LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvatietoisuuden kehittäminen organisaatiossa

Kelloniitty, Mervi

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvatietoisuuden kehittäminen organisaatiossa

Mervi Kelloniitty
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2011

Sisällys

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Mervi Kelloniitty

Tietoturvatietoisuuden kehittäminen organisaatiossa

Vuosi 2011 Sivumäärä 57

Opinnäytetyön päätavoitteena on selvittää kohdeorganisaation tietoturvallisuuden nykytilaa, jotta voidaan kehittää kohdeorganisaatiossa annettavaa tietoturvallisuuskoulutusta niin, että henkilöstö olisi motivoitunutta koulutukseen sekä kokisi tietoturvallisuuden tärkeäksi ja sitoutuisi toiminnassaan noudattamaan annettuja ohjeita ja toimintatapoja.

Opinnäyteyön toteutuksessa on käytetty työelämälähtöistä kvalitatiivista tapaustutkimusta. Opinnäytetyö koostuu kirjallisuusaineistosta, kohdeorganisaation henkilöstölle tehdystä kyselystä ja havainnoinnista kohdeorganisaatiossa. Organisaatiossa ei ole aikaisemmin tehty tietoturvatietoisuuteen liittyvää tutkimusta.

Kyselylomake koostuu neljästä osa-alueesta; tietoturvallisuusasenteet ja – tietoisuus, tietoturvallisuusjohtaminen, oma toiminta ja avoimista kysymyksistä. Kysely lähetettiin sähköpostilla kohdeorganisaation koko henkilöstölle yhteensä 327 henkilölle. Kyselyyn vastasi 87 henkilöä. Kyselyyn vastattiin anonyymisti eli vastaajia ei voitu tunnistaa.

Havainnoinnilla tuettiin kyselyä, koska ei voitu olla varmoja siitä, kuinka avoimesti ihmiset vastaavat omaa toimintaansa koskeviin kysymyksiin

Kyselyn ja havainnoinnin perusteella suurimmiksi haasteiksi ja kehityskohteiksi nousivat henkilöstön asenteet ja suhtautuminen tietoturvallisuuteen, koulutuksen puute sekä työssä käytettävät useat tietojärjestelmät, jotka tarvitsevat kirjautumisen yhteydessä käyttäjätunnusta sekä salasanaa. Kyselyn tulokset antoivat hyvän pohjan tietoturvallisuuskoulutuksen kehittämiselle organisaatiossa.

Asiasanat: tietoturvallisuus, tietoturvatietoisuus, tietoturvakoulutus

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

Mervi Kelloniitty

Developing information security awareness in an organization

Year 2011 Pages 57

The main objective of this thesis is to clarify the current state of the target organization's information security, so that information security training given within the organization can be improved, and so that the staff should be motivated towards the training and feel information security to be highly important as well as be committed to be complying with the given guidelines and practices in their work.

When completing this thesis, a work place-oriented qualitative case study was used. The thesis consists of literary material, a questionnaire designed for the target organization's staff, and of the personal observations within the organization. The organization has not participated in an information security awareness related study before.

The questionnaire consists of four areas: information security awareness and attitudes towards it, information security management and open questions. The questionnaire was sent to the entire staff of the organization, 327 persons in total, via e-mail. 87 employees answered the questionnaire. The questionnaire was answered anonymously, i.e. the participants could not be identified.

The personal observation was designed to support the questionnaire because it could not be guaranteed how openly the participants answered the questions concerning their own actions.

Based on the questionnaire and observation, the major challenges and targets of development were found in the staff's approaches and attitudes towards information security, the lack of training and the multiple information databases used in the organization, which all require a username and a password when logging in the program. The results of the questionnaire gave a good base for developing information security in an organization.

Keywords: information security, information security awareness, information security education

1 Johdanto

Tietoturvallisuus on osa jokaisen organisaation toimintaa ja kokonaisturvallisuutta. Usein tietoturvallisuus mielletään pelkästään tietotekniikaksi, tekniseksi suojaukseksi ja virustorjunnaksi, vaikka suurin osa tietoturvallisuudesta on lähtöisin organisaation oman henkilöstön toiminnasta.

Erään kyselytutkimuksen mukaan pk-yritysten omat työntekijät ovat suurin tietoturvauhka. Kyselystä selviää, että yritykset pyrkivät suojautumaan tietoturvauhkilta pääasiassa teknisin keinoin. Myös sisäisten tietoturvakäytäntöjen puuttuminen sekä yritysjohdon ymmärtämättömyys tietoturvan tärkeydestä koetaan tietoturvauhkina. (Työntekijä on pk-yrityksen suurin tietoturvauhka 2007.) Samansuuntaisia tuloksia on antanut myös eräs eurooppalainen tutkimus, jonka mukaan työntekijät ovat aiheuttaneet 54 % kaikista tietomurroista Euroopassa. (Suurin tietoturvauhka on työntekijä 2008.)

Opinnäytetyö on toteutettu eräässä valtionhallinnon organisaation toimintayksikössä. Opinnäytetyö on tehty työelämälähtöisenä kvalitatiivisena tapaustutkimuksena.

Opinnäytetyön päätavoitteena on selvittää kohdeorganisaation henkilöstön tietoturvatietoisuuden nykytilaa, jotta voidaan kehittää kohdeorganisaatiossa annettavaa tietoturvallisuuskoulutusta niin, että henkilöstö olisi motivoitunutta koulutukseen sekä kokisi tietoturvallisuuden tärkeäksi ja sitoutuisi toiminnassaan noudattamaan annettuja ohjeita ja toimintatapoja. Opinnäytetyössä ei ole tarkoitus tuottaa kohdeorganisaatiolle yksityiskohtaista tietoturvallisuuden koulutussuunnitelmaa, vaan haetaan kohdeorganisaation henkilöstön tarpeiden mukaisia kehitettäviä alueita, joiden mukaan tietoturvallisuuskoulutusta kehitetään.

1.1 Organisaation esittely

Opinnäytetyön kohdeorganisaatio on valtionhallinnon organisaation toimintayksikkö, jossa vakinaista henkilökuntaa noin on 330 henkilöä. Kohdeorganisaation turvallisuuspäällikön mukaan on havaittu, että henkilöstön tietotekninen tietotaito-osaaminen on hyvin eritasoista. Osa henkilöstöstä käyttää tietojärjestelmiä päivittäin, osalla käyttö painottuu muutamaan kertaan kuukaudessa tai jopa muutamaan kertaan vuodessa. Henkilöstön työtehtävät ovat myös hyvin erilaisia. Huomioitavaa on se, että tietoturvallisuus ei ole pelkästään tietojen käsittelyä tietojärjestelmillä, vaan jokaisen työntekijän päivittäiseen toimintaan liittyvä osatekijä. Turvallisuuspäällikkö on työssään havainnut, että tietoturvalliset toimintatavat ovat monelta henkilöltä unohtuneet tai niihin ei kiinnitetä riittävästi huomiota. Moni tietoturvatapahtuma olisi ehkä voitu välttää, jos henkilöstö olisi motivoituneempaa tietoturvaohjeistuksen noudattami-

sessa. Tämän vuoksi organisaation henkilöstön tietoturvatietoisuuteen liittyvien asenteiden tarkastelu on organisaatiossa ajankohtaista.

1.2 Opinnäytetyön tavoitteet ja rajaukset

Opinnäytetyön päätavoitteena on selvittää kohdeorganisaation henkilöstön tietoturvatietoisuuden nykytilaa, jotta voidaan kehittää kohdeorganisaatiossa annettavaa tietoturvallisuuskoulutusta niin, että henkilöstö olisi motivoitunutta koulutukseen sekä kokisi tietoturvallisuuden tärkeäksi ja sitoutuisi toiminnassaan noudattamaan annettuja ohjeita ja toimintatapoja. Kohdeorganisaatiossa on järjestetty kertaluonteisia tietoturvallisuuskoulutuksia henkilöstön perehdyttämisen yhteydessä. Muita tietoturvallisuuteen liittyviä koulutuksia ei ole järjestetty. Uusista muuttuneista toimintatavoista on pyritty informoimaan henkilöstöä tietojärjestelmäkohtaisesti.

Opinnäytetyössä selvitetään, miten tärkeäksi kohdeorganisaation henkilöstö kokee tietoturvallisuuden sekä millainen on henkilöstön tietoturvatietoisuuden taso. Lisäksi selvitetään, kuinka henkilöstö omassa työssään noudattaa ohjeistusta sekä mitkä ovat syyt mahdolliseen ohjeiden vastaiseen toimintaan.

Opinnäytetyö on rajattu koskemaan erästä valtionhallinnon organisaation toimintayksikköä. Opinnäytetyössä ei ole tarkoitus tuottaa kohdeorganisaatiolle yksityiskohtaista tietoturvallisuuden koulutussuunnitelmaa, vaan haetaan kohdeorganisaation henkilöstön tarpeiden mukaisia kehitettäviä alueita, joiden mukaan tietoturvallisuuskoulutusta kehitetään.

2 Tutkimusmenetelmät

Kehittämiskohdetta voidaan lähestyä monin eri tavoin. Lähestymistavan valinta ohjaa kehitystyön tekijää myös tutkimusmenetelmän valinnassa, kuitenkin kaikki menetelmät sopivat mihin tahansa lähestymistapaan. Lähestymistavaksi ei kannata valita vain yhtä, vaan poimitaan eri tavoista parhaat piirteet, jotka sopivat parhaiten omaan työhön. Valinnat kuvataan ja perustellaan kehittämistyöhön liittyvissä raporteissa. Kehittämistyössä käytettäviä tyypillisimpiä lähestymistapoja ovat tapaustutkimus, toimintatutkimus ja konstruktiivinen tutkimus. (Ojasalo, Moilanen & Ritalahti 2009, 51–52.)

Tapaustutkimusta käytetään kun tarkoituksena on tuottaa organisaatiolle kehittämisehdotuksia ja – ideoita esimerkiksi tietoturvallisuuskoulutukseen, jotta henkilöstö olisi motivoituneempaa. Tapaustutkimuksessa kohde valitaan aina käytännön tarpeen mukaan. Tyypillisesti tutkimuskohteeksi valitaan yksittäinen tapaus, tilanne, tapahtuma tai joukko tapauksia, kuitenkin niin, että kohde ymmärretään tiettynä kokonaisuutena. Kohdetta tutkitaan hyvinkin luonnollisissa tilanteissa ja ympäristöissä. Tapaustutkimuksessa pyritään tutkimaan ja selvittämään tapauksia miksi ja miten kysymysten avulla. (Ojasalo ym. 2009, 52–53.)

Tapaustutkimuksessa aiheeseen perehdytään ensin, jotta tiedetään mitä voidaan kysyä. On myös hyödyllistä tutustua aiheeseen liittyvään kirjallisuuteen, jossa on käsitelty samankaltaisia ongelmia kuin omassa kehittämiskohteessa. Usein tutkijalla onkin jo aikaisempaa tietoa kehittämisen kohteesta. Kehittämiskohteen valinta tutkimusprosessin alussa ei ole tärkeää vaan onkin luonnollista, että kehittämiskohde täsmentyy prosessin edetessä. (Ojasalo ym. 2009, 54.)

Tapaustutkimuksessa voidaan käyttää monenlaisia menetelmiä, jotta saataisiin monipuolinen ja kokonaisvaltainen kuva tutkimuskohteesta. Tapaustutkimusta voidaan käyttää niin laadullisissa kuin määrällisissäkin tutkimuksissa. Aineistoa kerätään luonnollisissa tilanteissa mm. havainnoimalla. Tiedonkeruumenetelminä käytetään myös haastatteluita, aivoriihityöskentelyä sekä benchmarkingia. (Ojasalo ym. 2009, 55.)

Kehittämistyössä voidaan käyttää kehittämisen tukena monenlaisia menetelmiä. Perinteisesti tutkimusmenetelmät on jaettu kvantitatiivisiin eli määrällisiin ja kvalitatiivisiin eli laadullisiin menetelmiin. (Ojasalo ym. 2009, 93.) Tutkimusmenetelmän valinta voi olla hankalaa, koska määrällisten ja laadullisten menetelmien raja tutkimuksellisessa kehittämistyössä hämärtyy (Ojasalo ym. 2009, 94).

Kvalitatiivisessa eli laadullisessa tutkimuksessa lähtökohtana on todellisen elämän kuvaaminen. Kvalitatiivisessa tutkimuksessa pyritään kohteen mahdollisimman kokonaisvaltaiseen tut-

kimiseen. Pyrkimyksenä on paljastaa ja löytää tosiasioita kuin todentaa jo olemassa olevia väittämiä. (Hirsjärvi, Remes & Sajavaara 2008, 157.) Ojasalon ym. (2009, 94) mukaan laadullisia menetelmiä käytetään kun tutkitaan aiheita, joita ei ennestään tunneta hyvin ja joita halutaan ymmärtää paremmin. Tutkittavia on huomattavasti vähemmän kuin määrällisessä tutkimuksessa, mutta toisaalta aineistoa syntyy usein runsaasti. Hankitaan siis paljon tietoa suppeasta kohteesta, jotta osattaisiin paremmin ja kokonaisvaltaisemmin ymmärtää ilmiöitä. (Ojasalo ym. 2009, 94.)

Havainnoinnin avulla tutkija saa tietoa siitä, miten henkilöt käyttäytyvät luonnollisissa toimintaympäristöissä ja toimivatko he niin, kuten sanovat toimivansa (Hirsjärvi ym. 2008, 207; Ojasalo ym. 103). Havainnointi ei kuitenkaan ole satunnaista tarkkailua, vaan havainnointia suoritetaan suunnitellusti ja systemaattisesti aina ennalta määrättyyn kohteeseen. Havainnoinnista saadut tulokset pyritään merkitsemään muistiin välittömästi käyttäen apuna havainnointilomakkeita, -päiväkirjaa, videoimalla, valokuvaamalla tai äänittämällä tilanteita. (Ojasalo ym. 2009, 103–104.)

Havainnointi on koettu työlääksi menetelmäksi, koska se vie tutkijalta paljon aikaa. Kyselyt ja haastattelut ovatkin syrjäyttäneet osin havainnointimenetelmät. Kritiikkiä havainnointimenetelmät ovat saaneet siitä, että tapahtuvat tilanteet saattavat häiriintyä tai muuttua havainnoijan läsnä ollessa. Havainnoija saattaa myös liiaksi sitoutua emotionaalisesti tapahtumaan tai henkilöihin. Etuna havainnoinnissa on kuitenkin mielenkiintoisen ja monipuolisen aineiston saaminen. (Hirsjärvi ym. 2008, 208–209.) Tutkijan täytyy havaintoja tehdessään muistaa pitää erillään oikeat havainnot sekä omat tulkinnat havainnoista (Hirsjärvi ym. 2008, 212).

Kyselytutkimuksen avulla voidaan kerätä laaja tutkimusaineisto, jota pidetään kyselyiden etuna. Kysely voidaan saattaa suuren ihmismäärän vastattavaksi ja heiltä voidaan kysyä monia eri asioita. (Hirsjärvi ym. 2008, 190; Ojasalo ym. 2009, 108.) Kyselyt ovat tehokkaita ja tutkijoille aikaa ja vaivannäköä säästäviä. Kun kyselylomake on huolellisesti suunniteltu, voidaan aineisto nopeasti siirtää käsiteltävään muotoon tietokoneella analysoitavaksi. Tutkijoiden käyttöön on kehitelty paljon tilastollisia analysointimenetelmiä, eikä tutkijan tarvitse itse kehitellä niitä. (Hirsjärvi ym. 2008, 190.)

Kyselyillä tuotettavaa tietoa voidaan pitää pinnallisena ja teoreettisesti vaatimattomina. Ei voida myöskään varmistua siitä, ovatko vastaajat suhtautuneet tutkimukseen riittävällä vakavuudella, ovatko vastaajat varmasti ymmärtäneet kysymykset tai väittämät ja tuntevatko vastaajat riittävästi kyselyn aihealueen. Lomakkeen laatiminen vaatii tutkijalta vankkaa pohjatietoa aiheesta sekä laatiminen vie tutkijalta aikaa. (Hirsjärvi ym. 2008, 190.)

Lomakkeen sekä kysymysten laadinnalla ja suunnittelulla voidaan tehostaa tutkimuksen onnistumista (Hirsjärvi ym. 2008, 193). Kyselyä ei kannata tehdä liian pitkäksi, sillä se saattaa heikentää vastaamishalukkuutta. Kysymysten määrän lisäksi harkitaan myös kysymysten järjestystä. Alkuun kannattaa laittaa kysymyksiä, joihin on helppo vastata. Kysymysten tuli olla lyhyitä eikä mitään kysytä varmuuden vuoksi. Kysymyksissä käytetään kieltä, jota vastaajat varmasti ymmärtävät. (Ojasalo ym. 2009, 116.)

Avoimia kysymyksiä käytetään vain jos niiden käyttöön on painava syy tai tiedetään vastaajien olevan aktiivisesti kantaa ottavia. Avoimilla kysymyksillä haettu tieto ei täytä tutkijan odotuksia jos niihin ei vastata. (Ojasalo ym. 2009. 117.) Avoimet kysymykset antavat vastaajille mahdollisuuden kertoa vapaalla sanalla omia näkökantojaan kysyttävästä asiasta, eivätkä ne ehdota valmiita vastauksia (Hirsjärvi ym. 2008, 196).

Asteikkoihin perustuvissa kyselyissä vastaaja valitsee vaihtoehdoista, miten voimakkaasti on samaa tai eri mieltä kuin väittämässä. Asteikkona voidaan käyttää esimerkiksi Likertin asteikkoa. (Hirsjärvi ym. 2008, 195.) 1930-luvulla Renesis Likertin kehittämässä asenneasteikossa olevat osiot ovat useampiluokkaisia. Vastaajille annetaan mahdollisuus valita viidestä vastausmahdollisuudesta eikä hänen tarvitse olla vain samaa mieltä tai eri mieltä. Yleensä vastausvaihtoehdot ovat; ”Täysin samaa mieltä”, ”Jokseenkin samaa mieltä”, ”En osaa sanoa”, ”Osittain eri mieltä” ja ”Täysin eri mieltä”. (Eskola 1975, 211–212.)

Ennen kyselylomakkeen lähettämistä kohderyhmälle, se testataan tavalla tai toisella. Tutkijan on hyvä itsekin vastata kyselyyn. Lähetettäessä lomaketta mukaan kirjoitetaan saatekirje, joka voi tuntua turhalta, mutta se vaikuttaa olennaisesti tutkimuksen onnistumiseen. Saatekirjeestä vastaajille selviää, mistä kyselyssä on kyse ja sen perusteella he tekevät päätöksensä, vastaako kyselyyn vai ei. Saatekirjeen tarkoitus on herättää luottamusta sekä lisätä vastausmotivaatiota. (Ojasalo ym. 2009, 118.)

3 Keskeiset käsitteet

Tietoturvallisuus

Hakalan, Vainion ja Vuorelan mukaan tietoturvallisuuden käsitettä määritellään kirjallisuudessa sekä tietoturvastandardeissa hieman toisistaan poikkeavilla määritelmillä. Kaikista niistä löytyy kuitenkin se yhteinen perusajastus, jonka mukaan organisaatioiden tärkein omaisuus on tieto, jota halutaan suojata. Tieto halutaan pitää luotettavana, oikeassa muodossa olevana sekä oikeiden ihmisten saatavilla. (Hakala, Vainio & Vuorela 2006, 4.)

Tietoturva ja tietosuoja yhdistetään helposti samaksi asiaksi vaikka ovatkin kaksi eri asiaa. Tietosuojan tarkoituksena on suojata ihmisen yksityisyyttä ja tiedollista itsemääräämisoikeutta. Tietoturvan tehtävänä on tarjota erilaisia keinoja ja toimintamalleja tietosuojan ylläpitämiseksi. On tärkeää tietää tietosuojaa koskevat perusasiat. (Laaksonen, Nevasalo & Tomula 2006, 17.)

VAHTI -ohjeistuksen mukaan tietoturvallisuus on tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista normaali- sekä poikkeusoloissa. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä pyritään turvaamaan uhkilta ja vahingoilta. (Käyttäjän tietoturvaohje 2003, 8.)

Tietoturvatietoisuus

Tietoturvatietoisuudella tarkoitetaan henkilöstön sitoutumista organisaation tietoturvallisuuteen. Henkilöstö tuntee tietoturvallisuuden tärkeäksi omassa työssään sekä ymmärtävät, mitä tietoturvallisuudella tarkoitetaan. Henkilöstön tietoturvatietoisuutta nostetaan oikealla ja riittävällä ohjeistuksella sekä koulutuksella. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 5.)

Tietoturvakoulutus

Tietoturvakoulutuksen tavoitteena on saada työntekijät toimimaan johdon haluamalla tavalla niin, että yrityksen tiedot suojataan tarkoituksen mukaisesti. Henkilökunnan ei tarvitse tietää kaikkea tietoturvasta vaan heidän tulee ymmärtää omaan työhönsä liittyvät riskit ja pyrkiä minimoimaan ne. Tietoturvan teknisten ratkaisujen tulisi näkyä työntekijälle mahdollisimman vähän. Koulutuksen suunnittelun tulisi ensisijaisesti pohjautua tietoturvapolitiikkaan ja sitä täydentäviin toimintaohjeisiin sekä prosessikuvauksiin. Myös erilaisissa auditoinneissa tai katselmoinneissa havaittujen tietoturvakäyttäytymisen puutteiden tulisi vaikuttaa koulutuksen sisältöön. Koulutuksen tehokkuus kuitenkin riippuu henkilöstön motivaatiosta. Tietoturvakoulutuksessa tulisi huomioida erilaisten motiivien vaikutus oppimiseen. Käytännön esimerkkien avulla henkilöstölle avautuu parhaiten mitä tietoturvapolitiikalla, ohjeilla ja toimintamalleilla tarkoitetaan. Jos tietoturvaohjeita ei avata käytännön tasolle, tietoturvallisuus ei tule olemaan tavoitteiden edellyttämällä tasolla. Erilaisten esimerkkien avulla on tarkoitus saada työntekijöiden kanssa keskustelua aikaiseksi erilaisista toimintatavoista sekä siitä miten tietoturvaohjeita käytännössä noudatetaan ja miksi niitä tulee noudattaa. (Laaksonen ym. 2006, 254–255.)

4 Tietoturvallisuuden ohjaus valtionhallinnossa

Valtiovarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. Johtoryhmä käy läpi valtionhallinnon tietoturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset. Johtoryhmä ohjaa valtionhallinnon tietoturvatoimenpiteitä. VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä. (Valtiovarainministeriö 2011.)

Valtioneuvoston periaatepäätös edellyttää, että kaikilla valtionhallinnossa työskentelevillä henkilöillä on riittävä tietoturvaosaaminen. Henkilöstön tietoturvatietoisuutta olisi seurattava säännöllisesti ja kehitettävä jatkuvasti. (Tietoturvallisuudella tuloksia 2007, 52.) Ohjeistamalla, kouluttamalla, kehittämällä työmenetelmiä ja vaikuttamalla asenteisiin pyritään vähentämään oman henkilöstön aiheuttamia tuottamuksellisia tietoturvallisuuteen liittyviä uhkia. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 21.) Tietoturvallisuus liittyy oleellisesti organisaation kokonaistoimintaan, joten henkilöstön sitouttaminen turvallisuusnäkökulmasta on ensiarvoisen tärkeää. Henkilöstön tietoturvallisuustietoisuuden kehittämisen täytyy olla jatkuvaa. (Tietoturvallisuudella tuloksia 2007, 52.)

Organisaation tietoturvallisuus on pääsääntöisesti riippuvainen henkilöstön toiminnasta. Hyvät järjestelmät ja välineet eivät auta jos niitä ei käytetä tai osata käyttää oikein. Henkilöstön toiminnan ohjeistus, koulutus ja motivointi tietoturvallisiin toimintatapoihin ovat ensiarvoisen tärkeitä asioita. Henkilöstöturvallisuudella, käsiteltäessä tietoturvallisuuden yhtenä osa-alueista, tarkoitetaan henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä. Organisaatioiden koko toiminnan haasteena on ihminen. Henkilökunta muokkaa, tallettaa, vastaanottaa, välittää ylläpitää ja lopulta tuhoaa tietoa. Henkilöstö on avainasemassa tietoturvan toteuttamisessa. Henkilöstöturvallisuuden tehtävä on henkilöstö aiheutuvien riskienhallinta. Keinot henkilöstöturvallisuuteen ovat riskianalyysit, avainhenkilöstön määrittelyt, varahenkilöjärjestelyt, työsuhteen elinkaaren hallinta ja tietenkin koulutus. Henkilöstöturvallisuuden toteutuminen kertoo organisaation tietoturvakulttuurin tason ja hyvän tiedonhallin-tavan toteutumisen. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008, 12.)

VAHTI 5/2003 määrittelee tietoturvallisuuden kolme keskeisintä käsitettä luottamuksellisuus, eheys ja käytettävyys. Voidaan puhua myös tietoturvallisuuden kolmesta ulottuvuudesta. (Käyttäjän tietoturvaohje 2003, 8.)

Luottamuksellisuudella tarkoitetaan keinoja, joilla taataan käyttöoikeuksien omaaville henkilöille pääsy tietoihin ja järjestelmiin niin, ettei sivullisilla ole mahdollisuutta päästä tietoon käsiksi. (Käyttäjän tietoturvaohje 2003, 8.)

Eheydellä tarkoitetaan keinoja, joilla taataan tietojen ja järjestelmien pysyminen luotettavina, oikeina ja ajantasaisina niin, etteivät ne ole hallitsemattomasti muuttuneet tai muutettavissa minkään tapahtuman tai toiminnan seurauksena. (Käyttäjän tietoturvaohje 2003, 8.)

Käytettävyydellä tarkoitetaan keinoja, joilla taataan että, järjestelmien tiedot ja palvelut ovat niihin oikeutettujen henkilöiden käytettävissä etukäteen määritellyssä vasteajassa eivätkä tiedot ole tuhoutuneet tai tuhottavissa minkään tapahtuman tai toiminnan seurauksena. (Käyttäjän tietoturvaohje 2003, 8.)

VAHTI -ohjeissa määritellään tietoturvatoiminta kahdeksaan osa-alueeseen, joita hallintajärjestelmällä ohjataan ja joiden tehokkuutta palautejärjestelmällä mitataan. Näitä ovat hallinnollinen tietoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoaineistoturvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus ja käyttöturvallisuus. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003.)

5 Tietoturvallisuuteen liittyviä riskejä

Organisaatioiden ja niiden henkilöstön kaikkeen toimintaan liittyy epävarmuus, joka on tietämättömyyttä tai epätietoisuutta tulevista tapahtumista. Seuraukset voivat olla negatiivisia tai positiivisia. Etukäteissuunnittelulla pyritään parantamaan turvallisuutta ja tulevaisuuden ennustettavuutta. Riski -käsitteellä kuvataan yleisesti mahdolliseen onnettomuuteen liittyvää vaaraa ja epätietoisuutta. Riskin toteutuessa menetykset kohdistuvat mihin tahansa arvon menetykseen, kuten esimerkiksi rahallisen arvon, ympäristöarvon, terveydellisen arvon taikka yhteiskunnallisen arvon menetyksinä. Kun riskejä määritellään, tarkastellaan epätoivotun seurauksen haitallisuutta sekä todennäköisyyttä. (Kuusela & Ollikainen 2005, 15–17.)

Riskienhallinta tietoturvallisuuden kannalta liittyy keskeisesti erilaisiin tietovarantoihin, arkistoihin sekä niiden käyttöön, mutta myös tiedonsiirtoon ja sanomavälitykseen verkoissa. Organisaatioiden toiminnassa henkilöstö on huomattavassa asemassa ja riskit kohdistuvatkin osin heidän tapoihinsa toimia. Kaikki tekevät joskus virheitä, mutta niiden määrä voidaan pienentää kokemuksen sekä koulutuksen avulla. Lisäksi organisaation täytyy tuottaa ohjeet sekä selkeät työnjaot virheiden minimoimiseksi. Henkilöstön toiminnan lisäksi riskejä syntyy erityisesti tietotekniikan välineistön, laitteiden ja ohjelmistojen nopeasta muuttumisesta. (Kuusela & Ollikainen 2005, 243–244.)

Vaarallisia työyhdistelmiä syntyy kun tehtäviä ja niiden mukaisia valtuuksia yhdistetään. Työtehtävien yhdistely tapahtuu usein huomaamatta ajan kuluessa tai esimerkiksi henkilön sairastuessa, hänen tehtäviään jaetaan muille tilapäisesti suoritettavaksi. Sen seurauksena tietojärjestelmien käyttö- ja käsittelyoikeuksia on laajennettava, jolloin sijainen pääsee käsiksi tietoihin, joihin hänellä ei oikeuksia aiemmin ollut. Väliaikainen järjestely voi muodostua vakinaiseksi ja työyhdistelmään liittyvät vaarat unohtuvat. (Kyrölä 2001, 85–86.)

Salassapito- ja vaitiolositoumuksen allekirjoitettuaan henkilö saa luvan perehtyä organisaation salassa pidettävään tietoon, mikäli niitä työtehtävissään tarvitsee. Salassapitosopimuksen allekirjoitettuaan, henkilö sitoutuu olemaan paljastamatta organisaation salassa pidettäviä tietoja asiattomille tai muutoin sitoutumattomalle taholle. (Laaksonen ym. 2006, 141.) Työsuhteen päättymisen jälkeen, henkilöä on miltei mahdotonta estää käyttämästä tietopääomaansa, kokemustaan ja osaamistaan, johon liittyy tietoutta edellisestä työpaikasta (Kyrölä 2001, 88).

Tietosuoja eli yksityisyys pyrkii takaamaan sen, että kaikki henkilöön liittyvä tieto, josta henkilö voidaan tunnistaa, on suojattu asiattomalta käytöltä. Tiedot ovat vain niiden käytettävissä, jotka tietoja työtehtävien hoidossa tarvitsevat. Yksityisyyden suoja vaarantuu esimerkiksi silloin, jos henkilöä koskevat tiedot ovat virheellisiä tai joutuvat asiattomien tietoon. Yksityisyyden suoja voi myös vaarantua jos asiankäsittelijät käsittelevät henkilötietoja sisältäviä asiakirjoja huolimattomasti ja asiattomat pääsevät lukemaan tietoja. Myös puhelimitse voi tapahtua henkilötietojen tietovuotoja tai tietojen urkintaa. Henkilötietoja sisältävät sähköpostit saattavat ohjautua väärään osoitteeseen tai paljastua yleiselle kirjoittimelle tulostettuna. (Kyrölä 2001, 96.)

Käyttöoikeudet eri tietojärjestelmiin myönnetään tehtävänkuvan perusteella (Laaksonen ym. 2006, 142). Laaksonen, Nevasalo ja Tomula (2006, 151) toteavat käyttöoikeuksien hallinnan olevat hyvin yksinkertaista. Käyttäjille annetaan vain ne oikeudet, joita he työtehtävissään tarvitsevat. Oikeudet poistetaan välittömästi, kun niitä ei enää tarvita. Käyttäjien hallinta on perustunut jo pitkään käyttäjätunnukseen ja salasanaan. Käyttäjien hajauttaminen eri tietojärjestelmiin tai palveluihin on kasvattanut luvattoman käytön riskejä. Käyttäjille tilanne muodostuu usein hankalaksi jos käytössä on monia eri järjestelmiä, joihin jokaiseen on eri käyttäjätunnukset ja salasanat. Yhdellä tunnuksella kirjautuminen olisi käyttäjille yksinkertaisempaa. Tällöin tunnuksen jouduttua ulkopuolisen haltuun, väärinkäyttäjällä on käytettävissään kaikki kyseiselle tunnukselle kuuluvat palvelut. (Kuusela & Ollikainen 2005, 246.)

Salasanojen heikkous on merkittävä tietoturvariski (Laaksonen ym. 2006, 178). Salasanoja säilytetään näppäimistön alla, työpöydällä tai muistikirjassa ja tällöin ne ovat helposti yhdistettävissä käyttäjään. Salasanoja pitäisi vaihtaa säännöllisesti sekä aina kun epäillään sen joutuneen vääriin käsiin. Salasanojen vaihtamisellakin on omat riskinsä. Jos salasana vaihdetaan usein, se helposti unohdetaan ja se kirjoitetaan muistiin. Salasanoja ja käyttäjätunnuksia lainataan toisille henkilöille. (Kuusela & Ollikainen 2005, 247–248.)

Tahattomien virheiden seurauksena tietojen sisältö voi muuttua toiseksi tai käyttökelvottomaksi, se voi hävitä osittain tai kokonaan, tuhoutua tai paljastua väärään aikaan. Tahattomia virheitä sattuu normaalien arkirutiinien yhteydessä. Salassa pidettävää tietoa luovutetaan ilman vastaanottajan henkilöllisyyden varmistamista tai luovutetaan taholle, jolle tietoa ei saisi luovuttaa. Tärkeitä asiakirjoja postitetaan vanhentuneisiin osoitteisiin. Henkilöstö jättää työasemat lukitsematta poistuttaessa työtilasta ja näin mahdollistetaan tiedon urkinta. Kun huomataan, että on toimittu tahattomasti väärin, hätäännytään ja unohdetaan toimintatavat, jolloin virheet kertaantuvat. Syitä virhetilanteiden syntymiseen voivat olla kiire, osaamattomuus, tiedon puute, ohjeistuksen puute tai epätarkkuus, välinpitämättömyys tai ohjeiden vastainen toiminta. (Kyrölä 2001, 98–99.)

Laiminlyönnin tapahtuessa, henkilö on jättänyt hänelle määrätyn tehtävän tarkoituksella suorittamatta tai hän ei noudata organisaation toimintaohjeita. Laiminlyönnin seurauksena tiedot voivat joutua ulkopuolisten käsiin tai jotkin tärkeät tiedot jäävät päivittämättä. Tietoturvarikkomukset ovat yleensä laiminlyöntejä. Laiminlyönnit johtuvat useimmiten huolimattomuudesta, välinpitämättömyydestä tai unohduksista. Henkilö voi olla liian kiireinen, ylirasittunut, jostain syystä järkyttynyt, huonokuntoinen, sairas tai toimii jostain syystä eri tavalla kuin normaalisti. (Kyrölä 2001, 102–103.)

Tietovuoto on esimerkiksi tilanne, jolloin henkilö kertoo ajattelemattomuuttaan asioita taholle, jolle tieto ei kuulu. Asioista puhutaan puhelimessa tai niin äänekkäästi, että ulkopuolinen taho kuulee puheen. Asioista puhutaan kotona, vapaa-ajan harrastuksissa tai jollekin muulle tuttavalle, joiden kautta tiedot leviävät edelleen. Tietovuoto voi olla myös tahallinen. Henkilö tietää mitä tietoa on ottanut haltuunsa ja mitä on paljastamassa. (Kyrölä 2001, 108–190.)

Tietojen urkkimisella tarkoitetaan tilannetta, jolloin henkilö hankkii organisaatiosta itseään tai kolmatta osapuolta kiinnostavia tietoja. Luvaton asiakirjojen selailu tai järjestelmissä olevien tietojen tutkiminen on urkintaa. Jos työssä käsitellään henkilö-, tili-, eläke-, verotus-, rikos- tai terveystietoja ja uteliaisuudesta katsellaan tietoja naapurista tai tuttavasta, syyllistytään näiden henkilöiden yksityisyyden suojan rikkomiseen. (Kyrölä 2001, 112.)

6 Motivointi

Peltonen ja Ruohotie (1987, 15) vertaavat motivaatiota ja asenteita vertauskuvauksellisesti säätilaan ja ilmastoon. Motivaatiota kuvataan säätilaksi, jonka kohdealue on suppea, aikajänne lyhyt ja nopeasti muuttuva. Asenteita kuvataan ilmastoksi, jonka alue on laaja, aikajänne pitkä ja muuttaminen vaikeaa. Jos halutaan selvittää johtuuko jokin ongelma säätilasta vai ilmastosta ja tilanteeseen halutaan parannusta, täytyy tietää onko kyse motivaatiosta vai asenteesta. Motivaation parantaminen edellyttää tilanteen mukaisia toimenpiteitä, esimerkiksi tulospalkkausta, välitöntä ohjausta ja palautteen antamista. Asenteisiin voidaan vaikuttaa pitkäaikaisemmilla toimenpiteillä, esimerkiksi henkilöstön ja organisaation kehittämistoimilla.

Motivaation kantasana on motiivi. Motiivista puhuttaessa viitataan tarpeisiin, haluihin, vietteihin, palkintoihin sekä rangaistuksiin, jotka ylläpitävät ihmisen käyttäytymisen suuntaa kohti päämääriä. Motiiveja pidetäänkin päämääräsuuntautuneina, joko tiedostetusti tai tiedostamattomasti. Motiivien aikaansaamaa, tiettyyn tilanteeseen liittyvää psyykkistä tilaa, kutsutaan motivaatioksi. Se määrää sen, miten vireästi, millä aktiivisuudella ja millä ahkeruudella ihminen toimii sekä mihin hänen mielenkiintonsa suuntautuu. Riippuu siis motivaatiosta miten halukkaasti henkilö käyttää omia fyysisiä ja henkisiä voimavarojaan esimerkiksi työtä tehdessään. (Peltonen & Ruohotie 1987, 23; Ruohotie 1998, 36–37.)

Kannusteet vaikuttavat siihen, miten innokkaasti ihminen tavoitteisiin pyrkii. Kannusteet voivat palkita joko sisäisesti tai ulkoisesti. Vastaavasti motivaatio voidaan jakaa sisäisiin motivaatioihin ja ulkoisiin motivaatioihin. Niitä ei kuitenkaan täysin voida pitää erillisinä, vaan ne täydentävät toisiaan. Sisäisessä motivaatiossa toiminta itsessään tuottaa mielihyvää suorituksen lopputuloksen sijasta, esimerkiksi ihminen kokee työniloa työn sisällön vuoksi. Sisäisesti motivoitunut opiskelija opiskelee, koska on kiinnostunut aiheesta tai saa tekemisestä mielihyvää. Sisäinen motivaatio tuo parhaiten esille ihmismielen positiivisen pyrkimyksen etsiä uusia haasteita, laajentaa ja harjoittaa omaa kyvykkyyttä, tutkia ja oppia. Sisäinen motivaatio on spontaania kiinnostusta ja omien rajojen tutkimista sekä se on lähde ilolle ja elämänhalulle koko elämän ajan. Sisäinen motivaatio on tärkeä motivaation tyyppi, mutta se ei ole ainoa. Se heikkenee jos koemme, että toiset yrittävät ohjata toimintaamme palkkioiden avulla. Suurin osa ihmisten päivittäisistä tekemisistä ei ole sisäisesti motivoitunutta toimintaa. Sisäinen mo-

tivaatio ja kiinnostus haastaviin tehtäviin ja osaamiseen tähtäävä ponnistelu voivat olla pysyviä persoonallisuuden piirteitä. Näin ollen se ei ole vain ohimenevä tila, joka katoaa kun tekeminen menettää uutuudenviehätyksensä. Ulkoinen motivaatio perustuu saataviin palkintoihin, kuten hyviin tenttiarvosanoihin, rahaan, muiden osoittamaan ihailuun, kiitokseen tai rangaistuksen pelkoon. Lähteenä ulkoiselle motivaatiolle voi olla esimerkiksi opiskelumenestyksestä saatava stipendi. Ulkoinen motivaatio voi vähitellen sisäistyä. Opiskelija voi esimerkiksi alkaa työskennellä ahkerammin itsearvostuksensa kohottamiseksi. Vähitellen hän löytää enemmän syitä miksi kannattaa opiskella ja lopulta itse opiskelu muodostuu hänelle tärkeäksi. (Peltonen & Ruohotie 1987, 25–26; Ruohotie 1998, 37–41.)

Asenteet ovat pysyvämpiä, sisäistyneitä ja hitaammin muuttuvia reaktiovalmiuksia. Asenteet vaikuttavat enemmän toiminnan laatuun kuin motivaatio. Asenteet vaikuttavat ihmisen taipumukseen tuntea, ajatella ja toimia tietyillä tavoilla. Asenteet ilmaisevat suhtautuuko ihminen positiivisesti tai negatiivisesti johonkin objektiin, ihmiseen tai tilanteeseen. Ihmisen kokemukset ja taipumukset sekä asioiden sisäistämisaste vaikuttavat asenteiden laatuun ja voimakkuuteen. Kun ihminen kokee onnistumisen tunteen jossakin asiassa, on hänen asennoitumisensa kyseiseen asiaan todennäköisesti jatkossa myönteisempää, joten hän lisää ponnistelujaan ja alkaa kehittää omia suoritusvalmiuksiaan. (Ruohotie 1998, 41–42.)

Ihmisen työsuorituksiin vaikuttavat myös motivaatio ja valmius. Valmiudella tarkoitetaan ihmisen edellytyksiä suoriutua annetuista tehtävistä. Ihmisen valmius riippuu motivaatiosta sekä päinvastoin ja ovat näin vuorovaikutuksessa keskenään. Ihmisen valmiuteen vaikuttavat esimerkiksi kyvyt, luonteenpiirteet, arvot, asenteet, tiedot ja taidot. Nämä valmiuteen vaikuttavat tekijät eivät muutu helposti tilanteesta toiseen vaan ovat melko pysyviä. (Peltonen & Ruohotie 1987, 26–27.)

7 Tietoturvatietoisuuden tutkimus kohdeorganisaatiossa

Tässä opinnäytetyössä on käytetty työelämälähtöistä kvalitatiivista eli laadullista tapaustutkimusta. Työ koostuu kirjallisuusaineistosta, kohdeorganisaation henkilöstölle tehdystä tietoturvatietoisuuskyselystä ja havainnoinnista kohdeorganisaatiossa.

Tietoturvatietoisuuskysely koostui neljästä osa-alueesta; tietoturvallisuusasenteet ja – tietoisuus (kysymykset nro 1 – 40), tietoturvallisuusjohtaminen (kysymykset 41–50), oma toiminta (kysymykset nro 51 - 80) ja avoimet kysymykset (nro 81 – 87). Tietoturvallisuusasenteet ja – tietoisuus väittämillä selvitettiin henkilöstön tietämystä, motivaatiota sekä asenteita organisaation tietoturvallisuutta kohtaan. Tietoturvallisuusjohtamisosion väittämillä selvitettiin henkilöstön mielipiteitä johdon osallistumisesta organisaation tietoturvallisuustyöhön. Oman toiminnan väittämillä selvitettiin, kuinka henkilöstö itse ottaa tietoturvallisuuden huomioon

päivittäisessä työssään. Avoimilla kysymyksillä haluttiin henkilöstön mielipiteitä tietoturvallisuuden epäkohdista kohdeorganisaatiossa sekä mahdollisia ehdotuksia koulutuksen kehittämiseen ja tietoturvallisuusmotivaation kasvattamiseen henkilöstön keskuudessa. Kyselyn väittämäkysymykset on esitelty osioittain taulukoissa 1 – 3 ja avoimet kysymykset luvussa 9.4.

Kysely toteutettiin Eduix E-lomake 3.1 ohjelmalla. Kyselylomakkeen laatiminen ohjelmalla oli yksinkertaista ja vastauksia käsiteltiin helposti yksittäin tai kootusti. Ohjelmasta saatiin myös helposti lomakkeen kentillä kerätyt tiedot näkyviin graafisesti havainnollistettuna.

Väittämäkysymyksissä käytettiin viisiportaista Likertin asteikkoa:

1 Täysin eri mieltä
2 Jokseenkin eri mieltä
3 En osaa sanoa
4 Jokseenkin samaa mieltä
5 Täysin samaa mieltä

Kysely testattiin ennen kyselyn lähettämistä koko kohdeorganisaation henkilöstölle. Kyselyn testaukseen osallistui kolme henkilöä organisaation eri toimintayksiköstä. Testauksessa olleet henkilöt eivät osallistuneet varsinaiseen kyselyyn. Testauksessa esiin tulleiden kommenttien mukaan kyselyn rakenteeseen tehtiin muutoksia sekä joitakin kysymyksiä selvennettiin.

Kyselyn vastaanottajina olivat kohdeorganisaation koko henkilöstö. Kysely lähetettiin 327 henkilölle organisaation sisäisellä sähköpostilla. Sähköpostiviestiin kirjoitettiin saatesanat liitteen 1 mukaisesti.

Vastausaikaa kyselyllä oli kolme viikkoa. Kahden viikon kuluttua kyselyn lähettämisestä henkilöstölle lähetettiin muistutus kyselyyn vastaamisesta (liite 2).

Havainnoinnin aikana kerättiin tutkimustietoa kohdeorganisaation henkilöstön tietoturvallisista toimintatavoista satunnaisesti eri työpisteillä. Havainnointitietoja kerättiin kahden viikon aikana. Havainnointiin osallistui tutkijan lisäksi kohdeorganisaation turvallisuuspäällikkö. Havainnointitietoja kerättiin pääsääntöisesti virka-aikana normaalin päivätyön ohella, eikä henkilöstöä tiedotettu havainnoinnista. Havainnoinnilla toivottiin saatavan hyödyllisiä tietoja henkilöstön toimintatavoista. Saatavat tiedot tukevat ja täydentävät kyselyillä saatuja tietoja.

Havainnoinnissa tarkasteltiin henkilöstön toimintaa seuraavien kysymysten pohjalta:

- Onko henkilöillä henkilökortti näkyvillä?
- Onko rakennuksen ulko-ovet suljettuina vai auki?
- Onko ikkunat suljettuina vai auki?
- Ovatko osastojen väliset sähköisesti lukitut ovet kiinni?
- Ovatko palo-ovet kiinni?
- Ovatko toimistojen ovet lukittuina jos henkilö ei ole paikalla?
- Ovatko ikkunat auki vai suljettuina?
- Jos huoneeseen on vapaa pääsy, onko henkilön toimikortti kaikkien saatavilla?
- Jos toimikortti saatavilla, onko siihen liittyvä PIN – koodi saatavilla?
- Onko tietojärjestelmien käyttäjätunnuksia ja/tai salasanoja saatavilla?
- Onko USB – muistivälineitä saatavilla? Saako USB – muistivälineeltä tiedon vapaasti käytettäväksi?
- Onko muita ulkoisia tallenteita (CD, DVD) saatavilla? Työasemassa?
- Jos huoneessa ei ole ketään, onko työasemalta kirjauduttu ulos?
- Onko kassakaapin ovi suljettuna? Lukittuna?
- Onko pöydällä turvaluokiteltua materiaalia? Jo on niin mitä?
- Onko roskakorissa turvaluokiteltua materiaalia?
- Puhuvatko henkilöt niin, että tieto saattaisi vuotaa ulkopuolisille?
- Havaitaanko tietojen urkkimista?

8 Tietoturvatietoisuustutkimuksen tulokset

Kyselyyn vastasi 87 henkilöä, kun kyselyn vastaanottaneita oli 327 henkilöä. Kun vastaajamäärää verrataan kaikkien vastauksien määrään, saadaan kyselyn vastausprosentiksi 26,6 %. Kyselyyn saatiin vastauksia ensimmäisen päivän aikana 14 kappaletta ja ensimmäisen viikon aikana yhteensä 38 kappaletta. Toisen kyselyviikon aikana vastauksia saatiin yhteensä 14 kappaletta. Kolmannen kyselyviikon alussa lähetetyn muistutusviestin jälkeen, saapui samana päivänä 2 vastausta ja kolmannen kyselyviikon aikana saapui yhteensä 35 vastausta.

Ennen varsinaista vastauksien analysointia, vastaukset tarkastettiin. Kaikki vastaukset, joissa 80 väittämästä oli vastattu alle 75 väittämään, hylättiin. Yksi vastauslomake hylättiin, koska siinä ei ollut vastattu yhteenkään kysymykseen. Vastauksien hylkäysprosentti on 1,1 %. Kyselyn avoimiin kysymyksiin oli vastattu 60 vastauslomakkeessa, jolloin 69,8 % vastaajista vastasi myös avoimiin kysymyksiin. Kaiken kaikkiaan 12 vastaajaa eli 20,0 % kaikista avoimiin kysymyksiin vastanneista oli antanut vastauksen jokaiseen seitsemään avoimeen kysymykseen.

Tietoturvatietoisuuskyselyn analysoinnin apuvälineenä käytettiin Microsoft Office Excel 2007 ohjelmaa sekä Eduix E-lomake 3.1 ohjelman raportointi ominaisuutta.

Aineiston alustavassa tarkastelussa selvitettiin vastausosuuksien määrät väittämillä ”Täysin samaa mieltä”, ”Täysin eri mieltä” sekä ” En osaa sanoa”. Kyselykokonaisuudessa nämä vastausvaihtoehdot esiintyivät prosentuaalisesti, väittämän ”Täysin samaa mieltä” osalta 28,8 %, väittämän ”Täysin eri mieltä” osalta 24,7 % ja väittämän ”En osaa sanoa” osalta 12,6 %.

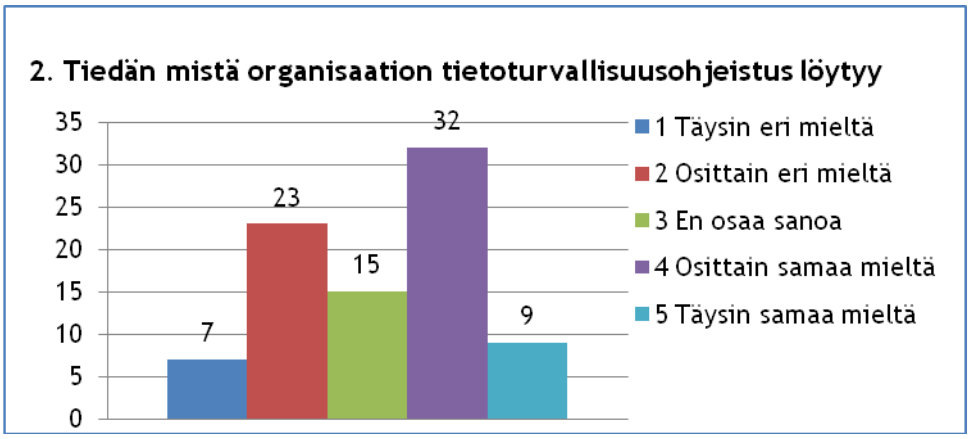
8.1 Tietoturvatietoisuus ja -asenteet

Tietoturvatietoisuuteen ja – asenteisiin liittyvien kysymysten, 1 – 40, vastaukset ja tunnuslukuna moodi ja keskiarvo on esitetty taulukossa 1. Moodi kertoo tyyppiarvon eli aineistossa useimmin esiintyvän vastauksen, kun taas keskiarvo vastausten ”keskimääräisyyttä" kuvaavan keskiluvun. Tietoturvatietoisuuskyselyn tuloksissa ei esitellä erikseen kaikkia kysymyksiä. Esitettäväksi on valittu ne, tietämykseen liittyvät kysymykset, jotka olennaisesti vaikuttavat henkilöstöön toimintaan ja joissa, esiintyvät tietämyksen puutteet, on korjattavissa koulutuksella. Taulukossa **korostetut** kysymykset esitetään tarkemmin kuvioissa 1-14.

Taulukko 1: Tietoturvatietoisuus ja – asenteet osion kyselytuloksia

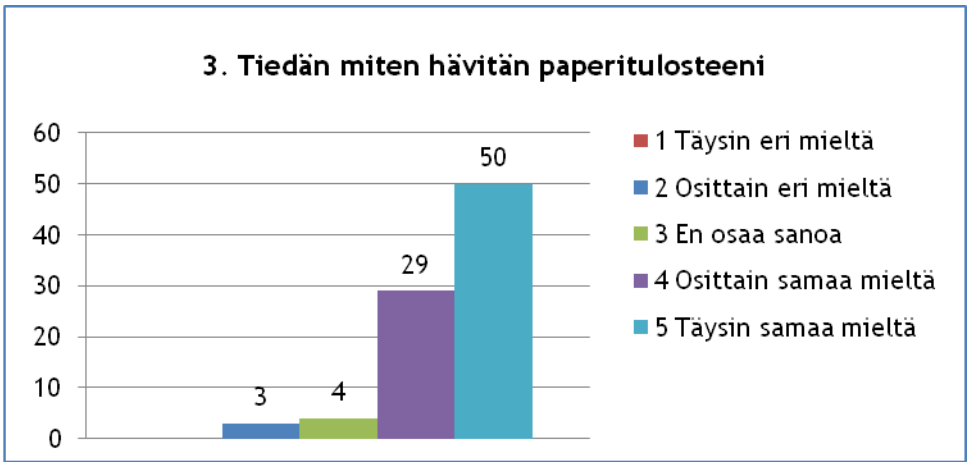
	1 Täysin eri mieltä	2 Osittain eri mieltä	3 En osaa sanoa	4 Osittain samaa mieltä	5 Täysin samaa mieltä	Moodi	Keski arvo
1. Tiedän ketkä kuuluvat organisaation tietoturvallisuushenkilöstöön	3	3	7	50	23	4	4,01
2. Tiedän mistä organisaation tietoturvallisuusohjeistus löytyy	**7**	**23**	**15**	**32**	**9**	**4**	**3,15**
3. Tiedän miten hävitän paperitulosteeni	**0**	**3**	**4**	**29**	**50**	**5**	**4,47**
4. Olen saanut riittävästi tietoturvallisuuteen liittyvää informaatiota	**2**	**10**	**19**	**37**	**18**	**4**	**3,69**
5. Tietoturvallisuuteen liittyviin asioihin saa vastauksen nopeasti	1	7	22	32	24	4	3,83
6. Myös minä olen vastuussa organisaatiomme tietoturvallisuudesta	**1**	**0**	**3**	**10**	**72**	**5**	**4,77**
7. Kaikilla organisaatioon tulevilla vierailijoilla täytyy olla vierailulupa	1	4	4	23	54	5	4,45
8. Tietoturvallisuuden tarkoitus on suojata tietoa	0	4	5	26	51	5	4,44
9. Tietoturvallisuuden tarkoitus on minimoida vahingot	5	5	8	21	47	5	4,16
10. Tietoturvallisuus on osa jokapäiväistä työtä	0	0	6	18	62	5	4,65
11. Tietoturvallisuuden kehitysehdotuksiin suhtaudutaan organisaatiossani hyvin	2	9	30	32	12	4	3,47
12. Yksi tietoturvallisuuden ulottuvuuksista on luottamuksellisuus	1	0	11	30	43	5	4,29
13. Tiedonkulku tietoturvallisuusasioissa toimii hyvin	**2**	**12**	**21**	**40**	**11**	**4**	**3,53**
14. Kaikkea organisaation tietoa ei tarvitse suojata	3	9	10	35	29	4	3,91
15. Tietoturvallisuutta korostetaan välillä liikaa, että se aiheuttaa ärtymystä	**9**	**21**	**19**	**26**	**11**	**4**	**3,10**
16. Organisaatiomme tietoturvallisuutta tarkastellaan säännöllisesti	0	16	39	26	5	3	3,23
17. Tunnen organisaatioin tietoaineistojen luokittelun	**1**	**12**	**11**	**44**	**18**	**4**	**3,77**
18. Riittää, että luottamukselliset asiakirjat ovat lukitussa pöytälaatikossa	34	30	7	10	5	1	2,09
19. Voin lainata toimikorttiani työkaverille jos hän on omansa unohtanut kotiin	**60**	**12**	**10**	**2**	**2**	**1**	**1,53**
20. Oma syntymäpäivä on hyvä toimikortin PIN -koodi	70	11	2	2	1	1	1,29
21. Työn helpottamiseksi voin käyttää kaikissa järjestelmissä samaa salasanaa	45	23	6	9	3	1	1,86
22. Salasana kannattaa vaihtaa vähintään puolen vuoden välein	10	12	12	23	29	5	3,57
23. Voin taltioida salasanani turvalliseen paikkaan	8	12	10	26	29	5	3,62
24. Mielestäni 9:hyv!!:ja:10:kaunista täyttää hyvän salasanan vaatimukset	10	11	17	19	28	5	3,48
25. Voin puhua vapaasti kotona viranomaiskäyttöön leimatuista asiakirjojen sisällöstä	68	13	4	0	1	1	1,29
26. Kaikilla henkilökuntaan kuuluvilla on oikeus lukea luottamuksellisia asiakirjoja	53	20	6	5	2	1	1,64
27. Tiedän mitä vaitiolositoumus tarkoittaa	**3**	**4**	**3**	**26**	**50**	**5**	**4,35**
28. Jos näen käytävällä tuntemattoman ihmisen harhailemassa, kysyn heti millä asialla hän liikkuu	**5**	**14**	**15**	**27**	**25**	**4**	**3,62**
29. Matkapuhelimissa voin puhua vain julkista tietoa	1	4	11	23	47	5	4,29
30. Voin vapaasti kuvata työpaikallani olevia asioita	47	27	9	2	1	1	1,64
31. Työsähköposti on tarkoitettu vain työasioiden hoitoon	1	4	5	21	55	5	4,45
32. Tiedän miten voin salata tiedostot	**14**	**19**	**15**	**20**	**18**	**4**	**3,10**
33. Voin esim. Facebookissa kertoa avoimesti työstäni	76	7	2	0	1	1	1,17
34. Tiedän mitä teen jos työasemaani tulee vika	2	4	8	31	41	5	4,22
35. Voin käyttää tarvittaessa omaa USB -muistivälinettä työasioiden hoitoon	61	17	4	1	3	1	1,47
36. USB -muistivälineeni katoaa, ilmoitan siitä välittömästi tietoturvallisuushenkilöstölle	**2**	**0**	**5**	**14**	**65**	**5**	**4,63**
37. Kaikki muistivälineet ja niiden sisältämät tiedostot on aina virustarkastettava ennen kytkemistä verkossa olevaan työasemaan	3	1	3	11	68	5	4,63
38. Haittaohjelmatarkastuksen voi tehdä verkkotyöasemalla	**20**	**12**	**18**	**14**	**22**	**5**	**3,07**
39. Kaikki luokiteltua tietoa sisältävät tiedostot täytyy salata jos niitä lähetetään Internetissä	3	3	25	9	46	5	4,07
40. Tiedän miten toimin jos työasemani ilmoittaa haittaohjelmasta	**2**	**4**	**10**	**33**	**37**	**5**	**4,15**

Väittämässä 2 selvitettiin, kuinka hyvin henkilöstö tietää, minne organisaation tietoturvaohjeistus on taltioitu? Vastaajista 42 henkilöä (47,7 %) tietää, minne ohjeistus on taltioitu (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 30 (34,9 %) ei tiedä, mistä ohjeistus löytyy (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastausvaihtoehdon on valinnut 15 henkilöä (17,4 %).



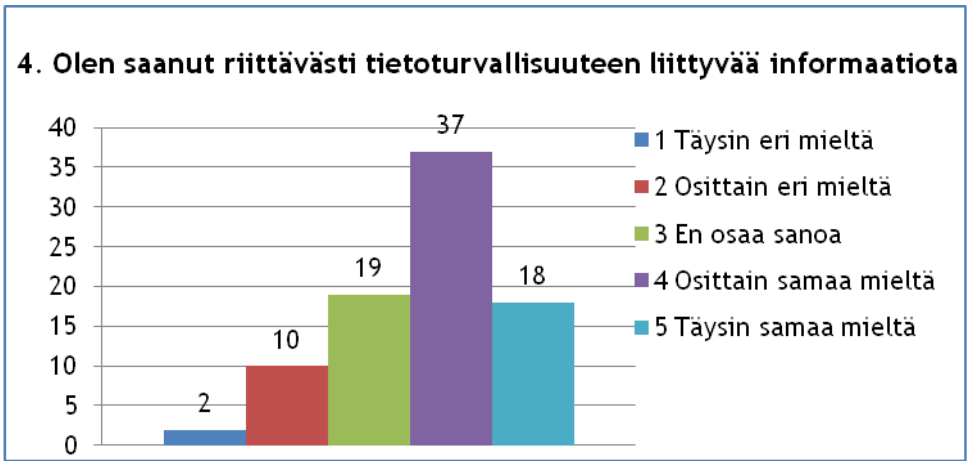
Kuvio 1: Väittämän ”2. Tiedän mistä organisaation tietoturvallisuus ohjeistus löytyy” vastausjakauma

Väittämä 3, joka koski paperitulosteiden hävittämistä, vastaajista 79 henkilöä (91,9 %) tietää miten hävittää paperitulosteensa (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). ”Osittain eri mieltä” vastauksen antoi kolme henkilöä (3,5 %). ”En osaa sanoa” vastauksen antaneita oli neljä henkilöä (4,6 %). ”Täysin eri mieltä” vastauksia ei ollut yhtään kappaletta.



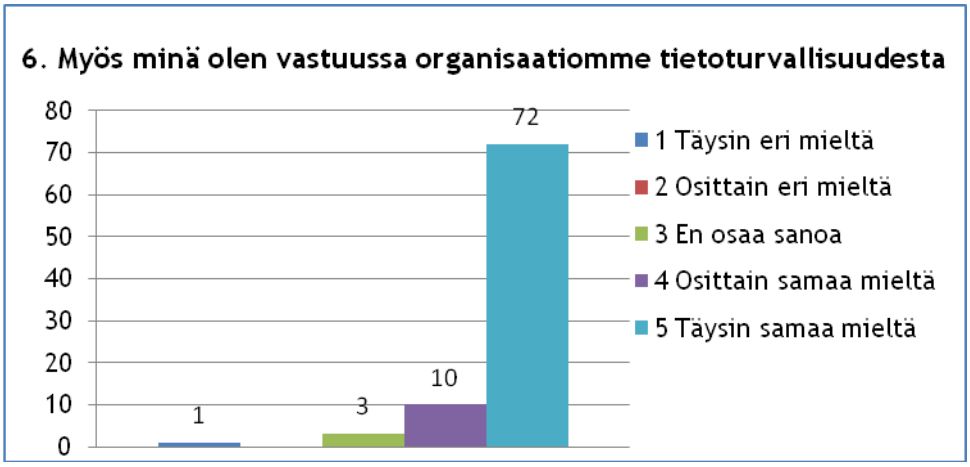
Kuvio 2: Väittämän ”3. Tiedän miten hävitän paperitulosteeni” vastausjakauma

Väittämä 4, koski henkilöstön tietoturvallisuuteen liittyvän informaation riittävyyttä. Vastaajista 55 henkilöä (63 %), on mielestään saanut riittävästi tietoturvallisuuteen liittyvää informaatiota (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 12 (14 %), ei ole mielestään saanut riittävää informaatiota tietoturvallisuuteen liittyen (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 19 henkilöä (23 %).



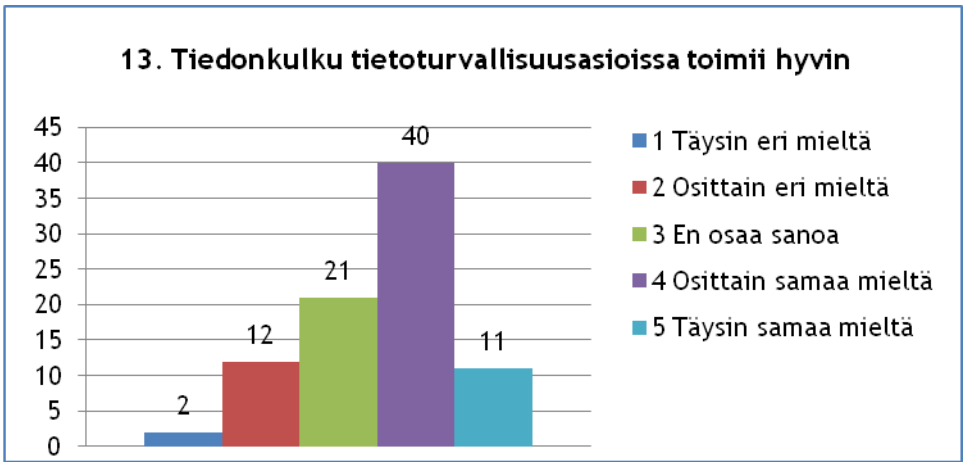
Kuvio 3: Väittämän ”4. Olen saanut riittävästi tietoturvallisuuteen liittyvää informaatiota” vastausjakauma

Väittämä 6, jossa kysyttiin henkilöstön omaa vastuuta organisaation tietoturvallisuudesta, 82 henkilöä (95,3 %) on vastannut, olevansa myös itse vastuussa organisaation tietoturvallisuudesta (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista yksi henkilö (1,2 %) vastasi, ettei itse ole vastuussa organisaation tietoturvallisuudesta (”Täysin eri mieltä”). ”En osaa sanoa” vastauksen antoi kolme henkilöä (3,5 %). ”Osittain eri mieltä” vastauksia ei annettu yhtään.



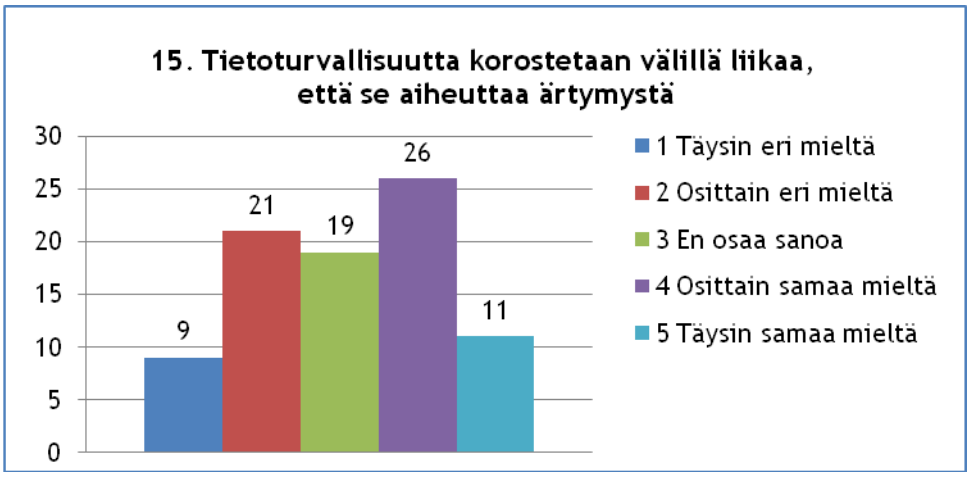
Kuvio 4: Väittämän ”6. Myös minä olen vastuussa organisaatiomme tietoturvallisuudesta” vastausjakauma

Väittämässä 13, kysyttiin henkilöstöltä, miten heidän mielestään tiedonkulku tietoturvallisuusasioissa toimii. Vastaajista 51 henkilöä (59,3 %) kokee, että tiedonkulku tietoturvallisuusasioissa toimii hyvin (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastanneista 14 henkilöä (16,3 %) on vastannut, ettei tiedonkulku toimi hyvin (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen on antanut 21 henkilöä (24,4 %).



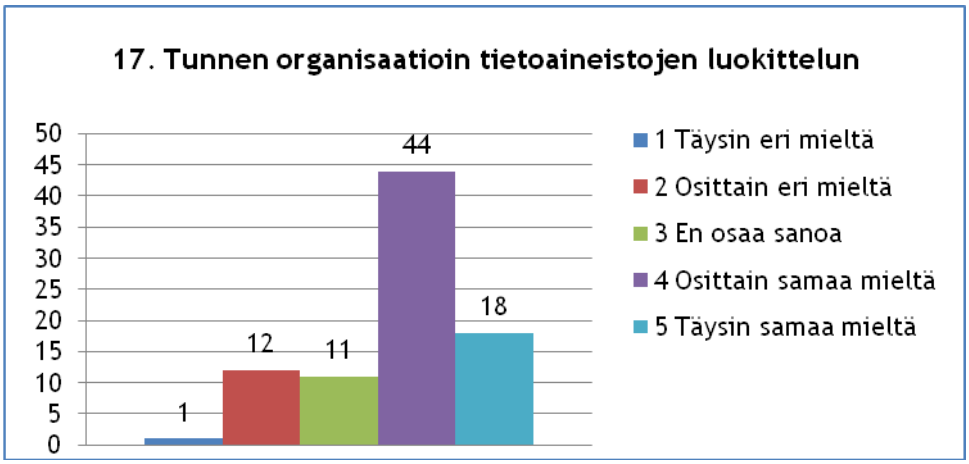
Kuvio 5: Väittämän ”13. Tiedonkulku tietoturvallisuusasioissa toimii hyvin” vastausjakauma

Väittämän 15, joka koski tietoturvallisuuden korostamisen aiheuttamaa ärtymystä. Vastausten mukaan, 37 henkilön (43,0 %) mielestä, tietoturvallisuutta korostetaan välillä liikaa, että se aiheuttaa ärtymystä (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastanneista 30 henkilön (34,9 %) mielestä, tietoturvallisuuden korostaminen ei aiheuta ärtymystä (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Vastanneista 19 henkilöä (22,1 %) on vastannut ”En osaa sanoa”.



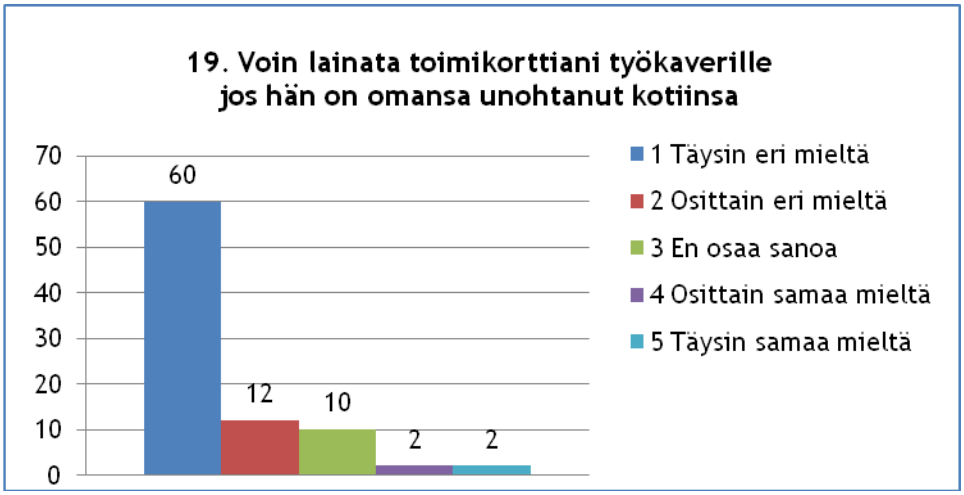
Kuvio 6: Väittämän ”15. Tietoturvallisuutta korostetaan välillä liikaa, että se aiheuttaa ärtymystä” vastausjakauma

Väittämässä 17, kysyttiin henkilöstön tietämystä organisaation tietoaineistoluokittelusta. Vastaajista 62 henkilöä (72,1 %), vastaa tuntevansa organisaation tietoaineistojen luokittelun (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Tietoaineiston luokittelua ei tunne vastaajista 13 henkilöä (15,1 %) (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia annettiin 11 kappaletta (12,8 %).



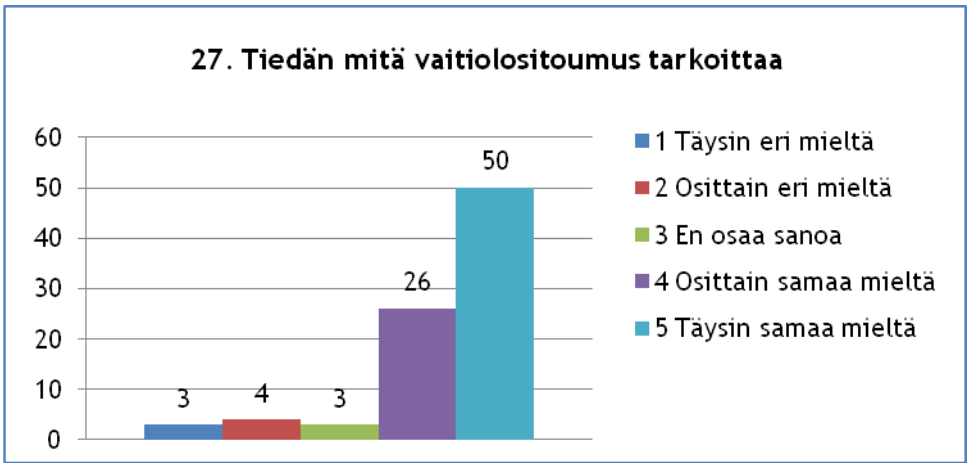
Kuvio 7: Väittämän ”17. Tunnen organisaation tietoaineistojen luokittelun” vastausjakauma

Väittämä 19, joka koski oman toimikortin lainaamista työkaverille, vastausten mukaan 72 henkilöä (83,7 %), on sitä mieltä, ettei omaa toimikorttia voi lainata työkaverille (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Vastaajista neljän henkilön (4,7 %) mielestä, omaa toimikorttia voi lainata työkaverille (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). ”En osaa sanoa” vastauksen on antanut 10 henkilöä (11,6 %).



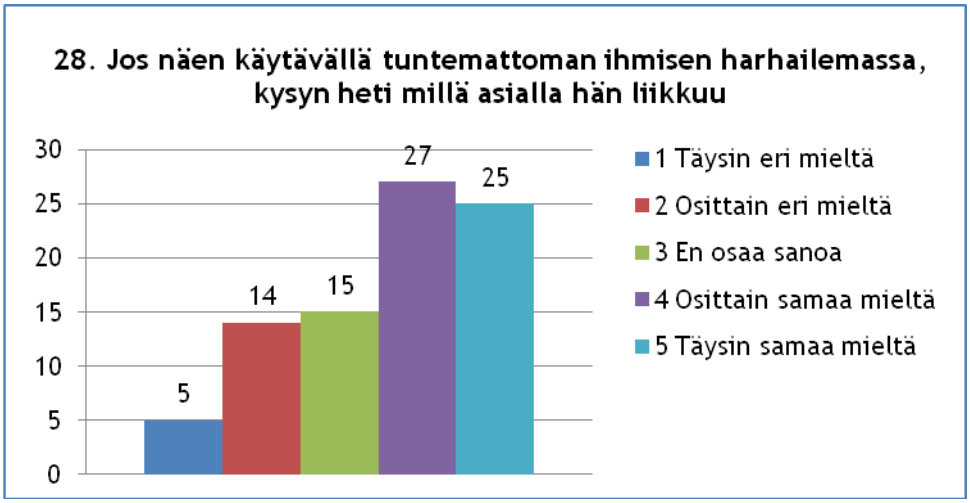
Kuvio 8: Väittämän ”19. Voin lainata toimikorttiani työkaverille jos hän on omansa unohtanut kotiinsa” vastausjakauma

Väittämässä 27 selvitettiin, tietääkö henkilöstö, mitä vaitiolositoumus tarkoittaa? Vastaajista 76 henkilöä (88,4 %), vastaa tietävänsä mitä vaitiolositoumus tarkoittaa (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista seitsemän henkilöä (8,1 %), ei tiedä mitä vaitiolositoumus tarkoittaa. ”En osaa sanoa” vastauksen antoi kolme vastaajaa (3,5 %).



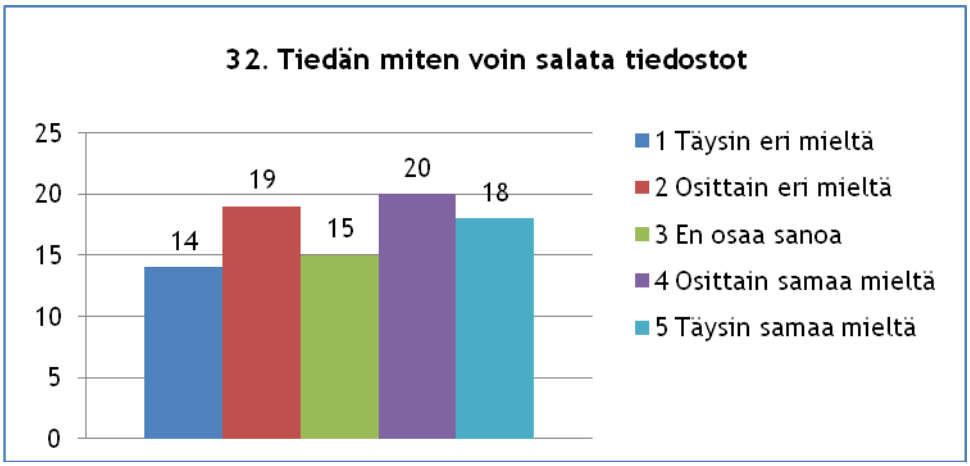
Kuvio 9: Väittämän ”27. Tiedän mitä vaitiolositoumus tarkoittaa” vastausjakauma

Väittämässä 28 kysytään, että reagoiko henkilöstö millään lailla, jos havaitsee tuntemattoman henkilön harhailemassa käytävällä. Vastaajista 52 henkilöä (60,5 %), vastaa kysyvänsä tuntemattomalta henkilöltä, millä asialla hän on, jos havaitsee vieraan käytävällä harhailemassa (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastanneista 19 henkilöä (22,1 %), ei kyseenalaista vieraan henkilön käytävällä liikkumista (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 15 henkilöä (17,4 %).



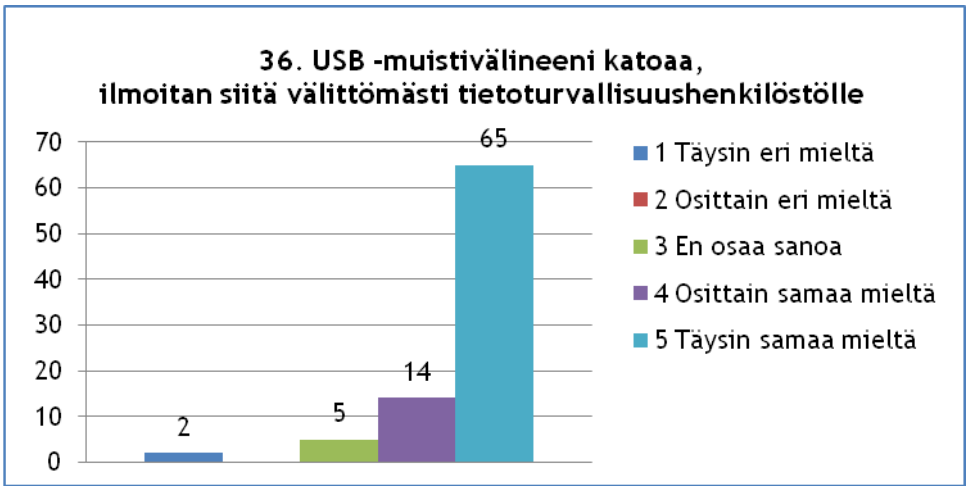
Kuvio 10: Väittämän ”28. Jos näen käytävällä tuntemattoman ihmisen harhailemassa, kysyn heti millä asialla hän liikkuu” vastausjakauma

Väittämä 32, joka koski henkilöstön tietämystä tiedostojen salaamisessa, 38 henkilöä (44,2 %) vastaa tietävänsä, miten tiedostojen salaus suoritetaan (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 33 henkilöä (38,4 %), ei tiedä miten tiedostot salataan (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Vastaajista 15 henkilöä (17,4 %) antoi ”En osaa sanoa” vastauksen.



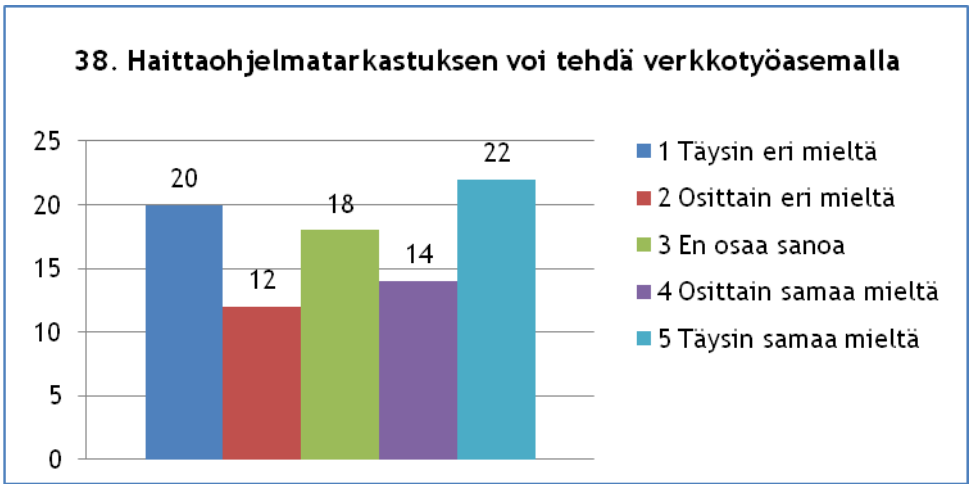
Kuvio 11: Väittämän ”32. Tiedän miten voin salata tiedostot” vastausjakauma

Väittämässä 36 kysytään, ilmoittaako henkilöstö USB – muistivälineen katoamisesta välittömästi tietoturvallisuushenkilöstölle? Vastaajista 79 henkilöä (91,9 %), ilmoittaa USB – muistivälineen katoamisesta välittömästi tietoturvallisuushenkilöstölle (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista kaksi henkilöä (2,3 %) vastaa, ettei ilmoita välittömästi (”Täysin eri mieltä”). Vastaajista viisi henkilöä (5,8 %) vastaa ”En osaa sanoa”. ”Osittain eri mieltä” vastauksia ei annettu yhtään.



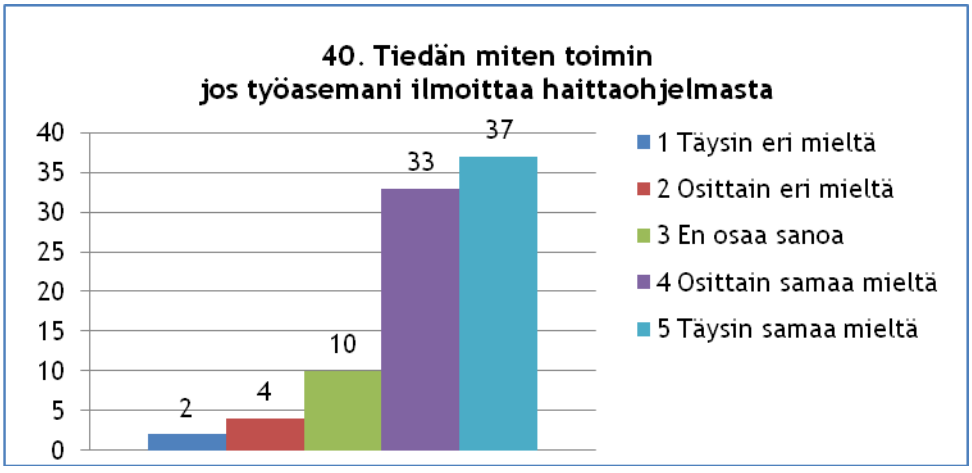
Kuvio 12: Väittämän ”36. Jos USB – muistivälineeni katoaa, ilmoitan siitä välittömästi tietoturvallisuushenkilöstölle” vastausjakauma

Väittämän 38, joka koski haittaohjelmatarkastusten tekemistä verkkotyöasemalla, 36 henkilöä (41,9 %) vastasi, että haittaohjelmatarkastuksen voi tehdä verkkotyöasemalla (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 32 henkilön (37,2 %) vastauksen mukaan, tarkastusta ei voi tehdä verkkotyöasemalla (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen on antanut 15 henkilöä (17,4 %).



Kuvio 13: Väittämän ”38. Haittaohjelmatarkastuksen voi tehdä verkkotyöasemalla” vastausjakauma

Väittämässä 40 kysytään, tietääkö henkilöstö, miten toimitaan työaseman ilmoittaessa haittaohjelmasta. Vastaajista 70 henkilöä (81,4 %), ilmoittaa tietävänsä toimintatavat työaseman ilmoittaessa haittaohjelmasta (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista kuusi henkilöä (7 %) ei tiedä toimintatapoja, haittaohjelmailmoituksen työasemalle saatuaan (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Vastaajista 10 henkilöä (11,6 %) on vastannut ”En osaa sanoa”.



Kuvio 14: Väittämän ”40. Tiedän miten toimin jos työasemani ilmoittaa haittaohjelmasta” vastausjakauma

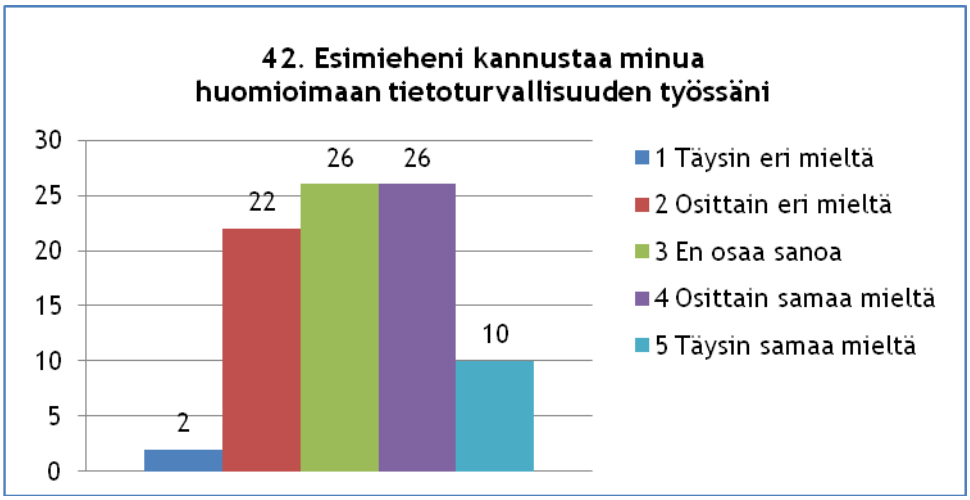
8.2 Tietoturvallisuusjohtaminen

Tietoturvallisuusjohtamiseen liittyvien kysymysten, 41 – 50, vastaukset ja tunnuslukuna moodi ja keskiarvo on esitetty taulukossa 2. Kaikkia tietoturvallisuusjohtamiseen liittyviä kysymyksiä ei esitellä erikseen, vaan esitettäviksi valittiin kysymykset, jotka kertovat henkilöstön mielipiteitä siitä, miten esimiehet huomioivat tietoturvallisuuden toiminnassaan ja mahdollisesti esiintyviä epäkohtia voidaan korjata koulutuksella. Taulukossa **korostetut** kysymykset esitetään tarkemmin kuvioissa 15–20.

Taulukko 2: Tietoturvallisuusjohtaminen osion kyselytuloksia

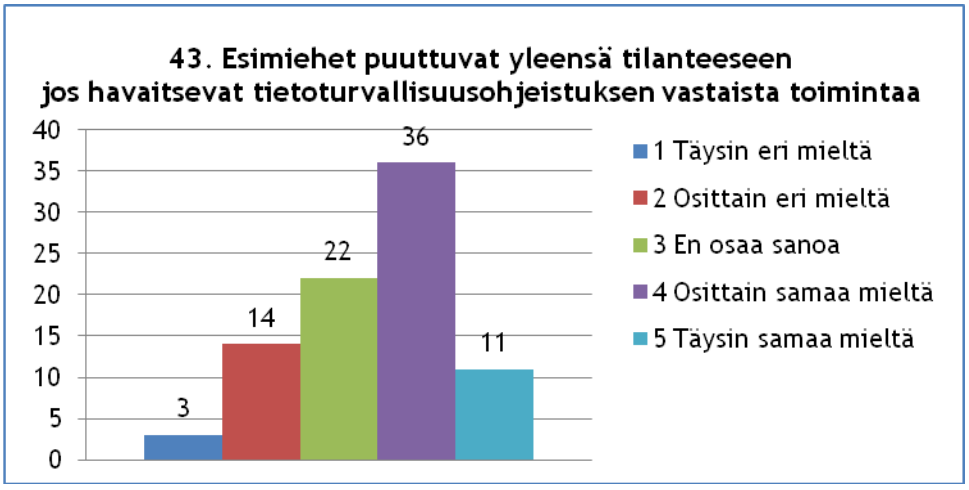
	1 Täysin eri mieltä	2 Osittain eri mieltä	3 En osaa sanoa	4 Osittain samaa mieltä	5 Täysin samaa mieltä	Moodi	Keski arvo
41. Organisaation johto osallistuu näkyvästi tietoturvallisuustyöhön	3	21	33	24	5	3	3,08
42. Esimieheni kannustaa minua huomioimaan tietoturvallisuuden työssäni	**2**	**22**	**26**	**26**	**10**	**3**	**3,23**
43. Esimiehet puuttuvat yleensä tilanteeseen jos havaitsevat tietoturvallisuusohjeistuksen vastaista toimintaa	**3**	**14**	**22**	**36**	**11**	**4**	**3,44**
44. Esimiehet ottavat tietoturvallisuuden huomioon jo toiminnan suunnitteluvaiheessa	**1**	**9**	**27**	**36**	**13**	**4**	**3,59**
45. Esimieheni suosivat esimerkillään tietoturvallisuuden huomioon ottamista	1	14	23	36	12	4	3,51
46. Tietoturvallisuus on organisaatiossamme tärkeä	**0**	**2**	**7**	**28**	**49**	**5**	**4,44**
47. Esimieheni on kiinnostunut alaisten tietoturvallisuutta koskevista ehdotuksista ja kommenteista	1	12	32	29	12	3	3,45
48. Mielestäni esimiehillä on riittävä tietämys tietoturvallisuusasioissa	**1**	**10**	**23**	**35**	**17**	**4**	**3,66**
49. Tietoturvallisuus otetaan huomioon kokouksia järjestettäessä	2	13	23	33	15	4	3,53
50. Organisaation johto osoittaa sitoutuneensa tietoturvallisuuden kehittämiseen	**3**	**13**	**26**	**35**	**8**	**4**	**3,34**

Väittämässä 42 kysytään, kannustaako oma esimies huomioimaan tietoturvallisuus työssä? Vastaajista 36 henkilöä (41,9 %) vastaa, että hänen esimiehensä kannustaa häntä työskentelemään tietoturvallisuus huomioiden (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 24 henkilön (27,9 %) vastausten mukaan, esimies ei kannusta huomioimaan tietoturvallisuutta työssä (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Vastaajista 26 henkilöä (30,2 %) vastasi ”En osaa sanoa”.



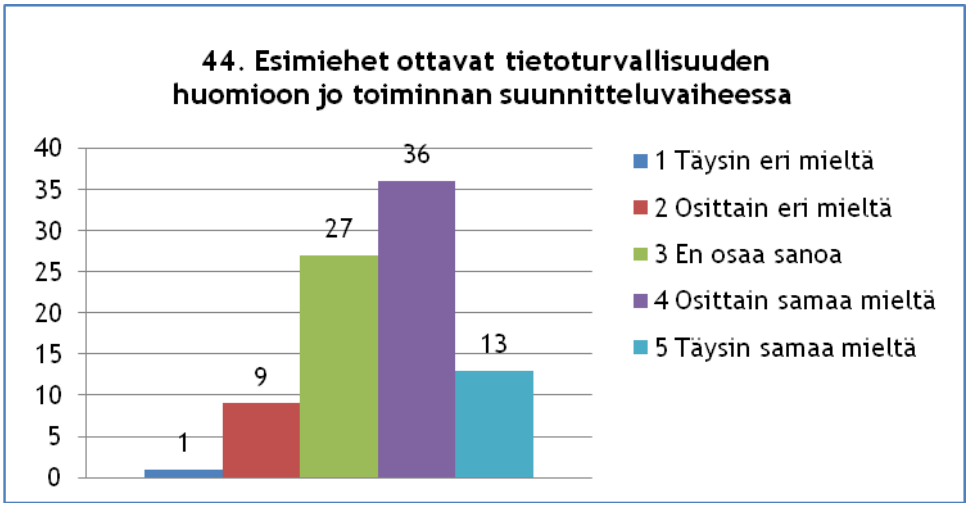
Kuvio 15: Väittämän ”42. Esimieheni kannustaa minua huomioimaan tietoturvallisuuden työssäni” vastausjakauma

Väittämässä 43 selvitettiin, puuttuvatko esimiehet yleensä tilanteeseen, jos havaitsevat tietoturvallisuusohjeistuksen vastaista toimintaa. Vastaajista 47 henkilön (54,7 %) vastausten mukaan, esimiehet puuttuvat yleensä tilanteeseen, havaitessaan tietoturvallisuusohjeistuksen vastaista toimintaa (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 17 henkilön (19,8 %) vastausten mukaan, esimiehet eivät yleensä puutu tietoturvallisuusohjeistuksen vastaiseen toimintaan (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 22 henkilöä (25,6 %).



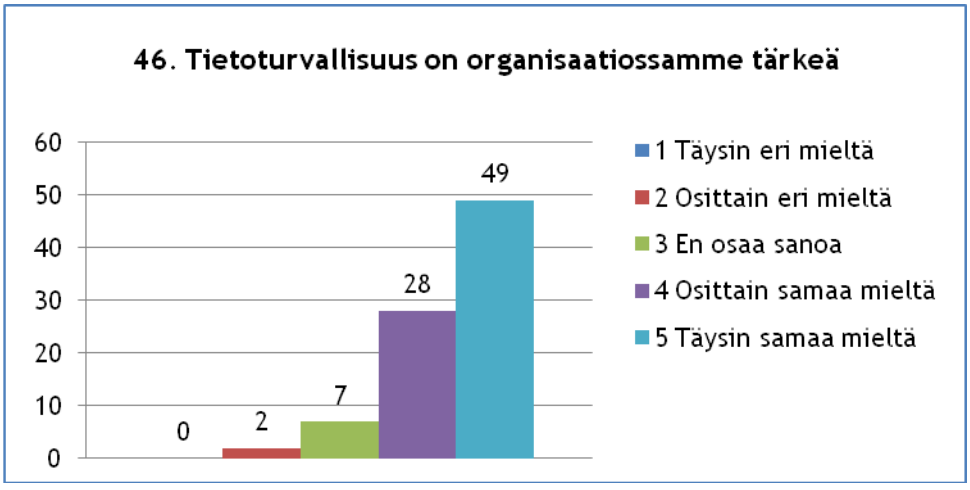
Kuvio 16: Väittämän ”43. Esimiehet puuttuvat yleensä tilanteeseen jos havaitsevat tietoturvallisuusohjeistuksen vastaista toimintaa” vastausjakauma

Väittämässä 44 selvitettiin, ottavatko esimiehet tietoturvallisuuden huomioon jo toiminnan suunnitteluvaiheessa. Vastaajista 49 henkilön (57 %) mielestä, esimiehet ottavat tietoturvallisuuden huomioon toimintaa suunnitellessaan (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 10 henkilön (11,6 %) mielestä, esimiehet eivät huomioisi tietoturvallisuutta toiminnan suunnitteluvaiheessa (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 27 henkilöä (31,3 %).



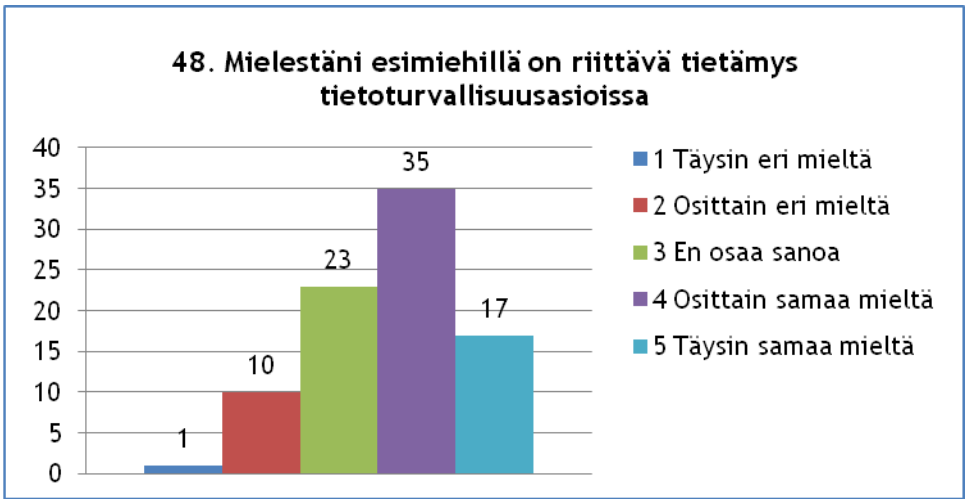
Kuvio 17: Väittämän ”44. Esimiehet ottavat tietoturvallisuuden huomioon jo toiminnan suunnitteluvaiheessa” vastausjakauma

Väittämä 46, joka koski tietoturvallisuuden tärkeyttä organisaatiossa, 77 henkilöä (89,5 %) kokee, että organisaatiossa tietoturvallisuus on tärkeä (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Kahden vastaajan (2,3 %) mielestä, organisaatiossa tietoturvallisuus ei ole tärkeä (”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi seitsemän henkilöä (8,1 %). ”Täysin eri mieltä” vastauksia ei annettu yhtään.



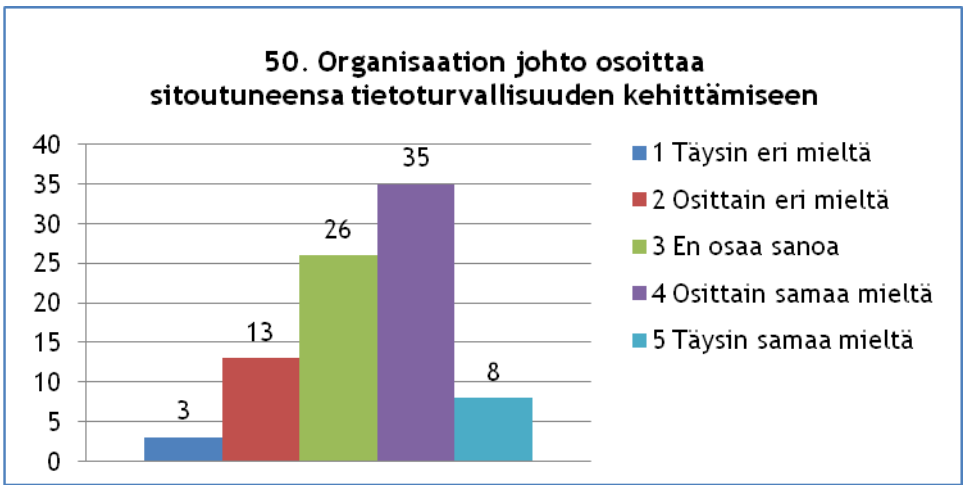
Kuvio 18: Väittämän ”46. Tietoturvallisuus on organisaatiossamme tärkeä” vastausjakauma

Väittämä 48, joka koski esimiesten tietämystä tietoturvallisuusasioissa, 52 henkilön (60,5 %) mukaan, esimiehillä on riittävä tietämys tietoturvallisuusasioissa (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 11 henkilön (12,8 %) mukaan, esimiehillä ei ole riittävää tietämystä tietoturvallisuusasioissa (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 23 henkilöä (26,7 %).



Kuvio 19: Väittämän ”48. Mielestäni esimiehillä on riittävä tietämys tietoturvallisuusasioissa” vastausjakauma

Väittämässä 50 kysyttiin henkilöstön mielipidettä, johdon sitoutumisesta tietoturvallisuuden kehittämiseen. Vastaajista 43 (50 %) mielestä, organisaation johto osoittaa sitoutuneensa tietoturvallisuuden kehittämiseen (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 16 henkilön (18,6 %) mielestä, organisaation johto ei ole osoittanut sitoutuneensa tietoturvallisuuden kehittämiseen (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 26 henkilöä (30,2 %).



Kuvio 20: Väittämän ”50. Organisaation johto osoittaa sitoutuneensa tietoturvallisuuden kehittämiseen” vastausjakauma

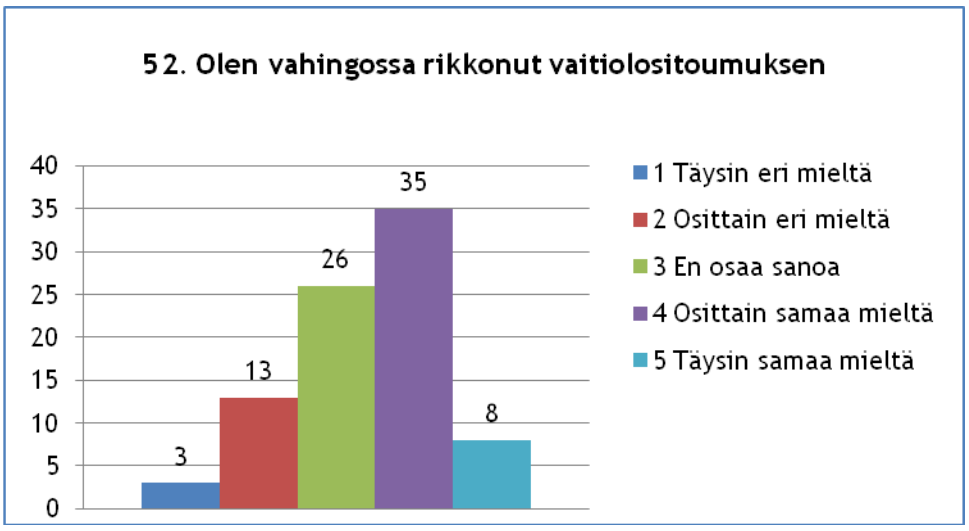
8.3 Oma toiminta

Omaan toimintaan liittyvien kysymysten, 51 – 80, vastaukset ja tunnuslukuna moodi ja keskiarvo on esitetty taulukossa 3. Kaikkia kysymyksiä ei esitellä erikseen. Esitettäväksi valittujen kysymysten, väittämät ovat selkeitä tietoturvallisuusriskejä, mikäli näiden osalta toimitaan ohjeistuksen vastaisesti. Taulukossa **korostetut** kysymykset esitetään tarkemmin kuvioissa 21 – 32.

Taulukko 3: Oma toiminta -osion kyselytuloksia

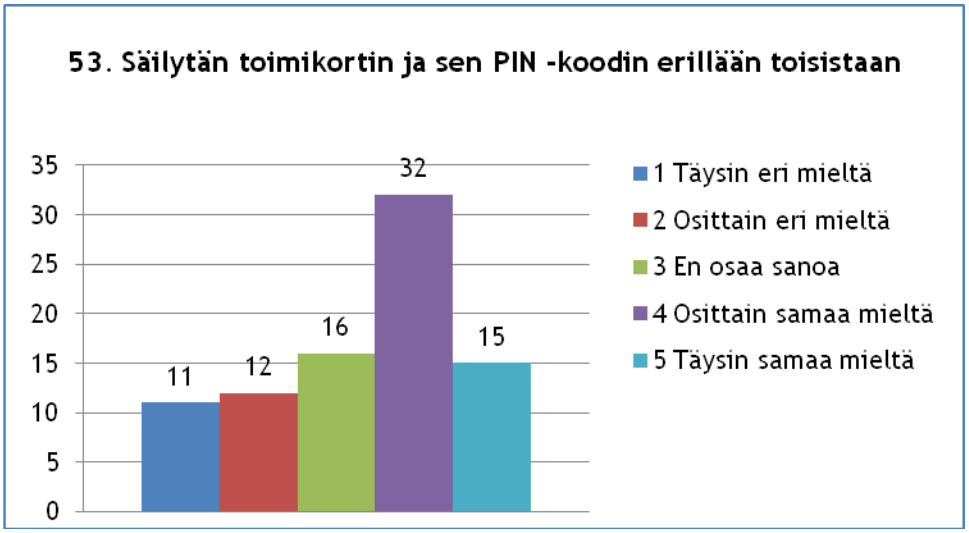
	1 Täysin eri mieltä	2 Osittain eri mieltä	3 En osaa sanoa	4 Osittain samaa mieltä	5 Täysin samaa mieltä	Moodi	Keski arvo
51. Olen toiminut joskus vastoin tietoturvallisuusohjeistusta	11	12	16	32	15	4	3,33
52. Olen vahingossa rikkonut vaitiolositoumuksen	**54**	**13**	**14**	**3**	**2**	**1**	**1,67**
53. Säilytän toimikortin ja sen PIN -koodin erillään toisistaan	**4**	**3**	**1**	**10**	**68**	**5**	**4,57**
54. Olen vaihtanut toimikorttini PIN -koodin alkuperäisestä	25	3	3	3	52	5	3,63
55. Olen lainannut toimikorttiani työkaverille	**69**	**3**	**1**	**8**	**5**	**1**	**1,57**
56. Poistan aina toimikortin työasemasta kun poistun työhuoneesta	**11**	**21**	**7**	**21**	**26**	**5**	**1,67**
57. Lukitsen aina työhuoneeni kun poistun huoneesta	18	14	20	15	19	3	3,35
58. Kirjaudun aina työasemalta ulos työpäivän päättyessä	3	6	1	8	68	5	3,03
59. Olen käyttänyt toisen henkilön tunnuksia	**58**	**5**	**3**	**11**	**9**	**1**	**4,53**
60. Olen antanut tunnukseni toisen henkilön käyttöön	**66**	**5**	**5**	**6**	**4**	**1**	**1,93**
61. Käytän eri tietojärjestelmissä eri salasanoja	2	9	6	35	34	4	1,57
62. Säilytän kaikki salasanani lukitussa paikassa muiden ulottumattomissa	11	14	11	22	28	5	4,05
63. En vaihda salasanojani, ellei järjestelmä sitä pakota	3	14	6	29	34	5	1,93
64. Olen kuunnellut musiikkia työasemalla	60	13	4	4	5	1	3,49
65. En jätä luokiteltuja asiakirjoja valvomatta	1	7	13	33	32	4	3,90
66. Käytän työsähköpostia vain työasioiden hoitoon	0	7	7	22	50	5	3,49
67. Olen hoitanut työasioita kotikoneella	38	12	4	16	16	1	3,90
68. Olen hoitanut työasioita siviilisähköpostilla	54	11	4	12	5	1	1,62
69. Minulla on profiili Facebookissa	45	0	1	5	35	1	4,02
70. Olen kirjautunut Facebookiin työsähköpostiosoitteellani	85	0	1	0	0	1	4,34
71. Olen julkaissut Facebookissa työhöni liittyviä valokuvia	76	4	3	0	3	1	2,53
72. Minulla on käytössäni organisaation USB -muistiväline	32	1	0	1	52	5	1,87
73. Olen käyttänyt omaa USB -muistivälinettä työasemalla	**64**	**9**	**1**	**3**	**9**	**1**	**2,83**
74. Minulla on varmuuskopiot omista tärkeistä tiedostoista	35	13	6	16	16	1	1,02
75. Olen liittänyt oman kameran työaseman USB -porttiin	**71**	**1**	**1**	**1**	**11**	**1**	**1,26**
76. Suoritan aina haittaohjelmatarkastuksen USB -muistivälineelle ennen liittämistä verkossa olevaan työasemaan	**8**	**8**	**9**	**20**	**41**	**5**	**3,47**
77. Suoritan aina haittaohjelmatarkastuksen kaikille Internetistä lataamilleni tiedostoille ennen työasemalle tallentamista	7	14	10	16	39	5	1,65
78. Olen aiheuttanut joskus haittaohjelmahälytyksen	**72**	**3**	**4**	**1**	**6**	**1**	**2,59**
79. Jos huomaan työkaverin toimivan ohjeiden vastaisesti, ohjaan häntä toimimaan oikein	**2**	**4**	**18**	**38**	**24**	**4**	**3,91**
80. Minulla on käynyt vieraita työpaikkani toimistotiloissa ilman vierailulupaa	**63**	**7**	**4**	**9**	**3**	**1**	**1,63**

Väittämä 52, joka koski vaitiolositoumuksen rikkomista, 42 henkilöä (48,8 %) ilmoittaa, joskus vahingossa rikkoneensa vaitiolositoumuksen (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 16 henkilöä (18,6 %) ei ole rikkonut vaitiolositoumusta (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi 26 henkilöä (30,2 %).



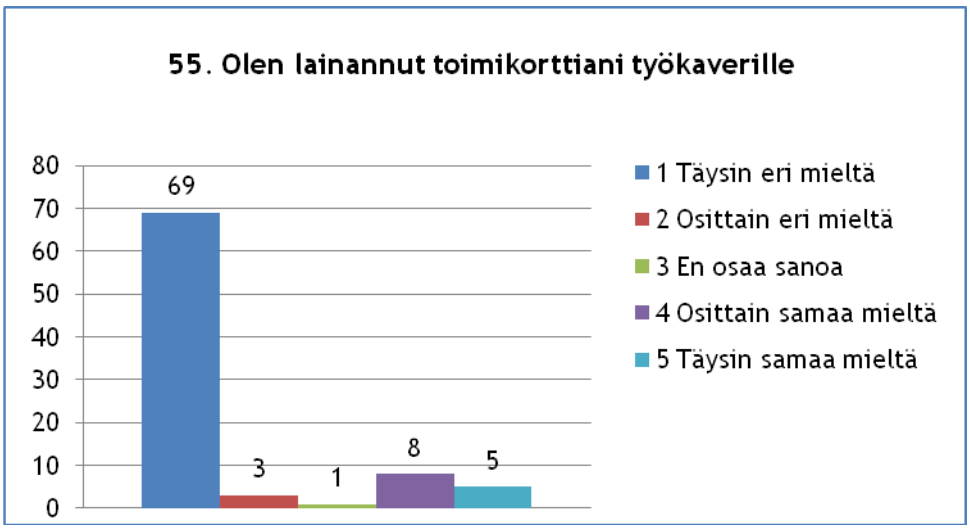
Kuvio 21: Väittämän ”52. Olen vahingossa rikkonut vaitiolositoumuksen” vastausjakauma

Väittämä 52, joka koski toimikortin ja PIN -koodin säilyttämistä, 47 henkilöä (54,7 %) ilmoittaa, säilyttävänsä toimikortin ja PIN – koodin erillään toisistaan (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 23 henkilöä (26,7 %), säilyttää PIN – koodin toimikortin yhteydessä (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia oli 16 vastaajalla (18,6 %).



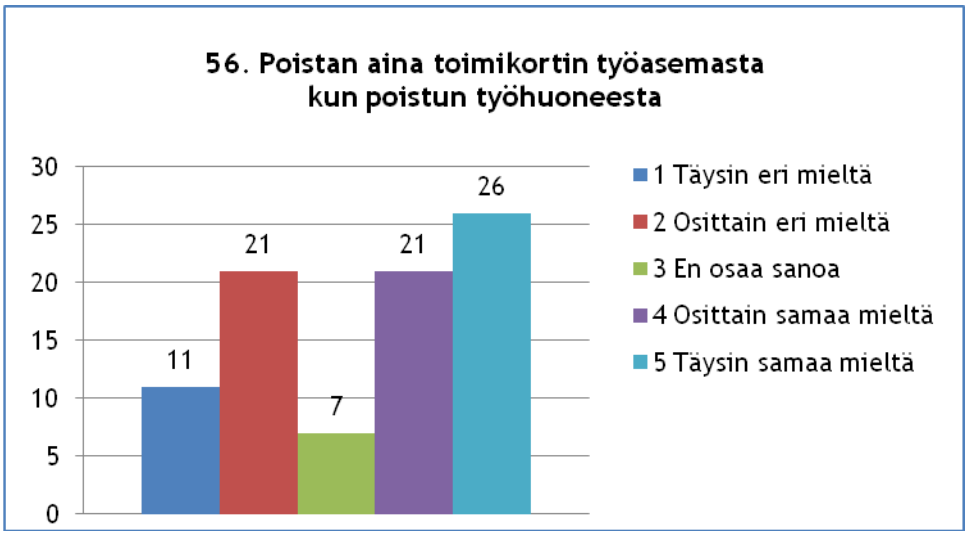
Kuvio 22: Väittämän ”53. Säilytän toimikortin ja sen PIN – koodin erillään toisistaan” vastausjakauma

Väittämä 55, joka koski toimikortin lainaamista työkaverille, 13 henkilöä (15,1 %) ilmoittaa, lainanneensa toimikorttiaan työkaverille (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 72 henkilöä (83,7 %), ei ole lainannut toimikorttiaan työkaverille (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Yksi henkilö (1,2 %) on vastannut ”En osaa sanoa”.



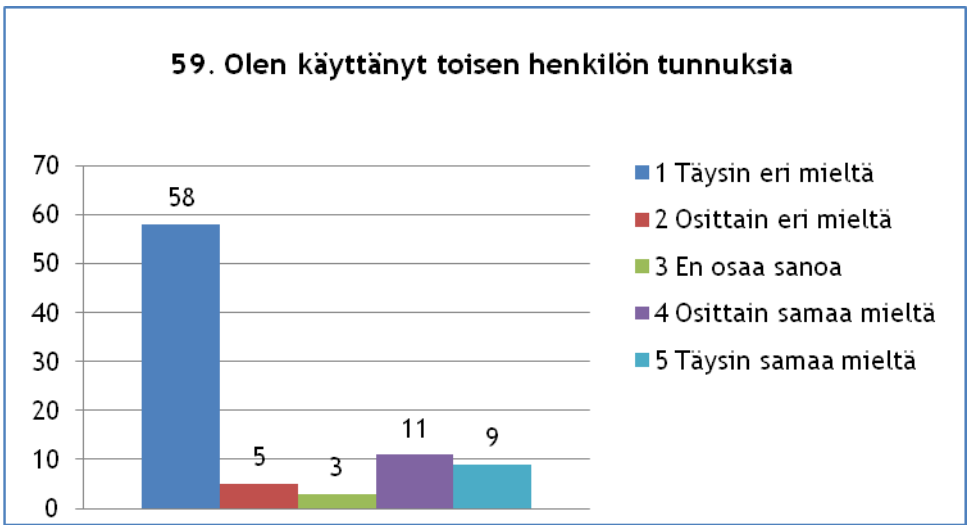
Kuvio 23: Väittämän ”55. Olen lainannut toimikorttiani työkaverille” vastausjakauma

Väittämässä 56 kysyttiin, poistaako henkilöstö toimikortin työasemasta aina työhuoneesta poistuessaan? Vastaajista 47 henkilöä (54,7 %), poistaa toimikortin työasemasta aina työhuoneesta poistuessaan (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 32 henkilöä (37,2 %), ei poista toimikorttiaan aina työasemasta työhuoneesta poistuessaan (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia annettiin seitsemän (8,1 %) kappaletta.



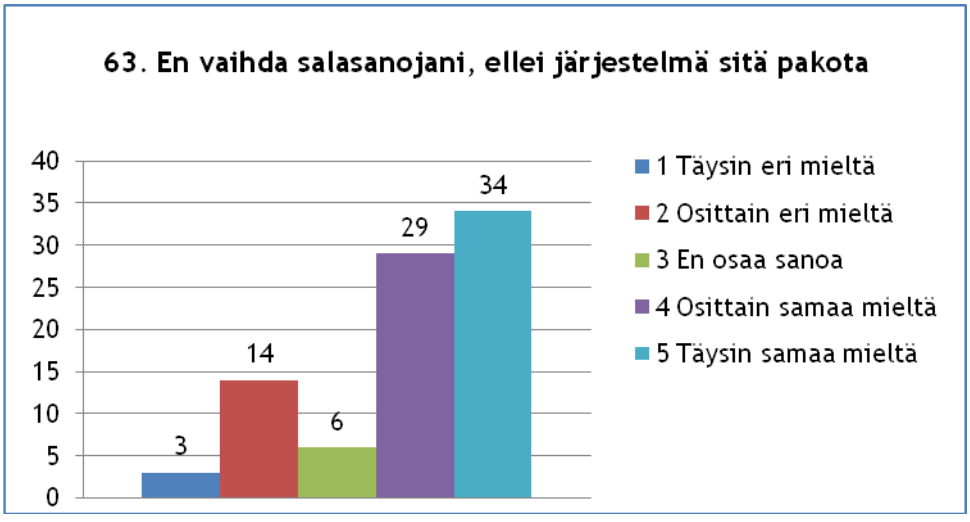
Kuvio 24: Väittämän ”56. Poistan aina toimikortin työasemasta kun poistun työhuoneesta” vastausjakauma

Väittämä 59, joka koski toisen henkilön tunnuksien käyttämistä, 20 henkilöä (23,3 %) ilmoittaa, käyttäneensä toisen henkilön tunnuksia (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 63 henkilöä (73,2 %), ei ole käyttänyt toisen henkilön tunnuksia (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastasi kolme henkilöä (3,5 %).



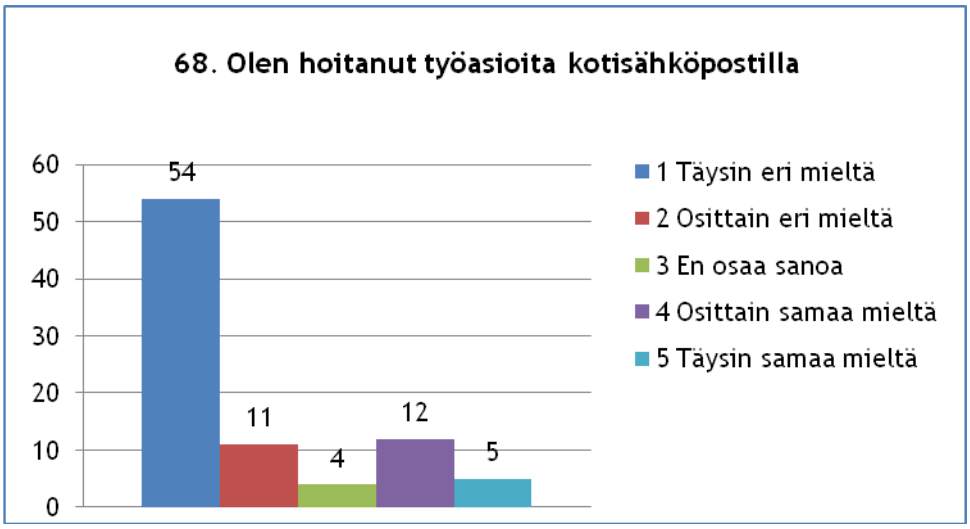
Kuvio 25: Väittämän ”59. Olen käyttänyt toisen henkilön tunnuksia” vastausjakauma

Väittämä 63, joka koski salasanojen vaihtamista, 63 henkilöä (73,2 %) ei vaihda salasanoja, ellei järjestelmä sitä pakota (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 17 henkilöä (19,8 %) vaihtaa salasanansa, ilman järjestelmän pakottamista (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksen antoi kuusi henkilöä (7 %).



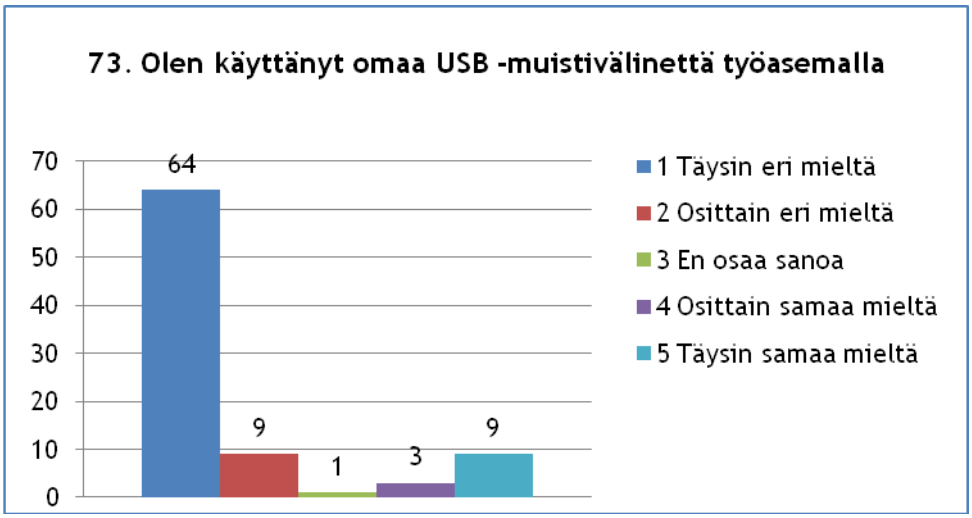
Kuvio 26: Väittämän ”63. En vaihda salasanojani, ellei järjestelmä sitä pakota” vastausjakauma

Väittämässä 68 kysyttiin, onko henkilöstö hoitanut työasioita kotisähköpostillaan? Vastaajista 17 henkilöä (19,7 %), on hoitanut työasioitaan myös kotisähköpostilla (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 65 henkilöä (75,6 %), ei ole hoitanut työasioita kotisähköpostilla (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia oli neljässä (4,7 %) vastauslomakkeessa.



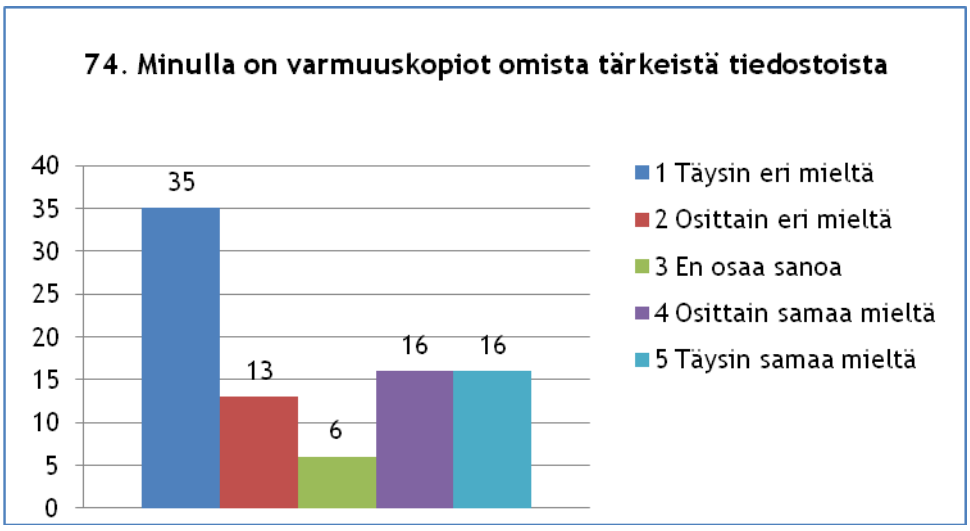
Kuvio 27: Väittämän ”68. Olen hoitanut työasioita kotisähköpostilla” vastausjakauma

Väittämä 73, joka koski omien USB – muistivälineiden käyttämistä työasemilla, 12 henkilöä (14 %), on käyttänyt työasemalla omaa USB – muistivälinettä (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 73 henkilöä (84,9 %), ei ole käyttänyt omaa USB – muistivälinettä työasemassa (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia annettiin yhdessä (1,2 %) vastauslomakkeessa.



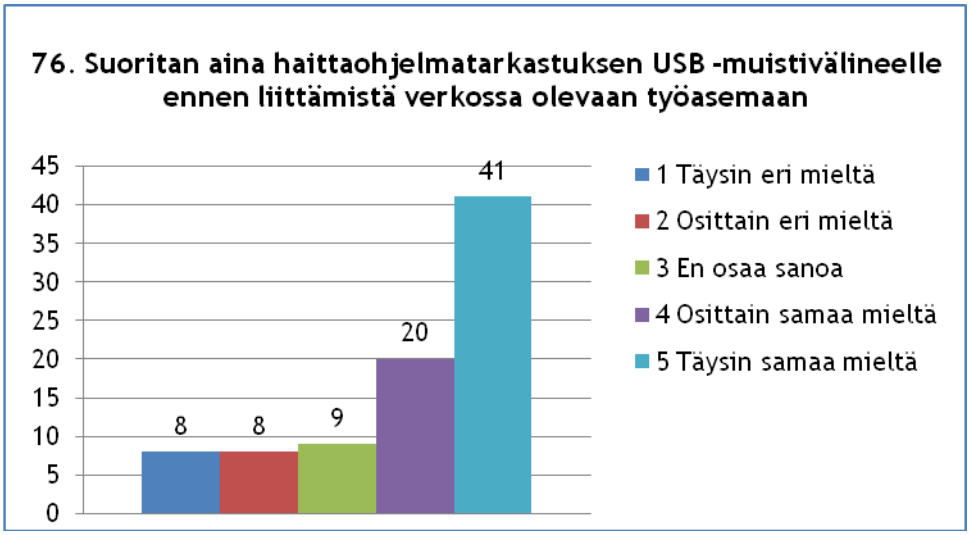
Kuvio 28: Väittämän ”73. Olen käyttänyt omaa USB – muistivälinettä työasemalla” vastausjakauma

Väittämässä 74 kysyttiin, onko henkilöstöllä varmuuskopiot omista tärkeistä tiedostoistaan? Vastaajista 32 henkilöllä (37,2 %), on varmuuskopiot omista tärkeistä tiedostoistaan (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 48 henkilöä (55,8 %), ei ole ottanut varmuuskopioita omista tärkeistä tiedostoistaan (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia oli kuusi (7 %) kappaletta.



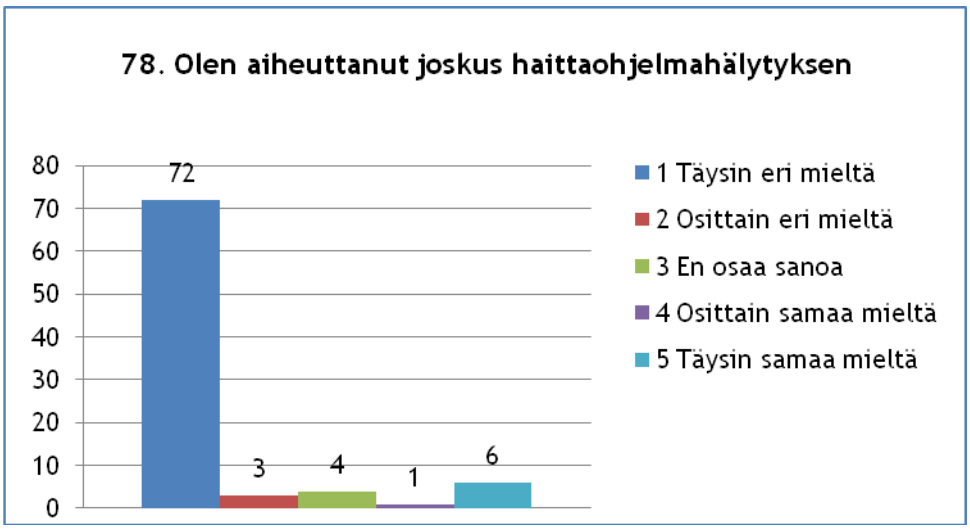
Kuvio 29: Väittämän ”74. Minulla on varmuuskopiot omista tärkeistä tiedostoista” vastausjakauma

Väittämä 76, joka koski USB – muistivälineille tehtäviä haittaohjelmatarkastuksia, 61 henkilöä (70,9 %) ilmoittaa, suorittavansa aina haittaohjelmatarkastuksen USB – muistivälineelle, ennen sen liittämistä verkkotyöasemaan (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 16 henkilöä (18,6 %) ilmoittaa, ettei aina suorita tarkastusta (”Täysin eri mieltä” ja ”Osittain eri mieltä”). Vastaajista yhdeksän henkilöä (10,5 %) vastasi ”En osaa sanoa”.



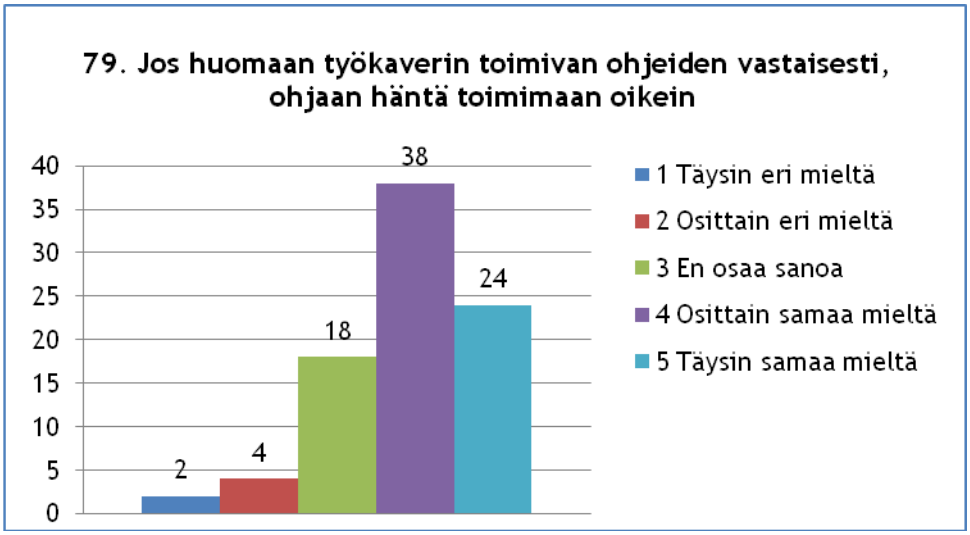
Kuvio 30: Väittämän ”74. Suoritan aina haittaohjelmatarkastuksen USB – muistivälineelle ennen liittämistä verkossa olevaan työasemaan” vastausjakauma

Väittämä 78, joka koski haittaohjelmahälytyksen aiheuttamista, seitsemän (8,1 %) henkilöä ilmoittaa, joskus aiheuttaneensa haittaohjelmahälytyksen (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Vastaajista 75 henkilöä (87,2 %), ei ole aiheuttanut haittaohjelmahälytystä (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia oli annettu neljä (4,7 %) kappaletta.



Kuvio 31: Väittämän ”78. Olen aiheuttanut joskus haittaohjelmahälytyksen” vastausjakauma

Väittämässä 79 kysyttiin, ohjeistaako vastaaja itse, työkaveriaan toimimaan ohjeiden mukaisesti, jos havaitsee niiden vastaista toimintaa? Vastaajista 62 henkilöä (72,1 %), ohjaa työkaveria toimimaan oikein, jos hän toimii ohjeiden vastaisella tavalla (”Täysin samaa mieltä” ja ”Osittain samaa mieltä”). Kuusi henkilöä (7 %) ilmoittaa, ettei ohjaa työkaveria toimimaan ohjeiden mukaisesti (”Täysin eri mieltä” ja ”Osittain eri mieltä”). ”En osaa sanoa” vastauksia oli annettu 18 (20,9 %) kappaletta.



Kuvio 32: Väittämän ”79. Jos huomaan työkaverin toimivan ohjeiden vastaisesti, ohjaan häntä toimimaan oikein” vastausjakauma

8.4 Avoimet kysymykset

81. Mitkä ovat mielestäsi työpisteesi suurimmat tietoturvallisuusongelmat?

Kysymykseen 81, jossa selvitettiin henkilöstön mielipiteitä oman työpisteen suurimmista tietoturvallisuusongelmista, vastasi 44 henkilöä (51,2 %) kaikista vastaajista. Suurimmaksi tietoturvallisuusongelmaksi henkilöstön keskuudessa nousi selkeästi liian monet tietojärjestelmät, jotka tarvitsevat kirjautumisen yhteydessä käyttäjätunnusta sekä salasanaa. Käyttäjätunnuksiin ja salasanoihin liittyviä kommentteja oli 11 vastauksessa (25 %).

”Liian monta tietojärjestelmää ja liian monta käyttäjätunnusta ja salasanaa.”
”Liian useat järjestelmät jotka vaativat salasanaa.”
”Aivan liikaa tietojärjestelmiä, joissa pitää olla salasana.”
”Minulla on tällä hetkellä käytössä järjestelmiä, johon käytän eri salasanoja nopeasti lueteltuna 10 kpl.”
”23 erilaista kirjautumistunnusta ja niiden salasanat.”
”Salasanojen älytön määrä…”
”Salasanojen paljous.”
”Salasanalaput näppäimistön alla/PIN -koodi dymotarralla toimikortissa.”
”Salasanoja on paljon ja vaadittavat salasanat ovat monimutkaisia ja niitä joudutaan vaihtamaan usein, niin 'työpöytien' muistilaput salasanoille ovat mielestäni suurin tietoturvariski organisaatiossamme.”
”Käytettävien salasanojen laatu ja säilytys eivät ole hyvällä tasolla.”
”Motivaatio kunnolliseen salasanojen hallintaan on huono, kun salasanamäärä kasvaa yli kymmenen.”

Suureksi tietoturvallisuusongelmaksi koettiin myös henkilöstön asenteet, suhtautuminen tietoturvallisuuteen ja muutoin henkilöstön toimintaan liittyvissä asioissa. Henkilöstön asenteisiin liittyviä kommentteja oli 9 vastauksessa (20,5 %).

”Henkilöstön huoleton asennoituminen tietoturvallisuuteen.”
”Ihmiset itse!”
”Välinpitämättömyys tietoturvaa kohtaan. Helposti ajatellaan, että eihän nämä asiat oikeasti ketään ulkopuolista kiinnosta.”
”Henkilöstön suhtautuminen luokiteltuun tietoon.”
”Pöydille jääneet paperit ja muistitikut.”
”Avoimet kirjat, paperit ja dokumentit pöydillä.”
”Korttien jääminen lukijalaitteisiin, paperiasiakirjat näkyvillä ja ovet auki.”
”Asenteet tietoturvallisuutta kohtaan.”
”Työasioihin/henkilöstöön liittyvät keskustelut työpaikan ulkopuolella.”
”Työntekijät vapaa-ajallaan hummailemassa ja humalassa ovat avoimia tietolähteitä, joita on hyvin helppo koukuttaa!”
”Joidenkin työntekijöiden työpaikan ulkopuolinen ja epämääräinen kaveripiiri.”

Kohtuullisen suurena ongelmana pidettiin tiedon ja koulutuksen puutteellisuutta sekä ohjeistuksen jäykkyyttä. Puutteelliseen koulutukseen ja hankalaan ohjeistuksen liittyviä kommentteja oli 6 vastauksessa (13,6 %).

”Puutteellinen koulutus.”
”Henkilöstön tietoisuus tietoturva-asioista.”
”Tiedon puute käytännön toimista.”
”Tiedon puute.”
”Tietämättömyys ohjeista ja käytännöistä.”
”Yleinen tietämättömyys siitä mitä saa tehdä mitä ei.”
”Kukaan ei osaa sanoa mistä löytyy viimeisimmät tietoturvaohjeet, koska asiakirjoihin tulee päivityksiä ja ne julkaistaan omina täydentävinä ohjeina.”
”Ohjeita on liikaa ja ne ovat osin ristiriitaisia.”
”Tietoturvaohjeistukset eivät palvele todellista elämää.”
”Ohjeistuksen täydellinen noudattaminen estää toiminnan, koska ohjeistuksen vaatimia välineitä ei ole saatavilla.”
”Jos tietoturva ei mahdollista työntekoa, onko silloin kaikki hyvin?”

Työpisteiden fyysinen tietoturvallisuus koettiin joiltakin osin myös ongelmana. Työpisteen sijaitessa avokonttorissa, jossa liikkuu usein organisaation ulkopuolisia henkilöitä, tietoturvallisuus voi heiketä. Papereita voidaan säilyttää lukituissa kaapeissa ja työasemalta kirjautua pois työpisteeltä poistuttaessa, mutta puhelinkeskustelut kuulevat ympärillä olevat henkilöt. Usein tietoa tarvitsee katsoa työasemalta, jolloin ei voi lähteä puhumaan muualle.

82. Mitkä ovat mielestäsi syitä tietoturvallisuusongelmiin?

Kysymykseen 82, joka koskee syitä mahdollisiin tietoturvallisuusongelmiin, vastasi 47 henkilöä (54,7 %) kaikista vastaajista. Suurimmaksi syyksi tietoturvallisuusongelmiin nousi selkeästi ihminen, asenteet ja suhteutuminen työhön ja tietoturvallisuuteen. Kuudessa (12,8 %) vastauksessa mainittiin henkilöstön välinpitämättömyys. Henkilöstön asenteisiin liittyviä kommentteja oli 15 vastauksessa (31,9 %).

”Asenne ja ihminen.”
”Työntekijöiden tahattomat unohdukset/vahingot, välinpitämättömyys ja huolimattomuus.”
”Asenteet ja suhtautuminen”
”Käyttäjien asenne.”
”Välinpitämättömyys on yksi tekijä.”
”Ajanpuutteen, asennoitumisen ja laiskuuden vuoksi työntekijät oikaisevat käsketyistä toimintamalleista.”
”Välinpitämättömyys ja kiire.”
”Ihmisten välinpitämättömyys.”
”Haluttomuus oppia uutta.”
”Välinpitämättömyys”
”Huolimattomuus - Ei ole ennenkään mitään tapahtunut - Ei minulla ole työssäni mitään tärkeää, joka ulkopuolisia hyödyttäisi.”
”Kaikki ihmiset eivät suhtaudu vakavasti tietoturvallisuuteen ja sen tärkeyteen.”
”Ei pidetä todennäköisenä, että joku voisi käyttää haltuun saamaansa tietoa väärin.”

Suureksi ongelmien aiheuttajaksi koettiin myös tietämättömyys sekä puutteellinen ja riittämätön tietoturvallisuuskoulutus. Puutteelliseen koulutukseen ja tiedon puutteeseen liittyviä kommentteja oli 7 vastauksessa (14,9 %).

> *”Tietoturva-asiat muuttuvat niin kovaa vauhtia jatkuvasti ja asiakirjoja tulee niin paljon, että on mahdotonta pysyä perässä siitä, mitä saa tehdä, miten toimitaan?”*
> *”Koulutuksen riittämättömyys.”*
> *”Koulutus tilaisuuksien puute riittävin väliajoin.”*
> *”Tiedon puute päivittäisistä toimenpiteistä.”*
> *”Huono koulutus.”*
> *”Tiedon puute.”*
> *”Ei tiedetä mitä tehdään tai inhimillinen erehdys!”*
> *”Ei osata erottaa, mistä voidaan puhua ja mistä ei.”*
> ”Asenteisiin *vetoavaa koulutusta tulisi olla lisää.”*
> *”Osaaminen luo varmuutta ja ammattiylpeyttä.”*

Ohjeistuksen kankeus ja ristiriitaisuus työtehtävien suorittamisen kannalta sekä jatkuva muuttuminen luo paineita tietoturvallisten toimintatapojen noudattamiselle. Hankalaan ohjeistukseen liittyviä kommentteja oli 6 vastauksessa (12,8 %).

> *”Vajavainen ja hankalalta tuntuva ohjeistus.”*
> *”Tietoturvallisuuden vuoksi käskettyjen toimenpiteiden vaivalloisuus, jotka hankaloittavat sujuvaa työntekoa.”*
> *”Ohjeistuksen mukaan toimiminen tekee työskentelystä lähes mahdotonta.”*
> *”Täydellisen tietoturvallisuuden noudattaminen tuo aivan liikaa ongelmia käytännön työn toteutukseen.”*

83. Mistä tietoturvallisuuteen liittyvistä asioista kaipaisit koulutusta?

Kysymyksessä 83 haettiin tietoa, mistä tietoturvallisuuteen liittyvistä asioista henkilöstö haluaisi koulutusta. Kysymykseen vastasi 40 henkilöä (46,5 %) kaikista vastaajista. Selvästi suurin tarve on asiakirjojen luokitteluun liittyvissä asioissa. Mitä eri tietojen suojaustasot todella tarkoittavat sisällöllisesti ja kuinka niitä tulee käsitellä? Suojaustasoihin ja tiedon luokitteluun liittyvää koulutusta toivottiin 11 vastauksessa (27,5 %).

”Tietoturvaluokkien määrittely on liian hankalaa.”
”Käyttöluokitusten määrittelyssä sekä siinä, miten mitäkin turvaluokitusluokkaa tulikaan käsitellä.”
”Asiakirjaluokittelussa ja paperiasiakirjojen kanssa toimimisessa.”
”Itse luotavien asiakirjojen ja tiedostojen luokittelu.”
”Asiakirjojen luokittelua olisi hyvä kerrata ainakin vuoden välein.”

Toinen vahvasti esille noussut koulutustarve oli tiedostojen salaamiseen liittyvät toimenpiteet (8/20 %). Myös tietoturvallisuuden perusteisiin liittyvistä asioista sekä niiden kertaamisesta säännöllisin väliajoin toivottiin koulutusta (6/15 %). Yksittäisissä vastauksissa kaivattiin koulutusta henkilötietojen käsittelystä, USB – muistivälineiden käytöstä, haittaohjelmatarkastuksen suorittamisesta, tiedonsiirrosta erillisten tietojärjestelmien välillä ja tiedostojen varmuuskopioinnista. Muutamaan lomakkeeseen oli vastattu, että *”En mistään”*.

”Perusasioita pitäisi säännöllisesti kerrata samalla tavoin kuin ensiaputaitoja.”
”Välineet ja ohjeet löytyy, veikkaisin että asenteesta löytyy kouluttamista.”

84. Mistä tietoturvaan liittyvistä asioista haluaisit tiedotettavan enemmän?

Kysymykseen 84, joka koski tietoturvallisuudesta tiedottamista, vastasi 16 henkilöä (18,6 %) kaikista vastaajista. Pääosa vastaajista haluaisi enemmän tiedotusta ajankohtaisista tietoturvallisuuteen liittyvistä asioista, päivittäisistä toiminnoista ja raportointia mahdollisista tietoturvatapahtumista (10/62,5 %). Yksittäisissä vastauksissa haluttiin tiedotettavan enemmän tietotekniikan perusteista, järjestelmämuutoksista, tietojen säilyttämisestä, henkilöstön vastuista sekä tiedon suojaustasoista.

”Tietoiskut siitä mikä on 'trendikästä' eli ajankohtaista.”
”Mahdollisista murroista, madoista ym. organisaation tietoverkoissa.”
”Esimerkkejä tapahtuneista ja mitä olisi voinut käydä jos...”
”Kertoa valikoivasti koko väelle faktoja, jotta väki ei pitäisi näitä asioita 'jamesbond' -juttuina.”

85. Jos olet itse joskus toiminut ohjeiden vastaisesti, mitkä ovat olleet syitä siihen?

Kysymykseen 85, joka koski syitä mahdolliseen ohjeiden vastaiseen toimintaan, vastasi 43 henkilöä (50 %) kaikista vastaajista. Suurimpia syitä ohjeiden vastaiseen toimintaa on ollut työtehtävien välttämätön hoitaminen ja kiire (15/34,9 %).

”Toiminta olisi estynyt täysin jos ohjeita noudattaisi täysin.”
”Tämä järjestelmä on niin sekava, hankala ja käytännön töiden kannalta täysin mahdoton, mikäli kaikkia annettuja ohjeita aina ja joka asiassa noudatetaan.”
”Job has to be done.”
“Tarve saada homma hoidetuksi.”
”Syy on ollut työn teon joustavuus.”
”Työtehtävät, jotka on pakko toteuttaa.”

Yhteensä 9 vastauksessa (30,9 %) viitattiin henkilöstön tietämättömyyteen, huolimattomuuteen, ajattelemattomuuteen, välinpitämättömyyteen, osaamattomuuteen tai laiskuuteen. Yksittäisissä lomakkeissa syiksi määriteltiin monimutkaiset tietojärjestelmät sekä niiden toimimattomuus.

86. Millä keinoin mielestäsi omaa tietoturvallisuustietoisuuttasi voitaisiin parantaa?

Kysymyksessä 96, vastaajilta pyydettiin keinoja, joilla juuri hänen tietoturvallisuustietoisuuttaan voitaisiin parantaa. Kysymykseen vastasi 29 henkilöä (33,7 %) kaikista vastaajista. Valtaosassa vastauksista (19/65,5 %) toivottiin säännöllistä koulutusta parantamaan tietoturvatietoisuutta. Myös tietojärjestelmien toimimattomuuden paranemista toivottiin sekä ohjelmistovalikoiman paranemista työasemilla (7/24,1 %). Ohjeistuksen järkeistäminen tuli esille muutamassa vastauksessa.

”Lisää koulutusta. Asenne kuntoon koko henkilöstön osalta!”
”Koulutustilaisuudet edes muutaman kerran vuodessa.”
”Säännöllisin väliajoin toteutettavilla lyhyehköillä infoilla.”
”Näin. Eli asia on esillä, jo tuo kysely toimii hyvänä muistutuksena/kertauksena.”
”Asenne kasvatuksella.”
”Yhteistä, säännöllistä, lyhyttä ja ytimekästä kertauskoulutusta kaikille työntekijöille.”
”Jakamalla ohjeistuksen vaatimat työvälineet.”
”Paikka, josta helposti saatavilla selkeät ohjeet eri temppujen tekemiseen esim. haittaohjien tarkastukseen.”

87. Millä keinoin mielestäsi omaa motivaatiotasi tietoturvallisuutta kohtaan voitaisiin parantaa?

Kysymykseen 87, joka koski keinoja tietoturvallisuuteen kohdistuvan motivaation parantamiseen, vastasi 30 henkilöä (34,9 %) kaikista vastaajista. Motivaatio tietoturvallisuutta kohtaan on vastausten perusteella kohdallaan vastaajista 11 henkilöllä (36,7 %). Motivaation parantamiskeinoiksi eniten vastattiin koulutusta ja informaation jakamista tietoturvallisuusasioista (7/23,3 %). Muita motivaation parannuskeinoja on ohjeistuksien muokkaaminen käyttäjäystävällisemmiksi, tietojärjestelmiin kirjautumisten yksinkertaistamisella sekä palkitsemisella.

> *”En näe ongelmaa omassa motivaatiossani.”*
> *”Motivaatio on koko ajan paranemaan päin, mitä enemmän järjestelmän toimintaa alkaa ymmärtää.”*
> *”Motivaatio lähtee jokaisesta itsestään.”*
> *”Asenteeni asiaan ja sen tärkeyteen ja vakavuuteen on kohdallaan... se vain pitäisi muistaa joka päivä!”*
> *”Ehkä tässä onnistuminen tarkoittaisi eniten asennekasvatusta…”*
> *”Helpoilla, yksinkertaisilla ja selkeillä ohjeilla tai pienillä muistilapuilla ja tietoiskuilla.”*
> *”Yhdellä kirjautumisella on KAIKKI tietojärjestelmät käytettävissä.”*
> *”Jos vuoden aikana on nolla negatiivista tapahtumaa, voisi jokin muistaminen olla koko työyhteisölle paikallaan. Vaikka kakkukahvit.”*
> *”No joo, millä nyt turhautuneisuutta parannetaan...”*

8.5 Havainnoinnin tulokset

Havainnoinnin tuloksissa ei eritellä jokaista kysymystä vastauksineen, vaan pyritään antamaan kokonaiskuva vastauksista. Havainnoinnin tuloksia ei kirjattu lomakkeelle havainnoinnin aikana, vaan kirjaus tehtiin heti havainnoinnin jälkeen.

Rakennuksien ulko-ovet ja ikkunat olivat suljettuina. Kulunvalvotut ovet olivat pääsääntöisesti kiinni, lukuun ottamatta yhtä kertaa. Ovi oli auki, koska henkilöstön mielestä lukituista ovista kulkeminen oli välillä vaivalloista. Ovi suljettiin välittömästi ja henkilöstöä huomautettiin asiasta. Palo-ovet olivat ohjeistuksen mukaisesti suljettuina. Yksittäisillä työntekijöillä oli työpäivän aikana henkilökortti näkyvillä.

Joidenkin toimistojen ovet olivat lähes poikkeuksetta avoinna, vaikka henkilö ei itse ollut paikalla. Toimintatapa ei muuttunut, vaikka asiasta huomautettiin. Muutamissa toimistoissa ovi oli kiinni, mutta ei lukittuna. Joidenkin toimistojen ovet olivat lukittuina, kun toimistossa ei ollut työntekijää paikalla.

Yksittäisten toimistojen työpöydillä oli asiakirjoja, joita ei olisi saanut olla muiden nähtävillä. Asiakirjoja oli myös jätetty työpöydälle, vaikka oli jo poistuttu työpaikalta. Toimiston paperiroska-astiasta löytyi suojaustason tulosteita. Yhtään USB – muistivälinettä ei löytynyt kiinnitettynä työasemaan, kun työpisteeltä oli poistuttu. Joitakin CD tallenteita oli unohtunut työaseman sisään ja olivat kenen tahansa työasemalle kirjautuvan henkilön käytettävissä. Kyseisistä CD tallenteista ei löytynyt turvaluokiteltua tietoa.

Tauoille poistuttaessa jätettiin kirjautumatta pois työasemalta ja toimikortti jätettiin lukijaan. Toimikortteja oli jätetty lukijoihin myös töistä poistuttaessa. Valtaosa oli kuitenkin kirjautunut työasemalta pois, eikä toimikortti ollut saatavilla. Toimikortteja oli taltioitu näppäimistön tai kirjoitusalustan alle. Yhteen korttiin oli liimattu tarra, jossa luki kortin PIN – koodi. Hiirimaton ja näppäimistön alta löytyi lapuille kirjoitettuja salasanoja.

Kassakaappien ovia oli jätetty avoimeksi vaikka toimistossa ei ollut ketään. Toimiston ovia jätettiin auki, kun poistuttiin tauolle. Muutamia kassakaappeja oli suljettu, mutta ei lukittu, vaikka työhuoneesta poistuttiin. Eräässä toimistossa kassakaappi oli lukittuna, mutta avain oli hyllyllä saatavilla.

Kaikissa toimistoissa tietoturvamääräykset eivät toteutuneet puheluiden osalta. Puhe kuului toimistosta käytävälle. Haitta esiintyi varsinkin toimistoissa, joissa oli enemmän kuin yksi työntekijä.

9 Johtopäätökset ja tulosten arviointi

Organisaation suurimmaksi tietoturvariskiksi sanotaan organisaation omaa henkilöstöä. Tämänkin tutkimuksen mukaan on huolestuttavinta ihmisten yleinen suhtautuminen tietoturvallisuuteen. Henkilöstö tietää yleisesti ottaen, mitä tietoturvallisuus on, mutta harva tietää tai osaa ajatella, mitä kaikkea se todellisuudessa on ja mitä se vaatii käyttäjiltä. Tietoturvallisuutta pidetään henkilöstön keskuudessa yleisesti toiminnan hidastajana. Henkilöstön keskuudessa on liikaa vallalla käsitys, ettei tämä asia kosketa minua ja ettei minulle ennenkään ole mitään sattunut. Työelämän kiivastahtisuudella on suuri vaikutus henkilöstön suhtautumiseen myös tietoturvallisuudessa. Kiire itse ei aiheuta mitään, vaan tekijänä on aina henkilöstö. Kiire voi kuitenkin olla osatekijänä tietoturvallisuusohjeistuksen vastaiseen toimintaan. Toisaal-

ta kun henkilöstöllä on paljon tekemistä ja kiireellä yritetään selvitä niistä, saattaa jäädä monta asiaa huomioimatta. Kaikkia erheitä ei siis aiheuteta tahallisesti.

Tutkimuksessa tehdyn kyselyn vastaanottajia oli 327 henkilöä ja kyselyyn vastasi 87 henkilöä, joten vastaamatta jättäneiden määrä oli 240 henkilöä (73,4 %). Mistä johtuu niin korkea vastaamatta jättäneiden määrä? Kertooko se jotakin henkilöstön asenteista tietoturvallisuutta kohtaan? Yleisten havaintojen perusteella, henkilöstö on kiireistä ja töitä on jokaisella paljon. Johtopäätöksenä voi tulkita, että kyselyyn ei ole ollut aikaa vastata tai se ei ole kiinnostanut henkilöstöä.

9.1 Tietoturvatietoisuus ja asenteet

Organisaation tietoturvallisuuteen liittyvä ohjeistus tulee johto-organisaatiosta, joten niistä poikkeavia paikallisia ohjeita ei voida laatia. Ohjeistus täytyy saattaa paremmin henkilöstön tietoisuuteen.

Organisaation ohjeistus edellyttää, että jokainen organisaatioon tuleva uusi henkilö koulutetaan tietoturvallisuuskäytänteiden osalta mahdollisimman pian, mielellään ennen tietojärjestelmien käyttöönottoa. Organisaatiossa koulutusta ei ehditä antamaan aina heti kun uusi henkilö tulee töihin, vaan aikaa saattaa kulua paljonkin. Kouluttaja ei saa aina tietoa ajoissa organisaatioon tulevasta uudesta ihmisestä, jotta tietoturvallisuuskoulutus voitaisiin heti pitää.

Tietoturva-asenteisiin liittyvässä osiossa suurimmiksi epäkohdiksi tulkitaan henkilöstön asenteet ja koulutuksen puute. Tietoturvallisuuden korostaminen aiheuttaa lähes puolille vastaajista ärtymystä. Asenteisiin liittyen erityisen hyvin henkilöstö tiedostaa kuitenkin, myös itse olevansa vastuussa organisaation tietoturvallisuudesta. Positiivista on myös se, että lähes kaikki vastaajat, ilmoittavat tietoturvallisuushenkilöstölle, jos kadottavat USB – muistivälineensä.

Suurimpia tiedonpuutteita henkilöstöllä on tiedostojen salaamisessa, organisaation tietojen luokittelussa ja vaitiolositoumuksen sisällöstä sekä vaikutuksesta. Tiedostojen salaamista kannattaakin harjoitella tulevissa tietoturvallisuuskoulutuksissa. Vaikka yli puolet vastaajista tunteekin organisaation tietoaineistoluokittelun, kannattaa se ottaa koulutuksen aiheeksi. Koulutuksissa tulisi myös kertoa henkilöstölle, vaitiolositoumuksen sisällöstä ja vaikutuksista tarkemmin. Kyselyn ”Oma toiminta” osiossa, ilmenee myös seikkoja, jotka puoltavat vaitiolositoumukseen liittyvien asioiden sisällyttämistä tietoturvallisuuskoulutukseen. Vastaajista lähes puolet ilmoittaa rikkoneensa vahingossa vaitiolositoumuksen ja noin kolmannes vastaajista, ei osaa sanoa ja ei tiedä rikkoneensa vaitiolositoumusta.

Vastauksissa eniten hajontaa oli haittaohjelmatarkastusten suorittamista verkkotyöasemalla koskevassa väittämässä. Yli puolet vastaajista oli vastannut, että tarkastusta ei voi tehdä verkkotyöasemalla tai ”En osaa sanoa”. Organisaation ohjeistuksen mukaisesti, haittaohjelmatarkastuksen voi tehdä verkkotyöasemalla, ellei sitä ole kytketty verkkoon. Kysymystä ei ollut ymmärretty, kuten oli tarkoitettu, tai vaihtoehtoisesti kysymykseen oli vastattu väärin eli asiaa ei tiedetty. Kysymys oli helposti väärin ymmärrettävä ja siinä oli liikaa tulkinnanvaraisuutta.

Toiminnan vaikeutuminen erinäisillä kielloilla aiheuttaa myös henkilöstön toimintaan, motivaatioon ja asenteisiin tietoturvallisuutta kohtaan. Jos esimerkiksi kielletään USB -muistivälineiden käyttö jossakin tietojärjestelmässä, voidaan sillä aiheuttaa toiminnan vaikeutumista. Kun työn tekeminen kohtuuttomasti vaikeutuu, ihmiset eivät sitten noudata kieltoja eivätkä ohjeistusta ja toimivat näin ohjeistuksen vastaisesti. Työt on kuitenkin saatava tehtyä.

9.2 Tietoturvallisuusjohtaminen

Organisaation johto on tietoinen organisaation tietoriskeistä ja suhtautuu niihin tarvittavalla vakavuudella, mutta organisaation johdon sitoutumista tietoturvallisuustyöhön tulisi lisätä. Tietoturvallisuus tulisi saattaa näkyvämmäksi osaksi organisaation kokonaisturvallisuutta myös johdon osalta. Esimiesten asemaa osan henkilöstön tietoturvallisuuskäyttäytymisessä tulisi korostaa sekä esimiesten asenteita tietoturvallisuutta kohtaan luoda myönteisimmiksi.

Tietoturvallisuusjohtamiseen liittyvien vastausten perusteella henkilöstö kokee, että organisaation johto ja esimiehet ottavat pääosin tietoturvallisuuteen liittyvät asiat huomioon toiminnassa. Henkilöstö on siis pääosin tyytyväinen esimiesten toimintaan tietoturvallisuusasioissa. Esimiehet eivät kuitenkaan kannusta, alaisiaan riittävästi huomioimaan tietoturvallisuutta työssään. Esimiehet puuttuvat hyvin tilanteisiin, joissa havaitsevat tietoturvallisuusohjeistuksen vastaista toimintaa. Lähes kaikki vastaajat ovat sitä mieltä, että tietoturvallisuus on organisaatiossa tärkeä, mutta johdon täytyisi osoittaa enemmän sitoutuneensa tietoturvallisuuden kehittämiseen.

Organisaation johtoon ja esimiehiin liittyvissä väittämiin oli vastattu erityisen paljon vastausvaihtoehdolla ”En osaa sanoa”. Syitä suureen määrään voivat olla, ettei henkilöstöllä ole kokemusta kysytystä asiasta tai ei haluta kommentoida johdon ja esimiesten suhtautumista ja sitoutumista tietoturvallisuuteen. Tietoturvallisuuskoulutuksia suunnitellessa tulee ottaa huomioon erikseen esimiesasemassa oleva henkilöstö. Heille tulee suunnitella erillinen koulutus, jossa voitaisiin keskittyä enemmän alaisten motivointiin tietoturvallisuutta kohtaan.

9.3 Henkilöstön toiminta

Omaan toimintaan liittyvien väittämien vastauksista, ilmenee paljon ohjeiden vastaista toimintaa. Huolestuttavaa on myös se, että lähes puolet vastaajista ilmoittaa, rikkoneensa vaitiolositoumuksen. Toimikortin lainaaminen työkaverille ja toisen henkilön tunnuksien käyttäminen on selkeästi organisaation tietoturvallisuusohjeistuksen vastaisia toimintatapoja. Huomioitavaa on, että lähes puolella kyselyyn vastanneista, ei ole varmuuskopioita omista tärkeistä tiedostoistaan. Kyselystä ei selviä, johtuuko varmuuskopioiden puute ajattelemattomuudesta vai siitä, ettei niitä osata tehdä. Varmuuskopioiden tärkeydestä kannattaa muistuttaa henkilöstöä tietoturvallisuuskoulutuksissa tai informaatioluonteisesti tiedottamalla.

Vaikka havainnointi ajanjakso ei ollut kovin pitkä, saatiin kuitenkin kerättyä tärkeää ja kyselyä tukevaa tietoa. Kyselyn vastauksiin ei voi sataprosenttisesti luottaa, joten havainnoinnin perusteella saatiin tietoa, miten henkilöstö toimii oikeassa tilanteessa. Havaintojen perusteella henkilöstön välinpitämätön käyttäytyminen tietoturvallisuuteen liittyen osoittaa, että henkilöstön tietoturvatietoisuutta on kehitettävä. Monissa asioissa toimitaan selkeästi ja tietoisesti vastoin tietoturvallisuusohjeistusta. Huomautuksista huolimatta henkilöstö jätti toimiston ovia auki tauoille poistuessaan ja työasemilta jätettiin kirjautumatta ulos. Näin ollen kaikki tietojärjestelmät olivat kenen tahansa huoneeseen tulevan henkilön käytettävissä.

9.4 Ongelmat tietoturvatietoisuudessa

Avoimien kysymysten perusteella suurimmiksi tietoturvaongelmiksi henkilöstön keskuudessa nousi selkeästi liian monet tietojärjestelmät, jotka tarvitsevat kirjautumisen yhteydessä käyttäjätunnusta sekä salasanaa. Useiden eri tietojärjestelmien ja niihin liittyvien käyttäjätunnusten sekä salasanojen kanssa on opittava elämään. Ohjelmistot organisaation käyttöön määritellään johto-organisaatioissa, eikä niihin paikallisesti voida vaikuttaa kuin palautetta antamalla. Koulutuksessa tulee kiinnittää riittävästi huomiota käyttäjätunnusten ja salasanojen hallintaan.

Henkilöstön asenteet ja suhtautumiseen tietoturvallisuutta kohtaan, oli myös vastauksissa suurena tietoturvaongelmana työpisteillä. Myös koulutuksen ja tiedonpuutetta pidettiin ongelmana. Henkilöstö toimii joissakin tilanteissa, tarkoituksen mukaisesti ohjeistusta vastaan tai vaihtoehtoisesti, henkilöstö ei tiedä ohjeistuksesta riittävästi. Koulutuksessa olisi pyrittävä vaikuttamaan henkilöstön suhtautumiseen ja asenteisiin tietoturvallisuutta kohtaan. Koulutuksessa tulisi myös korostaa jokaisen henkilön vastuuta myös työkaverin toiminnasta. Jokaisen täytyisi puuttua työkaverin tietoturvallisuusohjeistuksen vastaiseen toimintaan huomauttamalla tai ohjaamalla toimimaan ohjeistuksen mukaisesti.

Selkeästi suurimpina syinä tietoturvatietoisuuteen liittyviin ongelmiin pidettiin henkilöstöä itseään, tiedonpuutetta ja ohjeistuksen kankeutta. Henkilöstön asenteissa ja suhtautumisessa tietoturvallisuutta kohtaan on paljon parannettavaa. Näitä ja henkilöstön tietoturvatietoisuutta voidaan parantaa kouluttamalla. Koulutusta kaivattiin erityisesti tiedostojen salaamisesta, organisaation tietoturvaluokittelusta ja tietoturvallisuuden perusteista. Vastauksissa toivottiin myös, tietoiskuja tietoturvallisuuden ajankohtaisista asioista. Koulutuksen lisäämisellä voitaisiin monen vastaajan mielestä parantaa asenteita ja motivaatiota tietoturvallisuutta kohtaan.

10 Yhteenveto

Suurimmaksi puutteeksi tutkimuksen mukaan nousee selkeästi koulutuksen ja informaation puute. Organisaatiossa tulisikin jatkossa laatia vuosittainen tietoturvallisuuden koulutussuunnitelma. Koulutustilaisuuksia kannattaisi järjestää vuoden aikana ainakin 5-6 kertaa. Tietoturvallisuusasiat olisi hyvä sisällyttää, organisaatiossa järjestettävien sisäisen informaatiopäivien aiheiksi. Tietoturvallisuutta voidaan tuoda näkyvämmäksi jokaiselle, esimerkiksi tietoturvallisuuteen liittyvillä julisteilla ja hiirimatoilla. Jatkossa voidaan myös pohtia henkilöstön palkitsemista tietoturvallisten toimintatapojen edistämisestä työpisteellä.

Kyselyssä on joidenkin kysymysten osalta liikaa tulkinnanvaraisuutta, joten kyselyn väittämäosion vastauksiin ei voi täysin luottaa. Avoimet kysymykset täydensivät kyselyä ja vastaukset antoivat arvokasta tietoa, esimerkiksi koulutuksen sisällön tarkempaan suunnitteluun. Havainnoimalla saadut tiedot ja henkilöstön toimintatapoihin liittyvät huomiot toivat kyselylle lisää luotettavuutta. Kaikkiaan tutkimuksella kuitenkin saatiin perusteita ja tukea tietoturvallisuuskoulutuksen suunnitteluun, jotta koulutus tukisi parhaalla mahdollisella tavalla tietoturvallisuustyötä organisaatiossa.

Jos samankaltainen kyselytutkimus järjestetään henkilöstölle myös jatkossa, kannattaa miettiä tarkemmin kysymysten määrää ja niiden ymmärrettävyyttä sekä oikeakielisyyttä. Likertin viisiasteinen vastausasteikko, ei ole ehkä paras mahdollinen vastauksia tulkittaessa. Vastaukset eivät ole täysin luotettavia, esimerkiksi vastausvaihtoehdon ”En osaa sanoa” osalta. Jää liikaa tulkinnanvaraiseksi, mitä vastaaja on tarkoittanut vastausvaihtoehtoa valitessaan. Eikö vastaaja ole ymmärtänyt kysymystä vai, onko vastaaja tarkoittanut vastatessaan, että ei osaa sanoa vai, eikö vastaajalla ole kokemusta kysytystä asiasta.

Lähteet

Eskola, A. 1975. Sosiologian tutkimusmenetelmät 2. Porvoo: WSOY.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Porvoo: WS Bookwell.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2008. 13.-14., osin uudistettu painos. Tutki ja kirjoita. Helsinki: Tammi.

Kuusela, H. & Ollikainen, R. (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampereen Yliopisto.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Juva: WS Bookwell.

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

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

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOY-pro.

Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. 2003. VAHTI 6/2003. Valtionvarainministeriö. Helsinki: Edita Prima.

Peltonen, M. & Ruohotie, P. 1987. Motivaatio. Menetelmiä työhalun parantamiseksi. Keuruu: Otava.

Ruohotie, P. 1998. Motivaatio, tahto ja oppiminen. Helsinki: Edita.

Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. 2007. VAHTI 3/2007. Valtionvarainministeriö. Helsinki: Edita Prima.

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

Sähköiset lähteet:

Suurin tietoturvauhka on työntekijä. 2008. MicroPc. Viitattu 12.2.2011. http://www.mikropc.net/kaikki_uutiset/article231367.ece

Työntekijä on pk-yrityksen suurin tietoturvauhka. 2007. Tietoviikko. Viitattu 12.2.2011. http://www.tietoviikko.fi/kaikki_uutiset/article134756.ece

Valtiovarainministeriö. 2011. Tietoturvallisuus. Viitattu 14.3.2011. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

Kuviot

Taulukot

Liitteet

Liite 1: Kyselyn saateviesti

Arvoisa vastaanottaja!

Organisaatio x:n henkilöstölle on laadittu "Tietoturvatietoisuus 2011" kysely, jonka tarkoituksena on saada perusteita tietoturvallisuuskoulutuksen kehittämiseen henkilöstön tarpeiden mukaiseksi niin, että henkilöstö olisi motivoitunutta koulutukseen sekä kokisi tietoturvallisuuden tärkeäksi ja täten myös sitoutuisi toiminnassaan noudattamaan annettuja ohjeita ja toimintatapoja.

Tietoturvallisuus on osa jokaisen organisaation toimintaa ja kokonaisturvallisuutta. Usein tietoturvallisuus mielletään tietotekniikaksi, tekniseksi suojaukseksi ja virustorjunnaksi, vaikka tosiasiassa suurin osa tietoturvallisuudesta on lähtöisin organisaation oman henkilöstön toiminnasta. Valtioneuvoston periaatepäätös edellyttää, että kaikilla valtionhallinnossa työskentelevillä henkilöillä täytyy olla riittävä tietoturvaosaaminen. Henkilöstön tietoturvatietoisuutta on myös seurattava säännöllisesti ja kehitettävä jatkuvasti.

Kaikki kyselyn vastaukset tullaan käsittelemään nimettöminä ja ne ovat luottamuksellisia. Vastauksia käsittelee vain opiskelija Mervi Kelloniitty. Osaa kyselyn tuloksista tulen esittämään opinnäytetyössäni Laurea-ammattikorkeakoulussa, kuitenkin niin, että organisaatiota ei mainita työssäni.

Kyselyn vastaaminen kestää noin 10 minuuttia.
Vastaa kyselyyn viimeistään perjantaina xx.x.2011 kopioimalla oheinen osoite: https://xxx ja liittämällä se Internet-selaimen osoitekenttään.

Jokainen vastaus on arvokas tietoturvatietoisuuden ja -koulutuksen kehittämiselle.

Kiitos vaivannäöstäsi!
Terveisin Mervi Kelloniitty

Liite 2: Kyselyn muistutusviesti

Arvoisa vastaanottaja!

Muistutan "Tietoturvatietoisuus 2011" kyselyyn vastaamisesta.

Kyselyn tarkoituksena on saada perusteita tietoturvallisuuskoulutuksen kehittämiseen henkilöstön tarpeiden mukaiseksi niin, että henkilöstö olisi motivoitunutta koulutukseen sekä kokisi tietoturvallisuuden tärkeäksi ja täten myös sitoutuisi toiminnassaan noudattamaan annettuja ohjeita ja toimintatapoja.

Tietoturvallisuus on osa jokaisen organisaation toimintaa ja kokonaisturvallisuutta. Usein tietoturvallisuus mielletään tietotekniikaksi, tekniseksi suojaukseksi ja virustorjunnaksi, vaikka tosiasiassa suurin osa tietoturvallisuudesta on lähtöisin organisaation oman henkilöstön toiminnasta. Valtioneuvoston periaatepäätös edellyttää, että kaikilla valtionhallinnossa työskentelevillä henkilöillä täytyy olla riittävä tietoturvaosaaminen. Henkilöstön tietoturvatietoisuutta on myös seurattava säännöllisesti ja kehitettävä jatkuvasti.

Tällä hetkellä kyselyn vastausprosentti on 14 %.

Kaikki kyselyn vastaukset tullaan käsittelemään nimettöminä ja ne ovat luottamuksellisia. Vastauksia käsittelee vain opiskelija Mervi Kelloniitty. Osaa kyselyn tuloksista tulen esittämään opinnäytetyössäni Laurea-ammattikorkeakoulussa, kuitenkin niin, että organisaatiota ei mainita työssäni.

Kyselyn vastaaminen kestää noin 10 minuuttia.
Vastaathan kyselyyn viimeistään perjantaina xx.xx.2011 kopioimalla oheinen osoite: https://xxx ja liittämällä se Internet-selaimen osoitekenttään.

Jokainen vastaus on arvokas tietoturvatietoisuuden ja -koulutuksen kehittämiselle.

Kiitos vaivannäöstäsi!
Terveisin Mervi