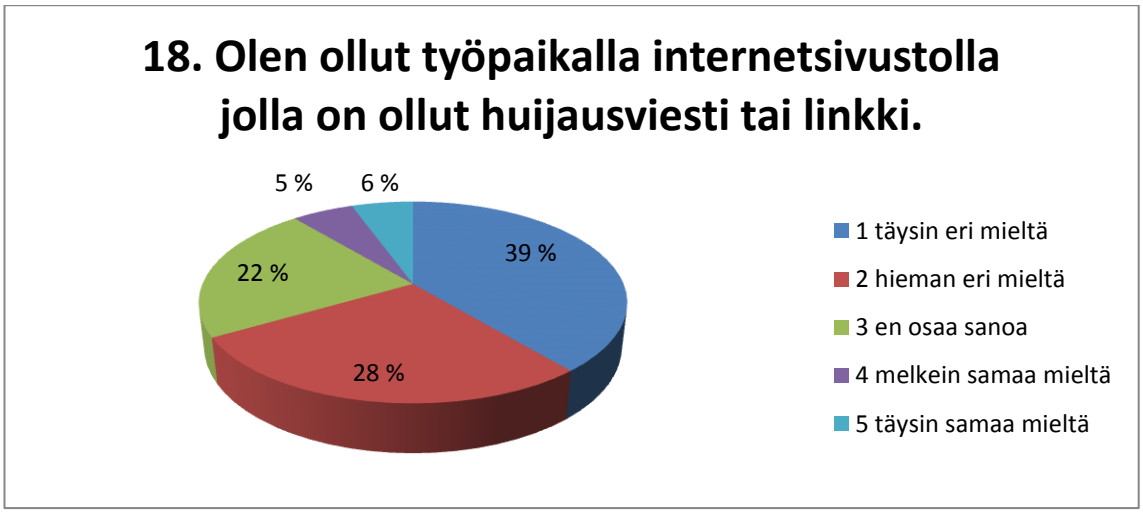
Kuvio 18: Väittämän "16. Tiedän mikä ActiveX-riski on." vastausjakauma.

Väitämmässä 16 tiedusteltiin, tietääkö vastaaja mikä ActiveX-riski on. Vastaajista 7 henkilöä (39%) vastasi"täysin eri mieltä" ja 3 (17%) vastasi "hieman eri mieltä". Vastaajista 3 (17%) vastasi "täysin samaa mieltä" ja 2 henkilöä (11%) vastasi "melkein samaa mieltä". Vastaajista 3 henkilöä (17%) vastasi "en osaa sanoa".



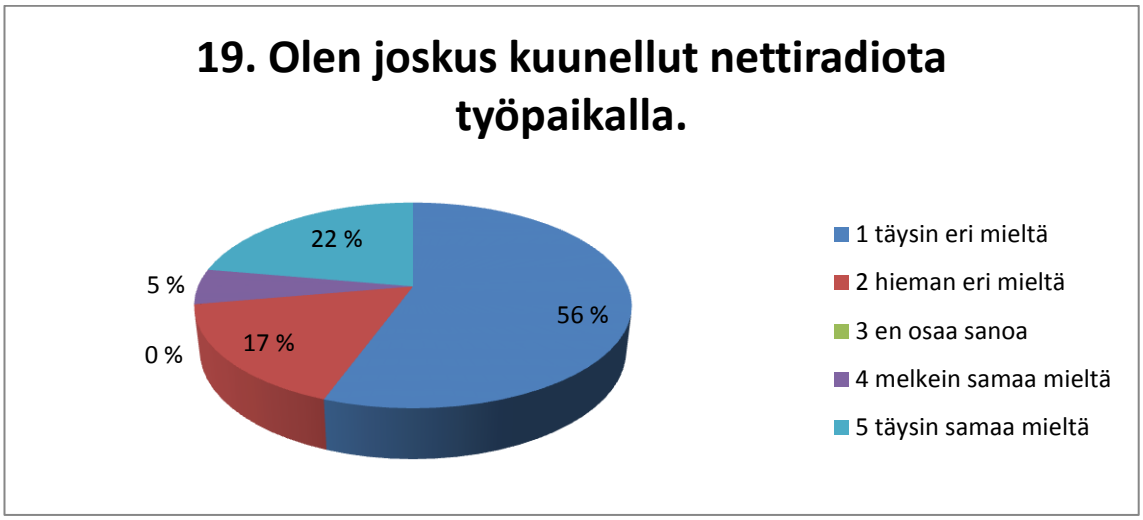
Kuvio 19: Väittämän "17. Olen kohdannut internettiä käyttäessä hankalasti suljettavan pop-up ikkunan." vastausjakauma.

Väitämmässä 17 tiedusteltiin, onko vastaaja kohdannut internettiä käyttäessä hankalasti suljettavan pop-up ikkunan. Vastaajista 4 henkilöä (22%) vastasi"täysin eri mieltä" ja 4 (22%) vastasi "hieman eri mieltä". Vastaajista 5 (28%) vastasi "täysin samaa mieltä" ja 4 henkilöä (22%) vastasi "melkein samaa mieltä". Vastaajista 1 henkilö (6%) vastasi "en osaa sanoa".



Kuvio 20: Väittämän "18. Olen ollut työpaikalla internetsivustolla jolla on ollut huijausviesti tai linkki." vastausjakauma.

Väitämmässä 18 tiedusteltiin, onko vastaaja ollut työpaikalla internetsivustolla jolla on ollut huijausviesti tai linkki. Vastaajista 7 henkilöä (39%) vastasi "täysin eri mieltä" ja 5 (28%) vastasi "hieman eri mieltä". Vastaajista 1 (6%) vastasi "täysin samaa mieltä" ja 1 henkilö (6%) vastasi "melkein samaa mieltä". Vastaajista 4 henkilöä (22%) vastasi "en osaa sanoa".



Kuvio 21: Väittämän "19. Olen joskus kuunellut nettiradiota työpaikalla." vastausjakauma.

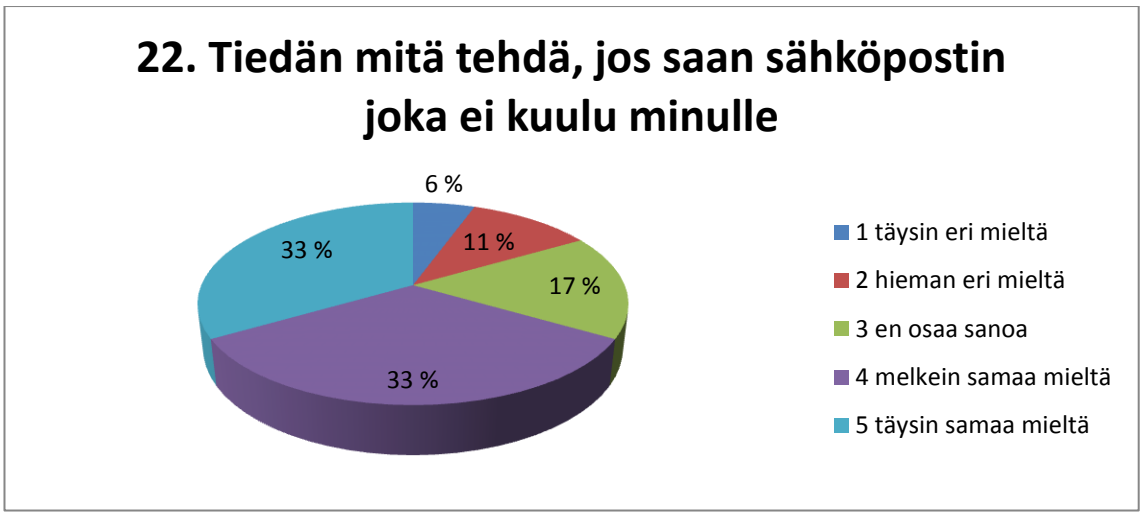
Väitämässä 19 tiedusteltiin, onko vastaaja joskus kuunellut nettiradiota työpaikalla. Vastaajista 10 henkilöä (56%) vastasi"täysin eri mieltä" ja 3 (17%) vastasi "hieman eri mieltä". Vastaajista 4 (22%) vastasi "täysin samaa mieltä" ja 1 henkilö (6%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".

Kuvio 22: Väittämän "20. Tiedän millaisilla sivustoilla saan käydä työkoneella." vastausjakauma.

Väitämmässä 20 tiedusteltiin, tietääkö vastaaja millaisilla sivustoilla saa käydä työkoneella. Vastaajista 1 henkilö (6%) vastasi"täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 8 (44%) vastasi "täysin samaa mieltä" ja 7 henkilöä (39%) vastasi "melkein samaa mieltä". Vastaajista 1 henkilö (6%) vastasi "en osaa sanoa".

Kuvio 23: Väittämän "21. Olen saanut sähköpostia joka ei ole kuulunut minulle." vastausjakauma.

Väitämmässä 21 tiedusteltiin, onko vastaaja saanut sähköpostia joka ei ole kuulunut hänelle. Vastaajista 4 henkilöä (22%) vastasi"täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 7 (39%) vastasi "täysin samaa mieltä" ja 4 henkilöä (22%) vastasi "melkein samaa mieltä". Vastaajista 2 henkilöä (11%) vastasi "en osaa sanoa".

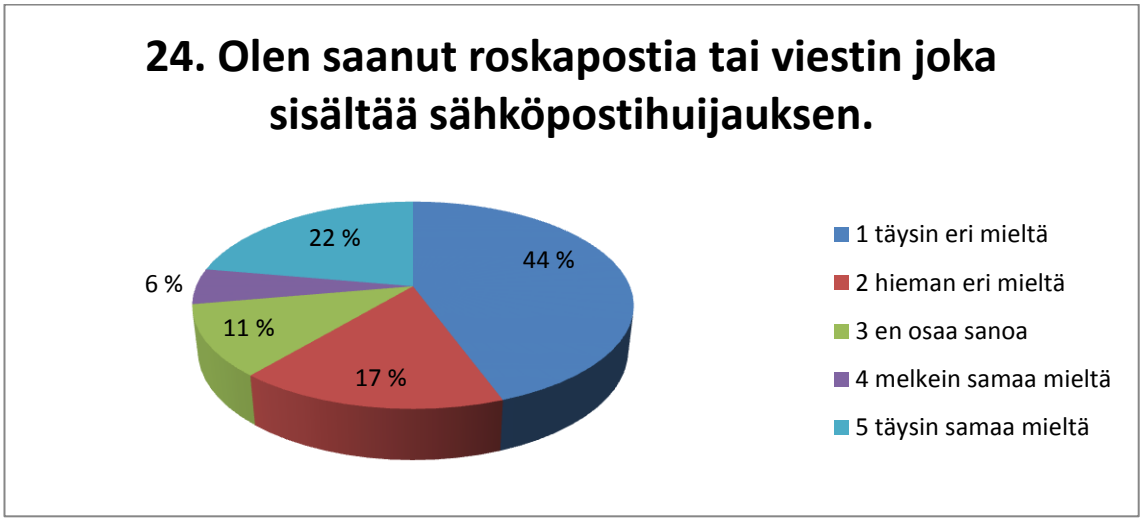


Kuvio 24: Väittämän "22. Olen saanut sähköpostia joka ei ole kuulunut minulle." vastausjakauma.

Väitämmässä 22 tiedusteltiin, tietääkö vastaaja mitä tehdä, jos saa sähköpostin joka ei kuulu hänelle. Vastaajista 1 henkilö (6%) vastasi "täysin eri mieltä" ja 2 (11%) vastasi "hieman eri mieltä". Vastaajista 6 (33%) vastasi "täysin samaa mieltä" ja 6 henkilöä (33%) vastasi "melkein samaa mieltä". Vastaajista 3 henkilöä (17%) vastasi "en osaa sanoa".

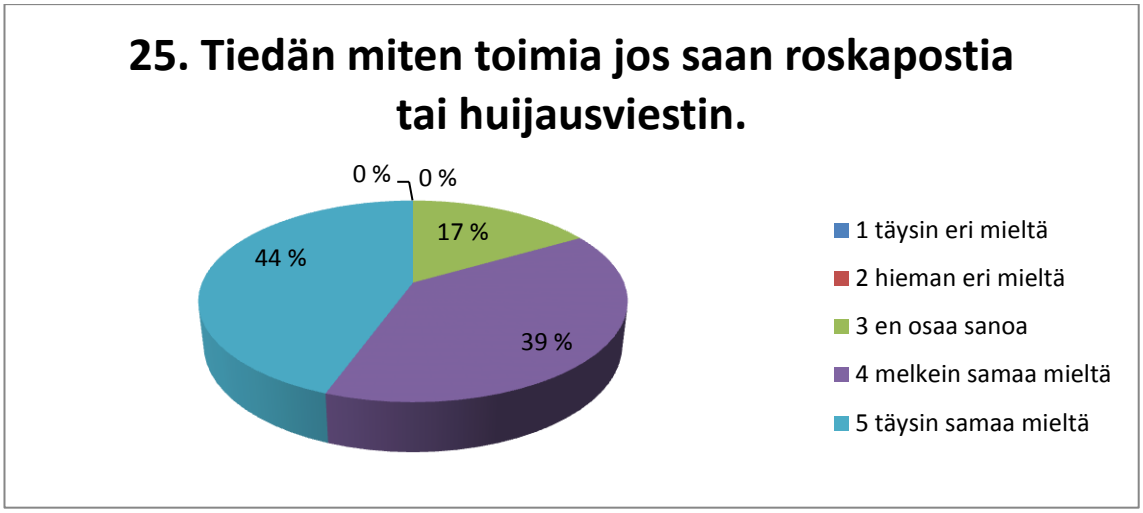
Kuvio 25: Väittämän "23. Olen avannut sähköpostista linkin, josta en ole voinut olla täysin varma mihin linkki johdattaa." vastausjakauma.

Väitämmässä 23 tiedusteltiin, onko vastaaja avannut sähköpostista linkin, josta ei ole voinut olla täysin varma mihin linkki johdattaa. Vastaajista 9 henkilöä (50%) vastasi "täysin eri mieltä" ja 3 (17%) vastasi "hieman eri mieltä". Vastaajista 1 (6%) vastasi "täysin samaa mieltä" ja 2 henkilöä (11%) vastasi "melkein samaa mieltä". Vastaajista 3 henkilöä (17%) vastasi "en osaa sanoa".



Kuvio 26: Väittämän "24. Olen saanut roskapostia tai viestin joka sisältää sähköpostihuijauksen." vastausjakauma.

Väitämmässä 24 tiedusteltiin, onko vastaaja saanut roskapostia tai viestin joka sisältää sähköpostihuijauksen. Vastaajista 8 henkilöä (44%) vastasi"täysin eri mieltä" ja 3 (17%) vastasi "hieman eri mieltä". Vastaajista 4 (22%) vastasi "täysin samaa mieltä" ja 1 henkilö (6%) vastasi "melkein samaa mieltä". Vastaajista 2 henkilöä (11%) vastasi "en osaa sanoa".



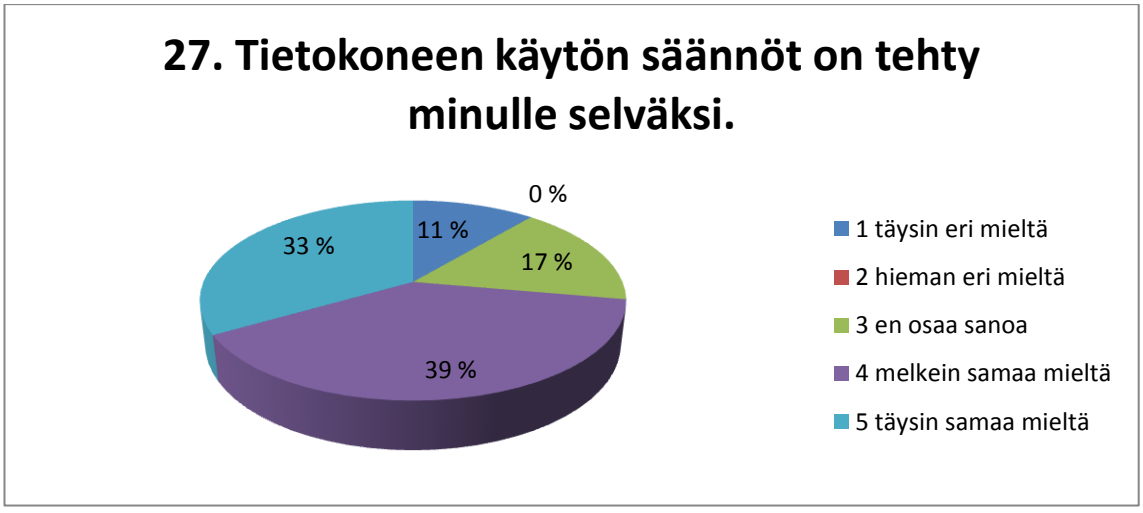
Kuvio 27: Väittämän "25. Tiedän miten toimia jos saan roskapostia tai huijausviestin." vastausjakauma.

Väitämmässä 25 tiedusteltiin, tietääkö vastaaja miten toimia jos saa roskapostia tai huijausviestin. Vastaajista 0 henkilöä (0%) vastasi "täysin eri mieltä" ja samoin 0 (0%) vastasi "hieman eri mieltä". Vastaajista 8 (44%) vastasi "täysin samaa mieltä" ja 7 henkilöä (39%) vastasi "melkein samaa mieltä". Vastaajista 3 henkilöä (17%) vastasi "en osaa sanoa".

4.5 Tietokoneenkäyttö ja mobiililaitteet

Kuvio 28: Väittämän "26. Olen jättänyt tietokoneen päälle päivän päätteeksi, koska koneen uudelleen käynnistys vie liikaa aikaa." vastausjakauma.

Väitämmässä 26 tiedusteltiin, onko vastaaja jättänyt tietokoneen päälle päivän päätteeksi, koska koneen uudelleen käynnistys vie liikaa aikaa. Vastaajista 13 henkilöä (72%) vastasi "täysin eri mieltä" ja 1 (6%) vastasi "hieman eri mieltä". Vastaajista 2 (11%) vastasi "täysin samaa mieltä" ja 2 henkilöä (11%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".

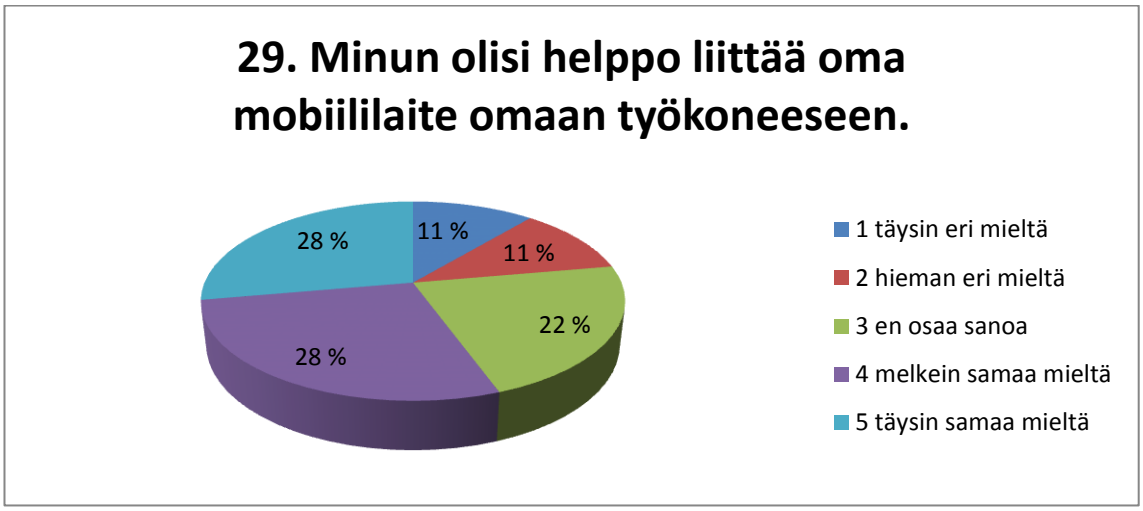


Kuvio 29: Väittämän "27. Tietokoneen käytön säännöt on tehty minulle selväksi." vastausjakauma.

Väitämmässä 27 tiedusteltiin, onko vastaajalle tehty tietokoneen käytön säännöt selväksi. Vastaajista 2 henkilöä (11%) vastasi "täysin eri mieltä" ja 0 (0%) vastasi "hieman eri mieltä". Vastaajista 6 (33%) vastasi "täysin samaa mieltä" ja 7 henkilöä (39%) vastasi "melkein samaa mieltä". Vastaajista 3 henkilöä (17%) vastasi "en osaa sanoa".

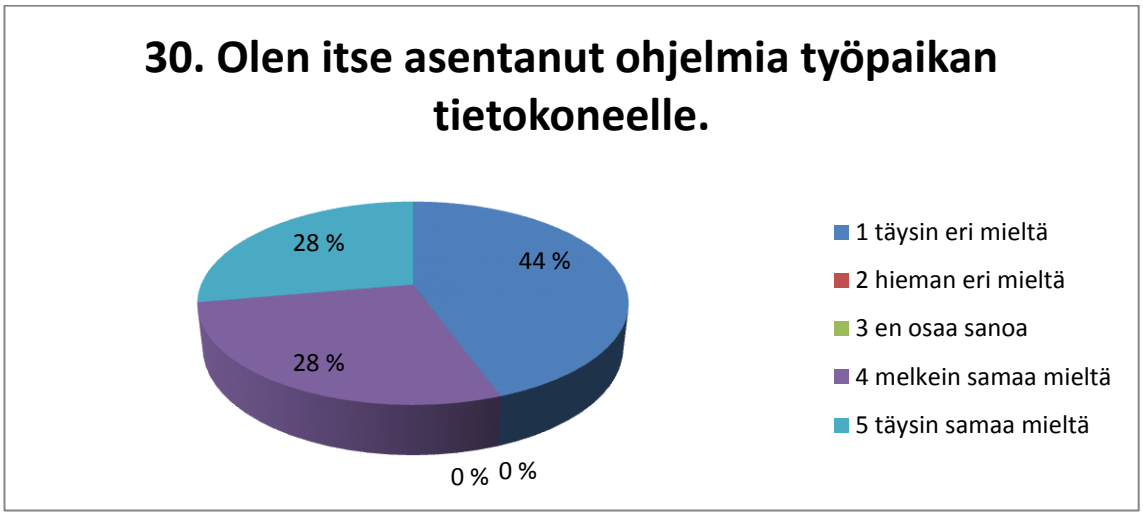
Kuvio 30: Väittämän "28. Mielestäni tiimin yhteisiä kannettavia tietokoneita ja mobiililaitteita käytetään työpaikalla turvallisesti ja oikein." vastausjakauma.

Väitämmässä 28 tiedusteltiin, käytetäänkö vastaajan mielestä tiimin yhteisiä kannettavia tietokoneita ja mobiililaitteita työpaikalla turvallisesti ja oikein. Vastaajista 0 henkilöä (0%) vastasi "täysin eri mieltä" ja 2 (11%) vastasi "hieman eri mieltä". Vastaajista 1 (6%) vastasi "täysin samaa mieltä" ja 9 henkilöä (50%) vastasi "melkein samaa mieltä". Vastaajista 6 henkilöä (33%) vastasi "en osaa sanoa".



Kuvio 31: Väittämän "29. Minun olisi helppo liittää oma mobiililaite omaan työkoneeseen." vastausjakauma.

Väitämmässä 29 tiedusteltiin, olisiko vastaajan helppo liittää oma mobiililaite omaan työkoneeseen. Vastaajista 2 henkilöä (11%) vastasi "täysin eri mieltä" ja 2 (11%) vastasi "hieman eri mieltä". Vastaajista 5 (28%) vastasi "täysin samaa mieltä" ja 5 henkilöä (28%) vastasi "melkein samaa mieltä". Vastaajista 4 henkilöä (22%) vastasi "en osaa sanoa".



Kuvio 32: Väittämän "30. Olen itse asentanut ohjelmia työpaikan tietokoneelle." vastausjakauma.

Väitämmässä 30 tiedusteltiin, onko vastaaja helppo liittää oma mobiililaite omaan työkoneeseen. Vastaajista 8 henkilöä (44%) vastasi "täysin eri mieltä" ja 0 (0%) vastasi "hieman eri mieltä". Vastaajista 5 (28%) vastasi "täysin samaa mieltä" ja 5 henkilöä (28%) vastasi "melkein samaa mieltä". Vastaajista 0 henkilöä (0%) vastasi "en osaa sanoa".

4.6 Avoin kysymys

Viimeisenä kysymyksenä oli avoin kysymys johon vastaaja pystyi kirjoittamaan ideoita ja toivomuksia koskien tietoturva-asioita. Avoimeen kysymykseen vastasi 7 henkilöä. Vastaajien kommentit olivat seuraavat:

"Uusien työntekijöiden koulutukseen selkeä tietoturvapaketti. Työohjeisiin liittyvien kuvien lähetys oman sähköpostin kautta on minusta tosi outoa."

"Perehdytyksessä sivuttiin tietoturva-asioita, mutta olisi suotavaa saada hieman laajempi perehdytys."

"Koulutus kokonaisuudessaan, turvavastaava Saxholm?"

"Työpaikan tietoturvakoulutusta enemmän."

"Selvät pelisäännöt kaikille!"

"Ei voida olettaa, että työntekijät automaattisesti tietäisivät tietoturvasta ilman koulutusta. Tietoturva ei paranna työn tuottavuutta, joten ehkä se selittää kouluttamisen haluttomuutta."

"Käytäisiin ohjeet tarkasti läpi"

5 Johtopäätökset ja kehitysehdotukset

Kyselytutkimuksesta saatiin paljon mielenkiintoisia ja erilaisia mielipiteitä teemojen aiheista. Vastausten antajilla on hyvin erilaisia taustoja ja koulutuksia, mikä luultavasti vaikutti siihen, että kyselytutkimukseen saatiin moneen väittämään paljon vaihtelevia mielipiteitä ja vastauksia. Tässä luvussa on pohdittu sitä, miten kyselytutkimuksen tulokset pystyvät vastaamaan kahteen viimeiseen aikaisemmin esitettyyn tutkimusongelmaan.

5.1 Tietoturvaohjeet ja -politiikka

Tutkimuksessa kävi ilmi, että 56% vastaajista ei ole varma tai ei tiedä mistä yrityksen tietoturvaohjeet ja tietoturvapolitiikka löytyy sekä yli 66% vastaajista ei ole ehtinyt huolellisesti tutustua niihin. Vastaajista vain pieni osa koki ,että työpaikalla on panostettu tarpeeksi tietoturvallisuuteen ja sen koulutukseen. Vastaajista ei ollut kukaan täysin samaa mieltä asiasta ja vain 33% oli melkein samaa mieltä.

Tietoturvallisuudesta ja sen tärkeydestä olisi hyvä saada lisäkoulutusta työntekijöille. Esimies voisi kutsua organisaation turvallisuuspäälikön osastojen viikkopalaveriin kertomaan yrityksen tietoturvallisuudesta ja vastamaan työntekijöiden kysymyksiin. Samalla työntekijät voisivat yhdessä käydä läpi mistä tietoturvapolitiikka ja -ohjeet löytyvät. Uusia koulutuksia pitäisi järjestää useamman kerran vuodessa. Työntekijöille pitäisi myös järjestää aikaa ohjeiden ja politiikan lukemiseen. Tähän soveltuu mainiosti työntekijöille järjestettävät lukutunnit, joita työntekijällä on yksi kuukaudessa.

Kouluttajia haastatellesani kyselytutkimuksen jälkeen kävi ilmi, ettei uusille työntekijöille järjestetä erillistä tietoturvallisuuskoulutusta, vaan uudelle työntekijälle kerrotaan muun koulutuksen ohella miten työpaikalla toimitaan. Tähän pitäisi tulla muutos. Ilman erillästä tietoturvakoulutusta, kouluttajalta saattaa helposti unohtua tärkeitä tietoturvakäytänteitä.

Uuden työntekijän tietoturvakoulutuksessa tulisi käydä tietoturvaohjeet ja -politiikka läpi ja kertoa mistä ne löytyvät.

5.2 Tiedon käsittely ja säilytys

Tutkimuksessa kävi ilmi, työntekijöiden tiedon käsitelyssä ja säilytyksessä on parannettavaa ja puutteita. Yli kaksi kolmas osaa vastaajista on tallentanut tiedostoja työpöydällä tai jonnekin muualle kuin henkilökohtaiselle työasemalle ja samoin yli 60% vastaajista on säilyttänyt joskus asiakastietoja hetkellisesti työpöydällä tai unohtanut vahingossa verkkotulostimeen. Hyvänä toimintapana kuitenkin nähdään, että vain harva työntekijä tulostaa mielummin materiaalit ja ohjeet paperille kuin katsoo ne tallennetuista paikoista, sekä vain yksi työntekijä on käyttänyt henkilökohtaista muistitikkua työpaikalla. Vastaajista vain 33% on mahdollisuus säilyttää muistitikkua ja muita tallenteita lukitussa tilassa.

Näistä havainnoista huolimatta yli 80% vastaajista kokee tieton suojaamisen, tallentamisen ja säilytyksen helpoksi. Tämä viittaa mielestäni siihen, etteivät työntekijät suhtaudu riittävällä vakavuudella tiedon käsiteelyyn ja säilytykseen.

Vaikka tietoturvaohjeistuksessa on kerrottu mihin tiedostot pitää tallentaa, monikaan työntekijä ei noudata ohjeistusta tai ei ole tietoinen asiasta. Asiasta olisi hyvä muistuttaa kaikille osastoilla. Omia kannettavia muistilaitteita vastaajat eivät käytä ja niiden käyttö onkin ohjeistuksessa kielletty. Tietoturvaohjeistukseen voisi lisätä muistutuksen, jossa neuvotaan säilyttämään asiakastietoja ja muita papereita lukitussa tilassa tai tuhoamaan ne heti käytön jälkeen. Ohjeistuksessa voitasiin myös kieltää turhan tiedon tulostamisen jos tiedot löytyvät tietokannasta ja kieltää kaikkien kannettavien muistilaitteiden käyttö jos käyttäjällä ei ole mahdollista säilyttää niitä lukitussa tilassa.

5.3 Salasanat ja käyttöoikeudet

Tutkimuksessa selvisi, että kohderyhmän tietämys salasanoista käyttöoikeiksista on suurimaksi osaksi hyvällä tasolla. Vaikka turvallisuusohjeissa ja turvallisuuspolitikkassa ei ole erillästä ohjeistusta salasanoista, on moni tutkimukseen vastanneista tietoinen miten ja millaisia salasanoja tulee käyttää. Vastaajista 22% prosenttia on säilyttänyt salasanaa paperilla ja yli 90% kokee ettei unohda helposti salasanaa. Yllättävänä voidaan myös pitää sitä, että vain noin 20% vastaajista on käyttänyt salasanaa joka sisältää oman nimen, kaverin nimen, lemmikin nimen tai syntymävuotensa. Huolestuttavana voidaan pitää sitä, että noin puolet vastaajista on jättänyt joskus tietokoneen lukitsematta kun on lähtenyt työpisteeltä.

Työntekijöiden tietämys salasanoista ja käyttöoikeuksista on ilmeisesti tullut muusta koulutusmateriaalista ja suoraan kouluttajilta, koska näitä ohjeita ei löydy tietoturvaohjeista. Salasanojen käyttö ja ohjeet tulisivat ehdottomasti myös olla tietoturvaohjeissa. Näin vielä erikseen painotettaisiin niiden tärkäydestä. Tietoturvaohjeistukseen voitaisiin lisätä seuraavat kohdat:

- Lukitse tietokone aina kun lähdet työpisteeltä
- Vältä salasanojen säilytystä paperilla
- Varmista ettei kukaan näe salasanaasi kun syötät sitä
- Älä sisällytä omaa nimeä, kaverin nimeä, lemmikin nimeä tai synttymävuottasi salasanaan

5.4 Internet ja sähköposti

Tutkimuksen tuloksista voidaan päätellä, että internetin ja sähköpostin käyttöön tarvitaan pientä parannusta. Suurin osa käyttäjistä tietää millaisilla sivustoilla saa käydä työpaikan tietokoneilla mutta silti yli 50% käyttäjistä käyttää yrityksen sisäisen verkon internettiä henkilökohtaisten asioiden selvittämäsiin. Tutkimuksesta selvisi myös ettei välttämättä ymmärrä nettisivujen vaaroja. Yli puolet vastaajista väittää etteivät ole työpaikalla internettiä käyttäessä törmänneet huijausviestiin tai -linkkiin. 44% vastaajista ei ole työpaikalla kohdannut hankalasti suljettavaa opo-up ikkunaa. Vain pieni ryhmä vastaajista tietää mikä ActiveX-riksi on.

Sähköpostin käyttö on vastaajilla paremmalla mallilla. Vastanneista yli 60% on saanut sähköpostia, joka ei ole kuulut heille ja yli 60% käyttäjistä tietää mitä tehdä jos saa sähköpostia joka ei kuulu hänelle. Vain alle 20% vastanneista on ehkä tai varmasti avannut sähköpostin linkin, josta hän ei le ollut täysin varma mihin linkki johdattaa. Vastaajista 20% on saanut työpaikalla roskapostia tai huijausviestin. Pienikin määrä käyttäjistä on sinänsä huolestustuttavaa, sillä työpaikan sähköpostia ei pitäisi käyttää muuhun kun työasioihin. Noin 80% käyttäjistä kuitenkin tietää miten toimia jos saa roskapostia tai huijausviestin.

Organisaation tietoturvaohjeissa kerrottaan lyhyesti mitkä internetsivustot ovat kielletty ja samoin selainsähköpostit ovat kielletty. Lataaminen sivustoilta on myös täysin kielletty. Ohjeissa mainitaan että osa sivustoista on estetty, mutta internetsivujen vaaroista ei mainita mitään. Tarkempi ohjeistus puuttuu myös sähköpostin käytöstä. Ohjeistuksiin voitaisiin lisätä seuraavat kohdat:

- Sähköposti ja Internet ovat työpaikalla tarkoitettu vain työkäyttöön
- Muista tyhjentää internet-selaimen evästeet ja välimuisti riittävän usein

- Älä anna lupaa ActiveX-komponenteille joista et ole täysin varma
- Käytä vain sellaisia sivustoja ja palveluja, jotka tiedät asiallisiksi
- Älä käytä nettiradiota työpaikalla
- Sähköpostin liitetiedostot voivat sisältää vaarallisia haittaohjelmia
- Varo kaikkia epäilyttäviä sähköposteja ja erityisesti liitetiedostoja
- Älä koskaan avaa epäilyttäviä sähköposteja, vaan toimi ohjeistuksen mukaisesti
- Ilmoita epäilyttävistä sähköposteista tietohallintoon
- Älä anna työsähköpostiosoitettasi ulkopuolisille.
- Älä välitä ketjukirjeitä eteenpäin

5.5 Tietokoneenkäyttö ja mobiililaitteet

Tietokoneen ja mobiililaitteden käyttö on tehty vastaajille suhteelisen selväksi. 22% vastanneista on jättänyt laiskuuttaan tietokoneen päivän päätteeksi päälle sekä yli 70% vastaajista kokee, että tietokoneen käytön säännöt on tehty hänelle selväksi. Myös yli puolet vastaajista kokee että yhteisiä kannettavia tietokoneita ja mobiililaitteita käytetään työpaikalla turvallisesti ja oikein. Noin 50% vastaajista on tietoisia että heidän olisi helppo liittää oma mobiililaite työkoneeseen. Kyselystä olisi pitänyt myös kysyä onko vastaaja joskus liittänyt omaa mobiililaitetta työpaikan tietokoneeseen. Yli puolet vastaajista on asentanut ohjelmia työpaikan tietokoneelle. Tämä oli oletettavaa sillä ulkoisenverkon tietokoneille on annettu lupa asentaa ohjelmia, jotta työntekijät voivat itse testailla miten ohjelmat vaikuttavat verkkopankin käyttöön.

Turvapolitiikassa ja ohjeistuksissa on vain hieman sivuttu tietokoneiden ja mobiililaitteiden käyttöä. Tietokoneen ja mobiililaiteiden käyttö on tehty selväksi osastojen yhteisissä pelisäännöissä, mutta tietoturvaohjeistuksesta ne puuttuvat. Ohjeistukseen voitaisiin lisä seuraavat kohdat:

- Vastaat käyttäjänä omasta tietokoneestasi. Ole siis varoivainen ja huolellinen
- Kirjaudu koneelle aina omilla käyttötunnuksilla
- Kirjaudu ulos tai sulje koneesi työpäivän päätteeksi
- Huolehdi kannettavien tietokoneiden ja mobiililaitteiden turvallisuudesta
- Älä säilytä ylimääräistä tietoa kannettavilla tietokoneilla tai mobiililaitteilla
- Älä lataa ja asenna laitteisiin mitään mikä ei kuulu työhösi

5.6 Avoin kysymys ja yhteenveto

Vastaajien kommenteista käy myös ilmi, että lisäkoulutusta ja selkeitä ohjeistuksia kaivataan. Kaikki kommentit koskivat lisäkoulutusta tai vastaajat haluavat selkeitä pelisääntöjä ja ohjeistuksia koskien tietoturvaa. Kommenteista voidaan myös päätellä etteivät vastaajat koe yrityksen suhtautuvan tietoturvallisuuteen tarvittavalla vakavuudella. Jos yritys itse ei suhtaudu sitoutuvasti tietoturvallisuuteen, ei voi olettaa että työntekijät tekisivät niin.

Tutkimuksesta voidaan todeta, että kohderyhmän tietoturvatietoisuudessa olisi kehitettävää. Ohjeistuksesta ja politiikasta puuttuu tärkeitä ja oleellisia osia koskien henkilöstön tietoturvallisuutta. Jokaiseen osa-alueeseen tulisi lisätä tarkennuksia käsitellyistä aiheista. Ohjeistukselle tulisi myös löytää paikka, mistä työntekijä löytää sen helposti. Tällä hetkellä ohjeistusta ja turvapolitiikkaa joutuu etsimään yrityksen laajoista tietokannoista. Tietoturvakouluksen yhteydessä kohderyhmä voisi yhdessä miettiä mikä olisi loogisin paikka tietoturvaohjeille.

Yrityksen olisi myös hyvä miettiä pitäisikö myös tietoturvapolitiikkaa päivittää. Tällä hetkellä politiikka pohjautuu ISO 17799/2000 standardiin, joka on vanhentunut. Kyseinen standardi korvattiin ISO 17799/2005 standardilla, josta myöhemmin tuli ISO 27002/2005 standardi. Yleistä tietoturvaa ei ilmeisesti ole ehditty miettiä, koska yrityksessä on tapahtunut suuria muutoksia ja työpaikoilla on ollut erittäin kiireellistä.

Vaikka kyselytutkimuksesta löydettiinkin paljon hyviä havaintoja, jäi joidenkin kysymysten osalta vastaukset liian avonaiseksi. Joistakin kysymyksistä ei voi olla varmoja saatiinko niistä haluttu vastaus kysymykseen ja voidaanko vastaukseen täysin luottaa. Kysymysten valintaan ja suunitteluun olisi pitänyt panostaa enemmän aikaa. Kyselytutkimuksessa olisi voinut olla enemmän avoimia kysymyksiä, jotka olisivat tukeneet kyselyn väittämiä.

Tutkimuksesta saatu tieto herätti uusia mahdollisuuksia lisäselvityksiin ja jatkotutkimuksiin. Nyt kun kohderyhmän tietoturvatietoisuuden tila on tiedossa voitaisiin mahdollisissa jatkotukimuksilla keskittyä kehittämään kokonaan uusi tietoturvaohjeistus henkilöstölle. Tämä tutkimus kertoo vain työntekijän kannan tietoturvallisuuteen, mikä ei välttämättä anna kokonaiskuvaa tilanteesta. Jatkotutkimuksella, jossa selvitettäisiin myös yrityksen kanta asiaaan, antaisi varmasti toisenlaisia näkökulmia ja selityksiä löydettyhin puutteisiin ja ongelmiin.

Lähteet

Anttila, P. 2007. Realistinen evaluaatio ja tuloksellinen kehittämistyö.
Hamina: Akatiimi Oy.

Hakala,m., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja.
Porvoo: Docendo Finland Oy.

Järvinen, P. 2002. Tietoturva & yksityisyys.
Porvoo: Docendo Finland Oy.

Järvinen, P 2006. Paranna tietoturvaasi.
Porvoo: Docendo Finland Oy.

Järvinen, P. 2009. Salausmenetelmät.
Porvoo: Docendo Finland Oy.

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

Ojasalo,k., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät.
Helsinki: WSOYpro Oy.

Sanastokeskus TSK. 2004. Tiivis tietoturvasanasto.
Helsinki: Taloustieto Oy.

Tipton, H., Krause, M. 2009. Information Security Management Handbook, Sixth Edition.
Boca Raton: Taylor & Francis Group.

Vacca, J. 2009. Computer and InformationSecurity Handbook.
Burlington: Morgan Kaufmann.

VAHTI 2/2008. Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta.
Helsinki: Edita Prima Oy.

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

VAHTI 10/2006. Henkilöstön tietoturvaohje. Valtionvarainministeriö.
Helsinki: Edita Prima Oy.

Whitman, M., Mattord, H. 2012. Principles of Information Security, Fourth Edition.
Boston: Course Technology.

Sähköiset lähteet

IT-Grundschutz Manual 2005. Federal Office for Information Security. Viitattu 13.12.2012
https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html

Yrityksen tietoturvaopas. Tietoturvaopas.fi. Viitattu 9.12.2012
http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html

Dangers of ActiveX and How to Disable It. Winferno Software Viitattu 15.2.2013
http://articles.winferno.com/web-browser-security/dangers-of-activex/

Kuvat ja kuviot

Liite 1: Kyselylomake

1. Tiedän mistä yrityksen tietoturvaohjeet ja tietoturvapolitiikka löytyy

2. Olen ehtinyt huolellisesti tutustua yrityksen tietoturvaohjeisiin ja -politiikkaan

3. Työpaikallani on mielestäni panostettu tarpeeksi tietoturvallisuuteen ja sen koulutukseen

4. Olen säilyttänyt hetkellisesti asiakastietoa työpöydällä tai unohtanut vahingossa verkkotulostimeen.

5. Olen tallentanut tiedostoja työpöydälle tai muualle kun henkilökohtaiseen kansioon.

6. Tulostan ohjeistukset ja materiaalit mielummin paperille kuin katson ne tallennetuista kohteista.

7. Voin säilyttää muistitikkua tai muita tallenteita lukitussa tilassa.

8. Olen käyttänyt henkilökohtaista muistitikkua työpaikalla.

9. Tiedon suojaaminen, talllentaminen ja säilytys on mielestäni helppoa työpaikalla

10. Minulta on jäänyt tietokone lukitsematta kun olen lähtenyt työpisteeltäni.

11. Olen säilyttänyt joskus salasanaa paperilla.

12. Olen kirjoittanut salasanan joskus niin, että joku muu on istunut vierässä ja on voinut nähdä sen.

13. Salasanani on sisältänyt oman nimeni, kaverini nimen, lemmikin nimen tai syntymävuoteni.

14. Unohdan helposti salasanan

15. Käytän myös sisäisen verkon internettiä henkilökohtaisten asioiden selvittämiseen.

16. Tiedän mikä ActiveX-riski on.

17. Olen kohdannut internettiä käyttäessä hankalasti suljettavan pop-up ikkunan

18. Olen ollut työpaikalla internetsivustolla jolla on ollut huijausviesti tai linkki.

19. Olen joskus kuunellut nettiradiota työpaikalla.

20. Tiedän millaisilla sivustoilla saan käydä työkoneella.

21. Olen saanut sähköpostia joka ei ole kuulunut minulle.

22. Tiedän mitä tehdä, jos saan sähköpostin joka ei kuulu minulle.

23. Olen avannut sähköpostista linkin, josta en ole voinut olla täysin varma mihin linkki johdattaa.

24. Olen saanut roskapostia tai viestin joka sisältää sähköpostihuijauksen.

25. Tiedän miten toimia jos saan roskapostia tai huijausviestin.

26. Olen jättänyt tietokoneen päälle päivän päätteeksi, koska koneen uudelleen käynnistys vie liikaa aikaa.

27. Tietokoneen käytön säännöt on tehty minulle selväksi.

28. Mielestäni tiimin yhteisiä kannettavia tietokoneita ja mobiililaitteita käytetään työpaikalla turvallisesti ja oikein.

29. Minun olisi helppo liittää oma mobiililaite omaan työkoneeseen.

30. Olen itse asentanut ohjelmia työpaikan tietokoneelle.

Mitä ideoita ja toivomuksia sinulla on tietoturva-asioista?