LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Palveluntuottajan tietoturvallisuustietoisuuden kehittäminen organisaatiossa

Masalin, Tuomas

2017 Laurea

Laurea-ammattikorkeakoulu

LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

# Palveluntuottajan tietoturvatietoisuuden kehittäminen organisaatiossa

Tuomas Masalin
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Syyskuu, 2017

**Laurea-ammattikorkeakoulu** **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Tradenomi

Tuomas Masalin

**Palveluntuottajan tietoturvatietoisuuden kehittäminen organisaatiossa**

Vuosi 2017 Sivumäärä 42

Tässä opinnäytetyössä tutkitaan palveluntuottajan tietoturvatietoisuuden nykytilaa, palveluntuottajan tietoturvaosaamisen kehittämiseksi. Tavoitteena on löytää tietoturvallisuuden kehityskohteita ja tunnistaa palvelun ulkoistamisen aiheuttamia tietoturvallisuuden kehittämishaasteita kohdeorganisaatiolle.

Opinnätetyössä on käytetty kvalitatiivista tapaustutkimusta, joka sisältää kirjallisuuskatsaksen, kyselytukimuksen kohdeorganisaation palveluntuottajan henkilöstölle ja havainnointi osuuden. Palveluntuottajan tietoturvatietämystä ei ole ennen tutkittu.

Kyselytutkimus koostui kuudesta osa-alueesta; yleinen osio, ohjeet ja koulutus, työasemien turvallisuus, tietoaineisto, viestintä sekä muut hälytykset. Kysely lähetettiin palveluntuottajan vakituiselle henkilöstölle yhteensä 15 henkilölle. Kyselyyn vastasi 10 henkilöä. Tulokset käsiteltiin anonyymisti vastausten yhteenvedosta massatietona, eikä niitä voida yksilöidä vastaajiin.

Tutkimustulosten perusteella suurimmiksi kehityskohteiksi osoittautuivat koulutuksen puute, palveluntuottajan kohdeorganisaation tietoturvaohjeiden tuntemuksen puute sekä viestintä. Tutkimuksen tuloksien perusteella analysoitiin palveluntuottajan ja kohdeorganisaation yhteistyöllä toteutetun koulutuksen olevan tehokkain keino parantaa palveluntuottajantietoturvallisuudessa havaittuja kehittämiskohteita.

Asiasanat: Tietoturvatietoisuus, Tietoturvallisuus, Tietotuvallisuuskoulutus

**Laurea University of Applied Sciences** **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Tuomas Masalin

**Developing Information Security Awareness in an Organization**

Year 2017 Pages 42

This thesis investigates the state of service providers' information security awareness in a target organization, so that the level of service providers' information security knowledge can be improved. The objective is to find areas of information security that need improvement and to recognize the challenges that outsourcing generates to the organization.

In this thesis qualitative case study was used as a method; the study consists of literary material, a questionnaire for the service providers' personnel and personal observations within the target organization. The level of service providers' information security awareness hasn't been studied before.

The questionnaire consists of six sections: general information, guides and training, workstation security, data, communications and other alarms. The questionnaire was sent to the service providers' staff that operates the service within the organization, in total 15 persons. 10 persons answered. The results were analyzed anonymously from the summary of answers and participants can not be identified.

The results of the study indicate that the areas that need the most improvement in information security were insufficient information security education, lack of knowledge about the target organization's instructions and communications. According to the results the most effective way to improve all three areas that needed to be improved was to arrange information security education in cooperation with the service provider and the target organization.

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

Sisällys

# 1 Johdanto

Opinnäytetyössäni tutkin palveluntuottajan henkilöstön tietoturvallisuustietämyksen tasoa organisaatiossa. Työn tavoitteena on selvittää palveluntuottajan henkilöstön tietoturvatietoisuuden nykytaso ja tehdä kehitysehdotuksia, jolla tietoturvallisuustietoisuuden tasoa voidaan kehittää.

Opinnäytetyö on toteutettu yhteistyössä valtion organisaation kanssa, jonne palveluntuottaja tuottaa turvallisuusvalvomotoiminnan. Palveluntuottajan kohdeorganisaatiossa toimivan henkilöstön tietoturvallisuustietämyksen taso selvitetään kvalitatiivisella kyselytutkimuksella, jota täydennetään havainnoinnilla. Tutkimustulosten perusteella pohditaan miten palveluntuottajan tietoturvatietoisuutta voidaan kehittää.

Opinnäytetyötä tehdessäni olen työskennellyt palveluntuottajalla noin 11 vuotta ja idea lopuutyöhön syntyi havainnoista työpaikalla. Niistä suurimpana oli havainto siitä että kohdeorganisaation omalle henkilöstölle tarkoitetut tietoturvallisuusohjeet on sijoitettu tietojärjestelmään, johon palveluntuottajan henkilöstöllä ei ole pääsyä. Tämä rajoittaa palveluntuottajan henkilöstön tietämystä kohdeorganisaation tietoturvaohjeista ja -käytännöistä.

Tässä opinnäytetyössä rajataan tutkimus koskemaan ainoastaan palveluntuottajan turvallisuusvalvomopalveluun. Turvallisuusvalvomopalvelun luonteen vuoksi ei tässä opinnäytetyössä tarkastella tietoturvallisuuden teknistä puolta kovin syvällisesti.

# 2 Toimintaympäristön kuvaus

Opinnäytetyössä tutkittava yksikkö toimii palveluntuottajana valtiohallinnon organisaatiossa. Yksikössä työskentelee tutkimuksen suorittamisen aikan noin 15 vakituista työntekijää ja muutama tuntityöntekijä varalla. Yksikön tehtävänä on hoitaa turvallisuusvalvomoa valtion organisaatiossa, jossa työskentelee tuhansia henkilöitä. Kohdeorganisaation henkilöstö on jakautunut useisiin kiinteistöihin ympäri pääkaupunkiseutua. Turvallisuusvalvomon tehtäviä ovat muun muassa kulun- ja hälytysvalvonta sekä organisaation henkilökunnan neuvonta, avustaminen ja valvonta turvallisuusasioissa.

Palveluntuottajan ylläpitämä turvallisuusvalvomo on toiminassa vuoden jokaisena päivänä 24 tuntia vuorokaudessa. Työvuorojen kestot vaihtelevat kahdeksan- ja kahdetoista tunnin välillä. Jokaisessa työvuorossa työskentelee useita henkilöitä samanaikaisesti ja osa työvuoroista päättyy porrastettuina kellonaikoina. Jatkuvan kolmivuorotyön sekä pitkien työvuorojen keston takia saattaa henkilöstön vapaa-aikojen jaksot olla jopa viikon mittaisia, joka osaltaan asettaa haasteita valvomon sisäiseen viestintään.

Kohdeorganisaation tietoturvapäällikön mukaan palveluntuottajan tietoturvatietoisuutta ei ole koskaan tutkittu. Palveluntuottajan koulutuksen järjestäminen on palveluntuottajan vastuulla. Ongelmana on että organisaation henkilöstölle tarkoitetut tietoturvaohjeet ovat sijoitettuna tietojärjestelmään, johon palveluntuottajan henkilöstöllä ei ole käyttöoikeuksia. Tämän vuoksi on tarpeellista selvittää palvelua tuottavan yksikön henkilöstön tietoturvatietoisuus, jotta se saadaan vastaamaan vaadittavaa tietoturvallisuuden tasoa.

## 2.1 Työn tavoitteet

Opinnäytetyön tavoitteena on selvittää palveluntuottajan henkilöstön tietoturvatietoisuuden taso ja pohtia kehitysehdotuksia sen parantamiseksi. Kehitysehdotuksissa otetaan huomioon selvityksessä havaitut heikkoidet tietoturvatietoisuudessa ja pohditaan keinoja, joilla palveluntuottajan ei-virkasuhteessa olevat työntekijät saisivat tietoa kohdeorganisaation tietoturvaohjeista ja -käytänteistä.

## 2.2 Työn rajaukset

Opinnäytetyössä keskitytään vain palveluntuottajan turvallisuusvalvomon henkilöstön tietoturvatietoisuuden selvittämiseen. Palveluntuottajan aulapalvelut ja kohdeorganisaation henkilöstö rajataan työn ulkopuolelle. Turvallisuusvalvomon toiminnan luonteesta johtuen opinnäytetyössä ei paneuduta tietoturvallisuuden teknisiin puoliin, kuten tietoverkkoihin, ohjelmistoihin, palvelimiin ja tietojärjestelmiin, kuin pintapuolisesti lähinnä kyseisten osa-alueiden vikatilanteiden havaitsemisen ja reagoimisen osalta.

# 3 Tietoturvallisuus

Tässä luvussa käsitellään tietoturvallisuutta, miten se on määritelty, kuinka se huomioidaan valtionhallinossa, minkälaisia riskejä se voi aiheuttaa organisaatiolle ja selitetään keskeisiä käsitteitä tietoturvallisuudessa. Kuten IT-grundschutz-katalogissa todetaan (2013, 10) nykyään valtaosa tiedosta on luotu hyödyntäen tietotekniikkaa. Tietoa myös varastoidaan, käsitellään ja siirretään tietotekniikkaa hyödyntäen. Koska tieto on organisaatiolle yksi tärkeimmistä voimavaroista, sitä täytyy myös suojata kustannustehokkaasti. Luotettavasti toimivat tiedonkäsittelyjärjestelmät ovat korvaamaton osa organisaation toimintaa. Riittämättömästi suojattu tietojärjestelmä on usein aliarvioitu riski, joka voi uhata koko organisaation toimintaa, vaikka tarvittava suojaustaso olisi saavutettavissa kohtuullisilla resursseilla.(IT-Grundschutz-Catalogues 2013, 10.)

## 3.1 Tietoturvallisuuden perusteet

Kirjallisuudessa tietoturvallisuuden määritelmät eroavat hieman toisistaan. Kaikille yhteistä on sama perusajatus, jossa tietoturvallisuus jaetaan kolmeen osatekijään tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Tämä tarkoittaa, että tieto tulee säilyttää luotettavasti, pidettävä nopeasti saatavilla, muuttumattomana ja vain oikeiden henkilöiden saatavilla. (Hakala, Vainio & Vuorela 2009, 4.)
**Luottamuksellisuudella** tarkoitetaan, että tietojärjestelmän tiedot ovat vain niiden henkilöiden käytössä, joilla on oikeus niiden käyttöön (Hakala ym. 2009, 4).
**Eheydellä** tarkoitetaan että tieto säilyy muuttumattomana eikä sisällä tahallisia tai tahattomia virheitä (Hakala ym. 2009, 4).
**Saatavuus** tarkoittaa ominaisuutta, jossa tieto, tietojärjestelmä tai palvelu on siihen oikeututuilla käytettävissä haluttuna aikana ja vaaditulla tavalla (Valtiohallinon tietoturvasanasto 2008, 54).

Perinteistä kolmijakoista tietoturvallisuuden määritelmää pidetään nykyään riittämättömänä, koska se ei huomioi tiedon omistajan identiteetiä eikä tietojärjestelmien arvoa. Tätä Hakala, Vainola ja Vuorela (2009, 5) kutsuvat laajennetuksi tietoturvallisuuden määritelmäksi. Se sisältää perinteisen kolmijakoisen määritelmän luottamuksellisuuden, eheyden ja käytettävyyden lisäksi pääsynvalvonnan ja kiistämättömyyden. Pääsynvalvonnalla rajoitetaan tietojenkäsittely infrastrukstuurin käyttöä ja kiistämättömyydellä tarkoitetaan tietojenkäsittelyjärjestelmän kykyä tallentaa ja tunnistaa luotettavasti järjestelmänkäyttäjän tiedot ja lokitiedot. (Hakala ym. 2009, 5.)

**Pääsynvalvonnalla** tarkoitetaan tietoja, toimintoja ja menettelyitä, joiden avulla järjestelmän käyttö mahdollistetaan vain valtuutetulle käyttäjille.(Valtiohallinon tietoturvasanasto 2008 s. 78)
**Kiistämättömyydellä** tarkoitetaan sitä, että tietoverkossa lähetetty tietty viesti voidaan kiistämättömästi yhdistää lähettäjään tai, että viestin on vastaanottanut tietty henkilö. Luovutukseen ja käsittelyyn voidaan lisäksi liittää aikaleima, joka todistaa viestin saapumis ajankohdan.(Valtiohallinon tietoturvasanasto 2008, 50.)

Klassisen määritelmän mukaan **tieto** on hyvin perusteltu tosi uskomus. Perinteisesti tiedonmääritelmä jakaa tiedon käsitteen kolmeen osaan. Ensinnäkin tieto pitää pystyä perustelemaan. Esimerkiksi väite kello on kolme, jonka voi perustella tarkastamalla ajan kellosta. Toiseksi tiedon pitää olla tosi, kellon tulee siis olla kolme, jotta väittämä olisi tietoa. ja kolmanneksi tiedon kertojan tulee uskoa väittämäänsä, jottei väittämään tule ristiriitaa. (Vähämäki 2015.)

Tietoa käsitellään ja muokataan, viestintätieteissä tästä käytetään termiä tiedon arvoketju. Se tarkoittaa datan jalostumista informaatioksi, informaation jalostumista tiedoksi ja tiedon jalostumista viisaudeksi. Data tarkoitta merkkejä ja symboleja joista voidaan muodostaa informaatiota. informaatio on välitettävänä tai viestitettävänä olevaa tietoa. Se on tiedon välittäjän muokkaamaa ja tiedon vastaanottajaan vaikuttavaa tietoa. Haasion (2017) mukaan informaatio syntyy datan tulkinnasta.(Haasio & Vakkari 2017.)

Tieto ja sen synonyymi tietämys tarkoittavat ihmisen ymmärrystä itsestään ja ympäröivästä maailmasta. Tietotaito ja osaaminen syntyvät kun informaatio johtaa toimintaan. Viisaus on kyky käyttää tietämystään ja osaamistaan omassa toiminnassan. Se on kokemuksen, osaamisen ja tietotaidon summa. (Haasio & Vakkari 2017.)

**Turvallisuus** on moniselitteinen käsite, jonka määritelmästä ei vallitse yksimielisyyttä tutkijoidenkaan joukossa. Turvallisuus esimerkiksi kansainvälisessä politiikassa merkitsee eri asiaa kuin arkikäytössä. Yleisesti turvallisuus määritellään vapaudeksi uhkista. Perinteinen turvallisuuden tutkimus on keskittynyt valtioiden ja niihin kohdistuvien sotilaallisten uhkien tutkimiseen. Laaja-alainen lähestymistapa turvallisuuden tutkimukseen käsittää valtioiden lisäksi aina maailmanlaajuisesta yksilötason turvallisuuden tutkimiseen. Myös kysymys keneltä tai miltä suojaudutaan on laajennettu käsittämään sotilaallisen turvallisuuden lisäksi taloudellisen, sosiaalisen ja ympäristöllisen suojautumisen. Käsitys turvallisuudesta on kehitttynyt pitkän ajan kuluessa, joka muuttuu muuttuvan maailman mukana. (Eskola 2008,1-2.)

**Tietoturvatietoisuudella** tarkoitetaan henkilöstön tietämystä ja sitoutumista organisaation tietoturvallisuuteen. Tietoturvatietoinen henkilökunta ymmärtää tietoturvallisuuden menetyksen aiheuttamien vahinkojen merkityksen oranisaatiolle, joka sitouttaa henkilöstöä organisaation tietoturvallisuuskäytänteisiin. (NIST 1995, 144). Henkilöstöä kouluttamalla ja ajantasaisilla ohjeilla parannetaan tietoturvatietoisuutta (Käyttäjän tietoturvaohje 2003, 8). Koulutus ja kertaaminen motivoi henkilöstöä suhtautumaan tietoturvallisuuteen vakavasti eikä vain suhtautumaan tietoturvaohjeisiin haittana ja hidasteena työnteolle. (NIST 1995, 145)

## 3.2 Tietoturvakoulutus

Tietoturvakoulutuksen tavoitteena on parantaa työntekijöiden tietoturvatietoisuutta sekä muuttaa asenteita ja vääränlaisia toimintatapoja (Nykänen 2011, 20). Koulutuksen tarkoitus on saada ihmiset toimimaan siten, että organisaation tieto tulee suojattua johdon määrittämällä tavalla. Koulutuksen suunnittelun tulee perustua organisaation määrittelemään tietoturvapolitiikkaan ja siinä tulee erityisesti huomioida esimerkiksi auditoinneilla selvitetyt puutteen henkilöstön tietoturvaosaamisessa. (Laaksonen, Nevasalo, & Tomula 2006, 254.)

Henkilökunnan ei tarvitse tietää kaikkea ogranisaation tietoturvasta, riittää kun he tiedostavat oman työnsä tietoturvariskit ja niiden minimoinnin. Koulutuksessa on hyvä huomioida että, liian tekninen kouluttaminen, jossa ei perustella syitä toiminnalle johtaa helposti siihen että henkilökunta pitää tietoturvaa liian byrokraattisena työntekoa haittaavana toimintana. (Laaksonen ym. 2006, 254 – 255.) Usein tietoturvakoulutuksen päämääränä on kouluttaa organisaation tietoturvakäytänteitä ja ohjeistuksia, siksi on tärkeää huomioida, että käyttäjien tietoturvaohjeet vastaavat henkilöstön työtehtäviä. Tietoturvaohjeiden ymmärtämättömyys ja työntekijän tunne etteivät ohjeet vastaa hänen työtehtäviään, johtaa helposti ohjeiden laiminlyöntiin. (Nykänen 2011, 21.)

Tietoturvakoulutuksen pyrkimyksenä on saada työntekijä ymmärtämään oma roolinsa tietoturva käytäntöjen toteuttajana, joten koulutuksen tulisi perustua objektiivisuuteen. Objektiivinen asenne ilmenee siten, että työntekijän henkilökohtainen näkemys ja asenne eivät vaikuta päätökseen noudattaa tai olla noudattamatta tietoturvaohjeita. (Nykänen 2011, 21–22). Koulutuksen tehokkuuteen vaikuttaa myös henkilöstön motivaatio. Motivaatiota on kahdenlaista sisäistä – ja ulkoista motivaatiota. Sisäinen motivaatio tarkoittaa henkilön omaa kiinnostusta asiaan. Ulkoisella motivaatiolla tarkoitetaan esimerkiksi kilpailuviettiä, joka kannustaa oppimaan. Koulutuksessa tulee kiinnittää huomiota motivaatioon. Koulutuksen ja tietoturvan perimmäisten syiden kertominen henkilöstölle parantaa jo itsessään motivaatiota. Motivoitunut henkilöstö myös kannustaa toisiaan oppimaan. (Laaksonen ym. 2006, 255.)

Käyttämällä käytännön esimerkkejä osana koulutusta saadaan henkilöstölle avattua paremmin mitä tietoturvapolitiikalla, ohjeilla ja toimintamalleilla tavoitellaan. Jos ohjeita ei selitetä käytännön tasolla, ei tietoturva todennäköisesti tule olemaan tavoitellulla tasolla. Esimerkkien tarkoitus on luoda keskustelua eri toimintatavoista ja samalla yhtenäistää henkilöstön toimintatapoja vastaamaan tietoturvaohjeita käytännössä. (Laaksonen ym. 2006, 255.)

Laaksosen, Nevasalon ja Tomulan (2006, 257) mukaan oppiminen voidaan jakaa kahteen luokkaan: ymmärtämiseen ja harjaantumiseen. Ymmärtämisellä tarkoitetaan käsitystä, joka työntekijälle syntyy koulutuksessa kuinka eri tilanteissa tulee toimia. Harjaantuminen on kokemuksen luomaa kykyä tehdä asioita. Harjaantumista ei voi tapahtua ilman asian ymmärrystä. Säännöllisyys ja vaihtelevat menetelmät ovat tietoturvakoulutuksessa menetelmät, joilla lisätään ymmärrystä ja edistetään harjaantumista. (Laaksonen ym. 2006, 257.)

Tietoturvakoulutuksen kohderyhmänä voi olla erilaisia toimioita. Kohderyhmä voi olla koko organisaatio tai jokin pienempi osa-alue esimierkiksi organissation johto tai IT-osasto. Organisaation tulee myös kouluttaa niin sanotut kolmannet osapuolet, näitä voivat olla esimerkiksi palvelun tuottajat, jonka henkilökunta toimii organisaatiossa. (Krause & Tipton 2009, 96.)

### 3.3 Tietoturvallisuus valtionhallinnossa

Valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Valtionhallinto on ohjeistettu kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä. Valtiovarainministeriö on asettanut julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) kehittämään valtiohallinnon tietoturvallisuuden yhteistyötä ja ohjausta. Tietoturvaa ohjeistetaan VAHTI-tietoturvaohjeilla, jotka mahdollistavat määriteltyjen tietoturvavelvoitteiden saavuttamisen. (Valtiovarainministeriö 2017; Tietoturvallisuudella tuloksia, 2007, 5).

Valtioneuvoston periaatepäätösessä valtionhallinnon tietoturvallisuuden kehittämisestä edelletytetään, että kaikilla valtion organisaatiossa työskentelevillä on riittävä tietoturvaosaaminen. Riitävällä tietoturvallisuudella tarkoitetaan organisaation johdon määrittämää tasoa, joka henkilökunnan työtehtävien tietoturvallinen hoitaminen vaatii. Tietoturvallisuus on läsnä organisaation kaikessa toiminnassa, joten henkilöstön tietoturvatietoisuuteen sitouttaminen on turvallisuusden näkökulmasta avaintekijä. (Tietoturvallisudella tuloksia 2007, 52.) Tietoturvallisuudessa henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa. Henkilöstöturvallisuustyöllä,

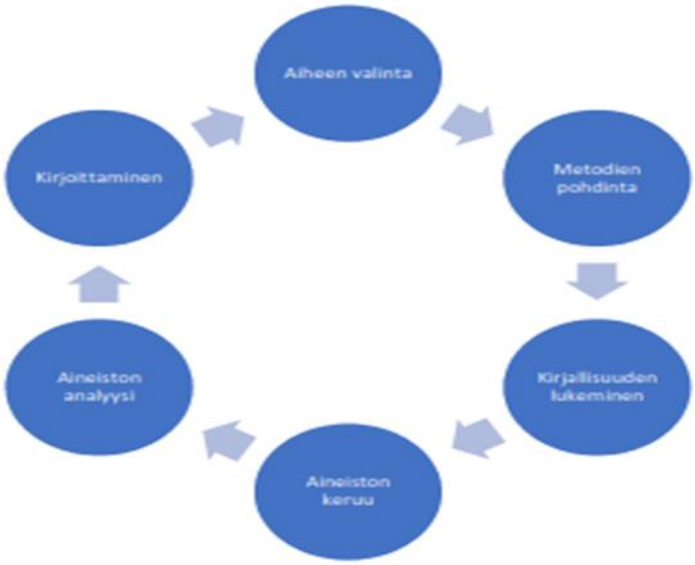
henkilöstön tietoturvatietoisuutta ylläpidetään ohjeistamalla, kouluttamalla ja työmenetelmiä kehittämällä. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008,19) Tietoturvakoulutusta tulee myös seurata ja kehittää jatkuvasti (Tietoturvallisuudella tuloksia 2007, 52).

Tietoturvakouluttajan oppaassa todetaan, (2006, 10) että tietoturvallisuudessa tärkein tekijä on ihminen. Henkilöstö on myös avainasemassa tietoturvallisuutta toteutettaessa. Organisaatioiden toimintaa hoitava henkilöstö vastaa siis pääosin sen tietoturvasta. Henkilöstö käsittelee tietoja muokkaamalla, tallentamalla ja tuhoamalla sitä.
Henkilöstöturvallisuustyöllä vähennetään henkilöstön aiheuttamaa uhkaa kouluttamalla ja ohjeistamalla. Henkilöstöturvallisuustyön yleisimpiä välineitä ovat: monitasoisten turvajärjestelmien käyttö, tietoja saa vain työtehtävän hoitamisen tarvittava vähimmäismäärä, tietojen lokerointi ja vaarallisten työuhdistelmien välttäminen. (Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta 2008,19-21.)

Organisaation vakituisen henkilöstön lisäksi tehtäviä voivat hoitaa myös esimerkiksi harjoittelijat ja palveluntoimittajat. Myös heidät on perehdytettävä organisaation tietoturvakäytänteihin (Tietoturvakouluttajan opas 2006, 11). Suurin osa tietoturvallisuuden uhista tulee organisaation sisältä. Ulkoituksessa sisäisten uhkien lähteet muuttuvat, koska ulkoistetun palvelutuottajan henkilöstöstä tulee ainakin osittain organisaation omaa henkilöstöä. Tämä muutos on otettava huomioon organisaation tietoturvakoulutusta suunniteltaessa, koska palveluntuottajan puutteellinen tietotaso ja heikko asenne tietoturvallisuuteen saattaa vaarantaa ulkoistavan organisaation tietoturvallisuuden. (Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen-hallittu prosessi 2006, 41.)
Palveluatuottavan yrityksen vastuulla on ettei viraston suojelukohteiden tai toiminan turvallisuus vaarannu sen henkilökunnan toimesta. Kuitenkaan vastuuta ei voi ulkoistaa, ulkoistavan organisaation johdon tulee varmistaa, että vaadittava tietoturvataso säilyy koko ulkoistuksen ajan. (Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen-hallittu prosessi 2006, 37.)

# 4 Tutkimusmenetelmät ja lähestymistapa

Tavoitteellinen ja suunniteltu tutkimus on vaiheistettu luova prosessi. Yleisimmin vaiheistus sisältää ainakin seuraavat vaiheet: aiheeseen perehtymisen, suunnitelman laadinnan tutkimuksen toteutuksen ja tutkimus selosteen laadinnan. Tutkimuksia on monenlaisia ja näkemyksiä vaiheistuksista on lukuisia. Yleisiä ovat esimerkiksi Tutkimuksen viisi askelta ja tutkimusspiraali. Tutkimuksen viisi askelta: 1. Valitse aihe. 2. Kerää tieto. 3. Arvio materiaali. 4. Järjestä ideat, tulokset, muistiinpanot. 5. Kirjoita artikkeli, essee, esitelmä, tutkielma (Hirsjärvi, Remes & Sajavaara 2008, 63)



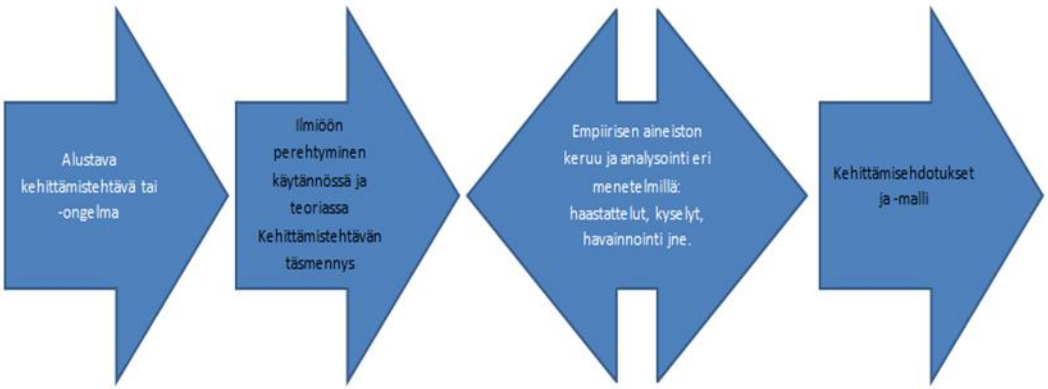

Kuvio 1: Tutkimusspiraali (Hirsjärvi ym. 2014)

Tutkimuksessa kehitettävää kohdetta voi lähestyä eri tavoin. Lähestymistavan valinta kehitystyössä vastaa tutkimusstrategian valintaa tieteellisessä tutkimuksessa. Lähestymistavaksi voidaan valita esimerkiksi tapaus- tai toimintatutkimus. Lähestymistapaa valittaessa ei vielä valita itse tutkimusmetodeja, vaikka se ohjaa kehittäjää myös niiden valinnassa. On hyvä muistaa, että lähes kaikki tutkimusmenetelmät sopivat eri lähestymistapoihin. Esimerkiksi haastatteluita ja kyselyitä käytetään lähes kaikissa lähestymistavoissa. Kehittämistöissä on tyypillistä yhdistää useampia lähestymistapoja esimerkisi toiminta- ja tapaus ja konstruktiivisia tutkimusmetodeja. (Ojasalo, Moilanen & Ritalahti. 2014, 51.)

Tapaustutkimus sopii hyvin kehittämistehtävään, jossa on tarkoituksena tuottaa kehittämisehdotuksia. Tutkittava kohde eli tapaus on esimerkiksi yritys tai sen osa. Tapaustutkimuksessa tuotetetaan tietoa nykyajassa tapahtuvasta ilmiöstä sen todellisessa toimintaympäristössä, tavoitteena on tuottaa syvällistä ja yksityiskohtaista tietoa tutkimuskohteesta. Tapaustutki-

mus vastaa usein miten ja miksi kysymyksiin, joilla pyritään tuottamaan uutta tietoa kehittämisen tueksi. (Ojasalo ym. 2014, 52-53).

Tapaututkimus alkaa tutkittavaan tapaukseen perehtymällä. Perehtyminen määrittelee mitä tapausesta voidaan kysyä. Tämän jälkeen tutustutaan kirjallisuuteen ja aiempiin tutkimuksiin, joissa tutkittu samankaltaisia ongelmia kuin omassa tutkimuksessa. Tarkan kehittämiskohteen valinta ei ole tärkeää tutkimuksen alkuvaiheessa sillä kehittämiskohde usein täydentyy tutkimuksen edetessä. Tämä on normaalia kehittämistyössä. Usein aiheeseen pitää perehtyä ennen kuin todellinen kehittämistehtävä hahmottuu. (Ojasalo ym. 2014, 54).




Kuvio 2: Tapaustutkimuksen vaiheet (Ojasalo ym. 2014)

Tapaustukimuksille on tyypillistä käyttää useita menetelmiä, joka mahdollistaa monipuolisen, syvällisena ja kokonaisvaltaisen luvauksen tutkittavasta kohteesta. Tutkimuksessa on mahdollista yhdistää niin laadullisia kuin määrällisiä menetelmiä esimerkiksi kyselyitä, joita tuetaan havannoinnilla. (Ojasalo ym. 2014, 55.)

Kehitystyössä käytettävät menetelmät on jaettu perinteisesti määrällisiin eli kvantitatiivisiin ja laadullisiin eli kvalitatiivisiin menetelmiin. Tutkimuksellisessa kehitytyössä menetelmien välinen raja hämärtyy ja metetelmät auttavat saavuttamaan parhaat uudet käytänteet. Menetelmien erot on kuitenkin syytä muistaa, jotta niitä käytetään oikein. (Ojasalo ym. 2014, 104-105.)

Kvalitatiivisen tutkimuksen lähtökohtana on todellisen elämän kuvaaminen, jossa pyritään tutkimaan kohdetta kokonaisvaltaisesti. Siinä suositaan ihmistä tiedonlähteenä, jossa tutkija luottaa enemmän omiin havainnoiteihin kuin mittausvälineisiin. Tiedonhankinnan tukena käytetään myös esimerkiksi lomakkeita täydentämään vastauksia. Kvalitatiivisessa tukimuksessa tutkimusjoukko valitaan tarkoituksen mukaisesti ei satunnaisesti ja aineiston hankinnassa huomioidaan, että tutkittavien näkökulmat pääsevät esille. Kvalitatiivisen tutkimuksen tarkoi-

tus on löytää odottomattomia seikkoja ennemmin kuin todistaa jo olemassa olevia väittämiä. (Hirsjärvi ym. 2009, 164.)

Kyselytytkimuksen eduksi on todettu seikka että sitä käytettäessä on mahdollista saada laaja tutkimusaineisto, jossa voidaan kysyä useita kysymyksiä suureltakin määrältä ihmisiä. Kysely on menetelmänä tehokas koska se säästää tutkijan aikaa ja vaivaa. Kysely voidaan lähettää suurelle määrää ihmisiä ja ainesto saadaan nopeasti analysoitua tietokoneen avulla. Tällä tavoin kerätylle tiedolle löytyy valmiiksi kehitetyt analyysi- ja raportointitavat, joten tutkijan ei tarvitse sellaisia kehitellä. (Hirsjärvi ym. 2009, 194.)

Kyselytutkimusten heikkoutena pidetään aineiston pinnallisuutta ja teoreettista vaatimattomuutta. Kyselyn tuloksista ei voida varmistaa vastaajien asennetta ja motivaatiota vastaamiseen. Vastausvaihtoehtojen osuvuus vastaajan näkökulmiin vaikuttaa möys tulosten luotettavuuteen, koska ei ole selvää miten vastaaja tulkitsee eri vastausvaihteohdot. Vastaajien tieto tutkittavasta aihealueesta saattaa myös vaihdella, joka pitää ottaa huomioon kysymyksiä suunniteltaessa. Kyselyyn vastaamattomuus eli kato nousee joissakin tapauksissa korkeaksi, jolloin kyselystä ei saada luotettavaa otantaa. (Hirsjärvi ym. 2009, 194.)

Lomakkeiden ja kysymysten suunnittelulla ja laadinnalla voidaan tehostaa tutkimuksen onnistumista, olennaista on että lomake sisältää kaikki olennaiset kysymykset tavoitteen saavuttamiseksi. Myös kyselylomakkeen ulkoasuun ja pituuteen tulee kiinnittää huomiota, liian pitkä ja sekava kysely laskee vastaamishalukkuutta. Kysymysten luomisessa tulee huomioida vastaajakunta siten, että varmasti ymmärtävät kysytyn asian oikein. Joten kysymysten on syytä olla selkeitä ja lyhyitä sekä niissä tulisi kysyä vain yhtä asiaa kerrallaan. (Ojasalo ym. 2014, 130-131.)

Asteikkoihin perustuvissa kyselyissä esitetään väittämiä, joista vastaaja valitsee vaihtoehdon, joka vastaa hänen näkemystä väitteen paikkaansa pitävyydestä. Asteikoksi sopii esimerkiksi Likertin asteikko, jossa vaihtoehdot muodostavat nousevan tai laskevan skaalan. (Hirsjärvi ym. 2009, 200.) Asteikot ovat tavallisimmin 5-portaisia ja väittämät ”täysin samaa mieltä”, ”Osin samaa mieltä”, ”ei samaa eikä eri”, ”Osin erimieltä” ja ”Täysin eri mieltä” (Vehkalahti 2014, 35.)

Vehkalahden (2014, 25) mukaan kyselytukimuksissa käytetään enimmäkseen suljettuja kysymyksiä, joissa vastausvaihtoehdot on annettu valmiiksi. Joissain tapauksissa avointen kysymysten käyttö toimii kuitenkin paremmin. Avoimissa kysymyksissä esitetään kysymys ja vastaja saa vastata vapaamuotoisesti kirjoittamalla. Avoimilla kysymyksillä voidaan esimerkiksi saada tärkeää tietoa, joka jäisi muuten havaitsematta. Se myös sallii vastaajan vastata omilla

sanoilla ja mahdollistaa vastaajan motivaation tunnistamisen. Avoimia kysymyksiä käytetään myös selventämään suljettyjen kysymysten poikkeamien tulkintaa. (Hirsjärvi ym. 2009, 201.)

Havainnointi on hyödyllinen kehitystyön tutkimusmenetelmä, sitä käytetään usein kyselyjen lisänä ja tukena. Sen avulla on mahdollista saada tietoa miten ihmiset käyttäytyvät ja toimivat luonnollisessa ympäristössä ja selvittää toimivatko ihmiset niin kuin sanovat toimivansa. Havainnointi on järjestelmällistä tarkkailua ja se täytyy suunnitella huolellisesti. Havainnoinnin tulokset kirjataan muistiin myöhempää analysointia varten. (Ojasalo ym. 2014, 114)

# 5 Tietoturvatietoisuuden tutkimus

Tässä työssä käytettiin kvalitatiivista tapaustutkimusta,joka sopii hyvin tilanteeseen, jossa pyritään ymmärtämään tutkimuskohdetta paremmin sen omassa ympäristössä sekä luomaan havaintojen perusteella kehitysedotuksia toiminnan parantamiseksi (Ojasalo ym. 2014, 105). Tämä työ koostuu kirjallisuustukimuksesta, kyselystä kohdeorganisaatiossa toimivan palvelutuottajan henkilöstölle sekä havannoinnista.

Tietoturvatietoisuuskysely oli jaoteltu kuuteen osa-alueeseen; yleinen osio, ohjeet ja koulutus, työasemien turvallisuus, tietoaineisto, viestintä sekä muut hälytykset. Yleisen osion kysymyksissä selvitettiin henkilöstön tietämystä kohdeorganisaation tietoturvaohjeista. Ohjeet ja koulutus kysymyksillä kysyttiin henkilöstön tietämystä kohdeorganisaation ohjeista sekä selvitettiin mielipidettä tietoturvakoulutuksen tilanteesta. Työasemien turvallisuus osiossa selvitettiin henkilöstön tietämystä työasemien tietoturvallisuudesta. Viestintäosiossa selvitettiin henkilöstön mielipidettä viestinnän tilasta työpaikalla. Muut hälytykset osiolla selvitettiin henkilöstön tietämystä erilaisiin ATK-hälytyksiin, joilla varmistetaan tietoteknisten laitteiden toiminta. Avoimilla kysymyksillä kysyttiin henkilöstön näkemystä suurimmista tietoturvallisuutta heikentävistä tekijöistä työpaikalla ja kuinka he kehittäisivät omaa tietoturvatietoisuuttaan. Kyselytutkimuksen tulokset on esitelty luvussa 6.1.

Kysely toteutettiin Google Sheets -laskentataulukolla, josta muokattiin kyselylomake. Kyselylomake loi vastauksista automaattisesti Excell taulukon. Laskentataulokko ohjelma muodosti vastauksista vastausjakaumat graafisena. Väittämäkysymyksissä käytettiin Likertin asteikkoa, jossa kyselyyn vastanneille kerrottiin että kyselyn tuloksista tietoa analysoidaan vastauksien yhteenvedosta massatietona, eikä niitä yksilöidä vastaajiin. Kyselyyn vastanneita kehotettiin vastaamaan kysymyksiin asteikolla 1-5. Tässä kyselyssä 5 tarkoitti ”Täysin samaa mieltä" ja 1 ”Täysin eri mieltä”. Numero 5 kehotettiin laittamaan vastaukseksi vain jos vastaaja koki tietävänsä vastauksen läpikotaisin. Muuten vastaukset kohtiin 1-4 riippuen siitä, kuinka hyvin vastaaja koki tietävänsä vastauksen. Kohtia 2-4 ei oltu määritelty sanallisesti vaan tutkija oletti että vastaus määrittyy sen mukaan, mitä lähempänä vastaajan tietämys on väittämiä ”täysin samaa mieltä” ja ”täysin eri mieltä”. Tutkimuksessa vastaukset 2-4 huomioidaan epävarmuutena väittämää kohtaan 4 kuvaa lievää epävarmuutta vastaukseen. Asteikkokysymyksiä arvioidaan myös käyttämällä vastausien mediaania, koska kyselyssä käytetään viisiportaista asteikkoa tulkitaan arvon neljä ja alle sen mediaaniarvon saadut vastaukset sellaisiksi, jotka tarvitsevat erityisesti kehittämistä.

Kysely testattiin ennen sen lähettämistä palveluntuottajan henkilöstölle. Testaukseen osallistui kohdeorganisaatoin tietoturva-asiantuntija, jonka palautteesta kyselyyn lisättiin- ja tarkennettiin kysymyksiä. Kysely lähetettiin palveluntuottajan kohde organisaatiossa työskentelevälle vakituiselle henkilöstölle. Kohteessa työskentelevät tuntityöntekijät jätetiin

pois kyselystä, koska he eivät toimi kohteessa yksin vailla palveluntuottajan vakituisen henkilöstön valvontaa. Kysely lähetettiin 15 henkilölle viestiin lisättiin saateteksti (liite 1). Vastausaikaa oli yksi viikko, kolme päivää myöhemmin palveluntuottajan henkilöstölle lähetettiin muistutusviesti kyselystä (liite2).

Havainnointia suoritettiin organisaation valvomossa 10 kertaa hutikuussa 2017. Havainnoinnista ei ilmoitettu palveluntuottajan henkilöstölle. Havainnoinnilla keskityttiin henkilöstön toimintatapoihin ja sen tarkoitus on samalla tukea kyselyn analysointia.

Havainnoinnissa tarkasteltiin seuraavia asioita:

- sisäistä viestintää
- toimintaa vuoron vaihdossa
- reagointia sähköpostiin
- reagointia hälytyksiin
- toimintaa uusien ohjeiden saapuessa (suullinen ohje virkamieheltä)
- omien laitteiden käytön seurantaa (älypuhelin, ulkoiset muistivälineet, tietokoneet)
- turvaluokiteltujen materiaalien käsittely

# 6 Tutkimustulokset

Kyselyyn vastasi yhteensä kymmenen (10) viidestätoista (15) palveluntuottajan henkilöstöön kuuluvasta työntekijästä. Vastauprosentti oli täten 66,6 prosenttia. Kyselytutkimuksessa oli yhteensä kolmekymmentäkaksi (32) kysymystä, joista neljä (4) oli avoimia kysymyksiä.

Ennen tuloksien analysointia kyselyn vastaukset tarkastettiin. Kaikki väittämiin vastanneet lomakkeet hyväksyttiin, koska jokaisessa lomakkeessa oli vastattu kaikkiin väittämiin. Avoimiin kysymyksiin oli vastattu myös jokaisessa lomakkeessa, yksi avoimiin vastauksiin vastannut oli vastannut tyhjää jokaiseen kysymykseen kirjaamalla kohtaan vain pisteen, nämä vastaukset hylättiin. Avoimiin vastauksiin vastausprosentti oli 90. Kaikkiin avoimiin kysymyksiin vastanneiden osuus oli 72,5 % kaikista kyselyyn vastanneista.

## 6.1 Kyselytutkimuksen tulokset

Tietoturvatietoisuuskyselyn kysymykset, vastaukset, keskiarvo ja mediaani esitetty taulukoissa 1 ja 2. Mediaani on joukon keskimmäinen havaintoarvo, jonka molemmin puolin on yhtä monta vastausta. Keskiarvo on lukujen summa jaettuna niiden lukumäärällä. Tutkimuksessa mediaanin alle neljä ja vastaukset joissa suurta hajontaa tulkittiin tuloksisksi, jotka tarvitsevat erityistä kehitystä jatkossa. Nämä vastaukset merkitty tummalla excelissä ja vastaukset esitetään tarkemmin kuvioissa 3-18.

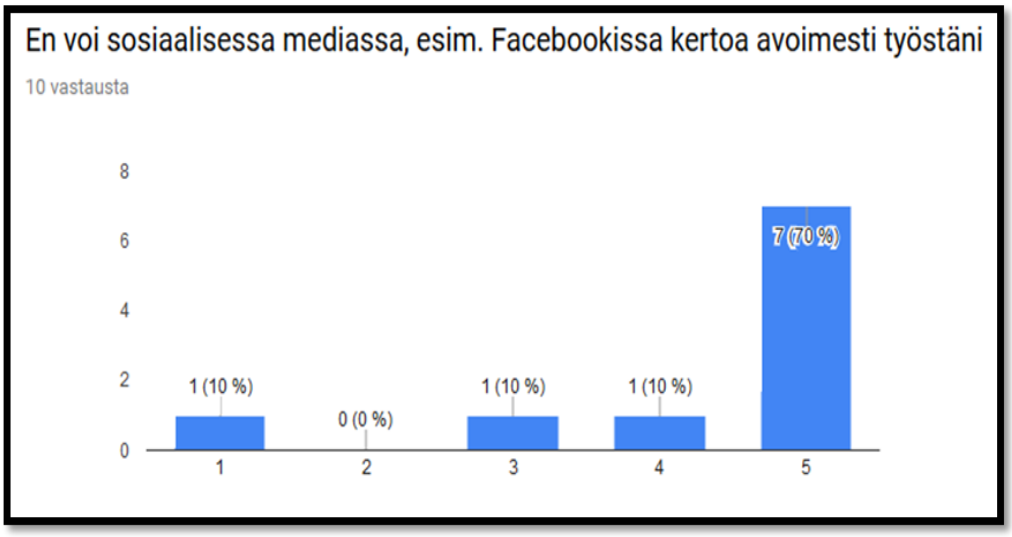
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | Myös minä olen vastuussa organisaatiomme tietoturvallisuudesta | | | 1 | 2 | 7 | 5,0 | 4,6 |
| 2 | En voi sosiaalisessa mediassa, esim. Facebookissa kertoa avoimesti työstäni | 1 | | 1 | 1 | 7 | 5,0 | 4,3 |
| 3 | Omia USB-tallennus välineitä ei saa käyttää organisaation tietokoneissa | 1 | | | 3 | 6 | 5,0 | 4,3 |
| 4 | Tiedän mitkä kaikki järjestelmät toimivat teknisessä verkossa | | 1 | 3 | 4 | 2 | 4,0 | 3,7 |
| 5 | Olen saanut tietoturvakoulutusta viimeisen x vuoden aikana? Vaihtoehdot: 1, 2, 3, 4, 5 tai yli 5 vuotta | 1 | 4 | 2 | | 3 | | |
| 6 | Koen, että olen saanut tarpeeksi koulutusta tieturva-asioista | 3 | 4 | 2 | 1 | | 2,0 | 2,1 |
| 7 | Tunnen organisaation säännöt omien laitteiden käytöstä | | 3 | 1 | 4 | 2 | 4,0 | 3,5 |
| 8 | Olen saanut riittävästi tietoturvallisuuteen liittyvää informaatiota koskien organisaatiota | 2 | 4 | 1 | 2 | 1 | 2,0 | 2,4 |
| 9 | Tiedän mistä organisaation tietoturvallisuusohjeistus löytyy | 2 | 1 | 5 | 2 | | 3,0 | 2,7 |
| 10 | Tiedän mihin ilmoittaa tietoverkkohäiriöistä | | 2 | 3 | 4 | 1 | 3,5 | 3,4 |

Taulukko 1: Kyselytutkimuksen tulokset 1-10

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 11 | Tiedän miten toimia, jos työasemaani tulee vika | | | 2 | 3 | 5 | 4,5 | 4,3 |
| 12 | Tiedän toimintatavat, jos työasemaani tulee virus/ haittaohjelma | | | 3 | 5 | 3 | 4,0 | 4,1 |
| 13 | Tiedän mitkä seikat viittaavat virus/haittaohjelman tartuntaan | | | | 6 | 4 | 4,0 | 4,4 |
| 14 | Työasemia ei saa kytkeä langattomaan vierailijaverkkoon | | 1 | 1 | 2 | 6 | 5,0 | 4,3 |
| 15 | Tunnen organisaation salasanakäytänteet | 1 | 2 | 1 | 3 | 3 | 4,0 | 3,5 |
| 16 | Tiedän miten toimia epäilyttävien sähköpostien | | | | 2 | 8 | 5,0 | 4,8 |
| 17 | Tiedän miten hävitän paperitulosteeni | | | | 1 | 9 | 5,0 | 4,9 |
| 18 | Tunnen organisaation tietoaineistojen luokittelun | 1 | | 1 | 7 | 1 | 4,0 | 3,7 |
| 19 | Tunnen salassa pidettävän tietoaineiston elinkaaren eri vaiheet | 1 | 4 | 2 | 1 | 2 | 2,5 | 2,9 |
| 20 | Tunnen organisaation tietojenluovutus käytännöt | 1 | 1 | 1 | 3 | 4 | 4,0 | 3,8 |
| 21 | Työpaikallani tiedonkulku tietoturvallisuusasioissa toimii hyvin | 3 | 2 | 4 | | 1 | 2,5 | 2,4 |
| 22 | Koen, että saan tietoa organisaation muuttuneista tietoturvakäytännöistä ja -ohjeista | 3 | 2 | 5 | | | 2,5 | 2,2 |
| 23 | Tiedän miten toimia, jos turvahuoneista tulee hälytys | | 2 | 3 | 3 | 2 | 3,5 | 3,5 |
| 24 | Tiedän miten toimia ATK-lämpöhälytyksissä | | | | 2 | 8 | 5,0 | 4,8 |
| 25 | Tiedän miten toimia UPS-hälytyksissä | | 1 | 1 | 1 | 7 | 5,0 | 4,4 |
| | | Kyllä | | | Ei | | | |
| 26 | Tiedän ketkä kuuluvat organisaation tietoturvallisuushenkilöstöön | 5 | | | 5 | | | |
| 27 | Tiedän mistä tarkastaa onko henkilö turvaselvitetty | 10 | | | 0 | | | |
| 28 | Tiedän miten lähetän salatun sähköpostin | 8 | | | 2 | | | |

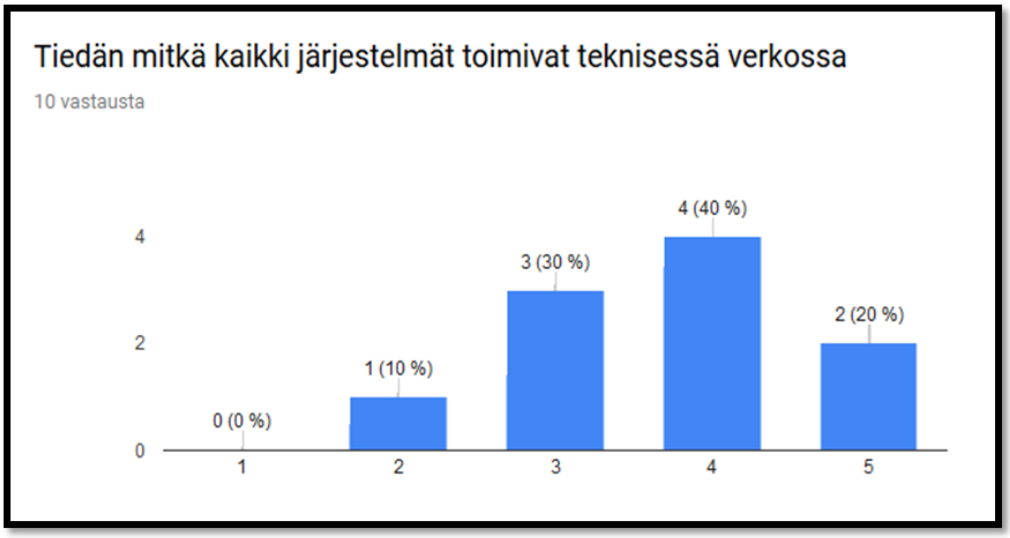
Taulukko 2: Kyselytutkimuksen tulokset 11-28

Kysymyksessä koskien oman työn kertomisesta sosiaalisessa mediassa yksi (1) vastaajista oli sitä mieltä, että hän voi kertoa siitä avoimesti kun taas seitsemän(7) vastaajista oli täysin samaa mieltä siitä, että työstä ei voi kertoa. Yksi (1) vastaajista vastasi numero 3 ja yksi(1) numero 4.



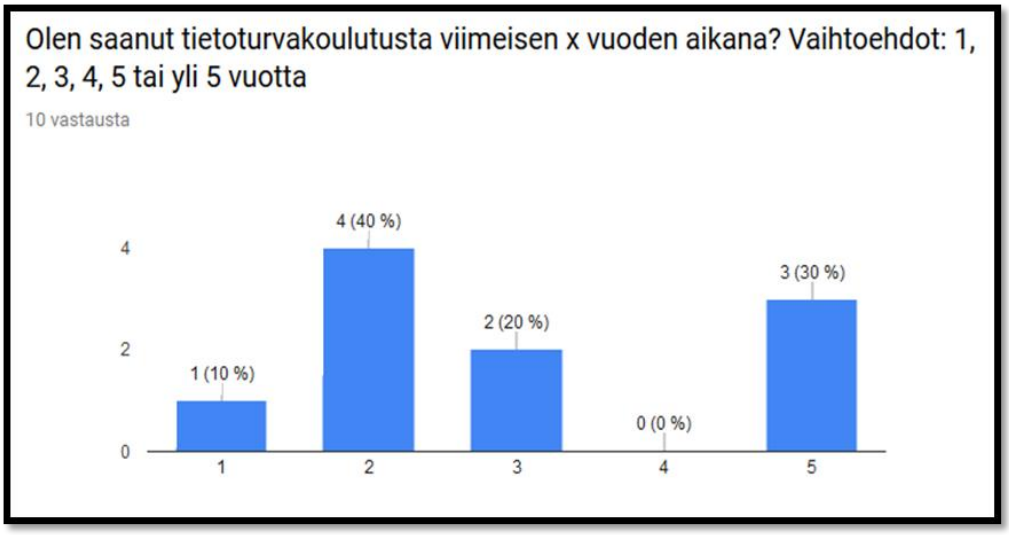

Kuvio 3: Väittämä ” En voi sosiaalisessa mediassa, esim. Facebookissa kertoa avoimesti työstäni”

Väittämässä kysytään, tietääkö vastaaja mitkä kaikki laitteet kuuluvat tekniseen verkkoon. Vastaajista kaksi (2) vastasi viisi (5) eli tiesivät varmuudella mitkä laitteet ovat teknisessä verkossa, neljä vastaajaa (4) vastasi 4, eli eivät olleet täysin varmoja mitkä laitteet teknisessä verkossa. Kolme vastaaja vastasi 3, eli kokivat tietävänsä osan laitteista mutta kokivat kohtalaista epävarmuutta tiedosta. Yksi vastaaja (1) vastasi 2, eli koki suurta epävarmuutta tiedosta.



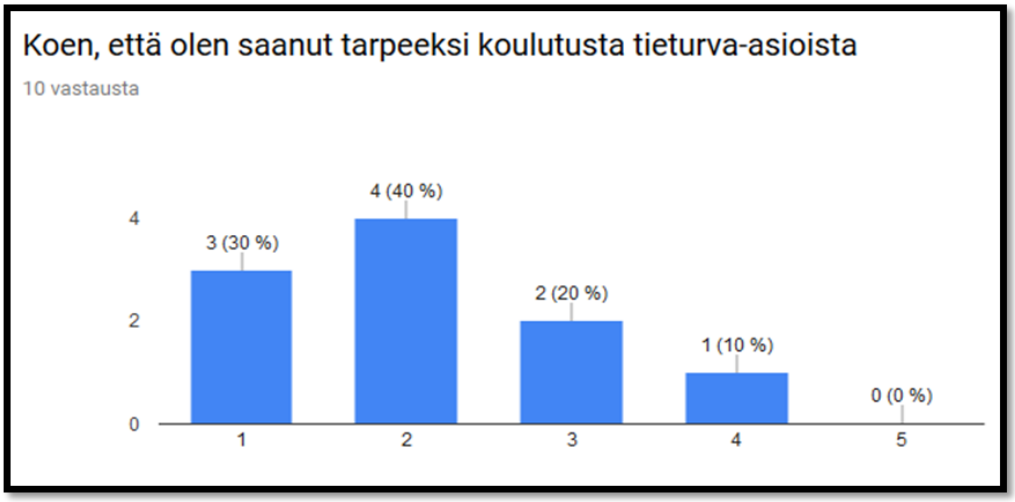

Kuvio 4: Väittämä "Tiedän mitkä kaikki järjestelmät toimivat teknisessä verkossa"

Kysymyksessä tiedustellaan kauanko on kulunut edellisestä tietoturvakoulutuksesta. Yksi (1) vastaaja on saanut tietoturvakoulutusta viimeisen vuoden aikana. Neljä (4) vastaajaa on saanut koulutusta viimeisen kahden vuoden aikana. Kaksi vastaajaa on saanut koulutusta kolmen vuoden aikana. Kaksi (2) vastaajaa ei ole saanut koulutusta viiteen vuoteen tai yli.



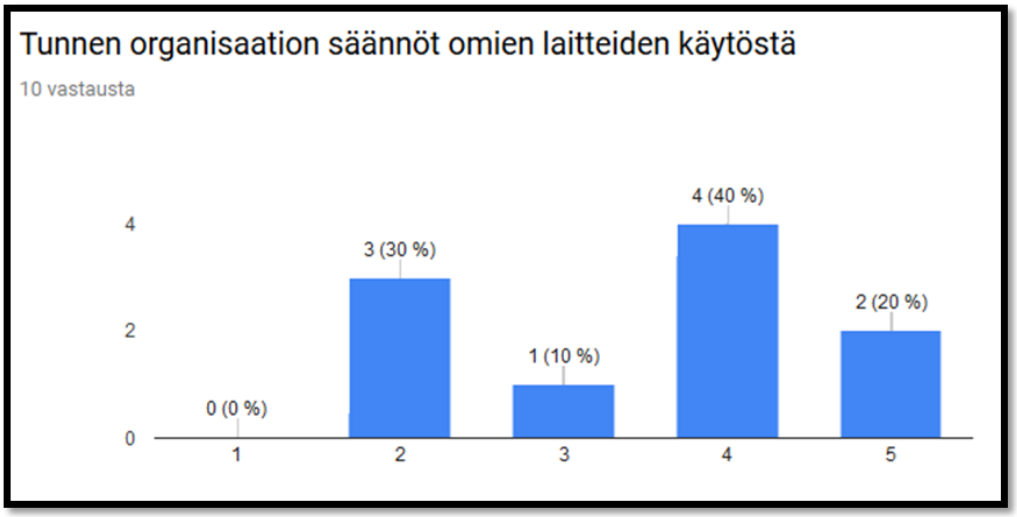

Kuvio 5: Kysymys edellisen tietoturvakoulutuksen ajankohdasta

Kysymyksessä tiedustellaan onko vastaaja saanut mielestään tarpeeksi koulutusta tietoturva-asioista. Kolme vastasi yksi (1) Neljä vastasi kaksi (2) Kaksi vastasi (3) ja yksi vastasi neljä(4). Seitsämän kymmenestä vastaajasta koki, ettei ole saanut tarpeeksi koulutusta tietoturva asioista. Kaksi vastaajaa valitsi vaihtehdon kolme (3), eli kokivat että ovat saaneet kohtalaisesti koulutusta tietoturvasta. Yksi vastaaja vastasi neljä (4), eli koki saaneensa lähes tarpeeksi tietoturvakoulutusta.



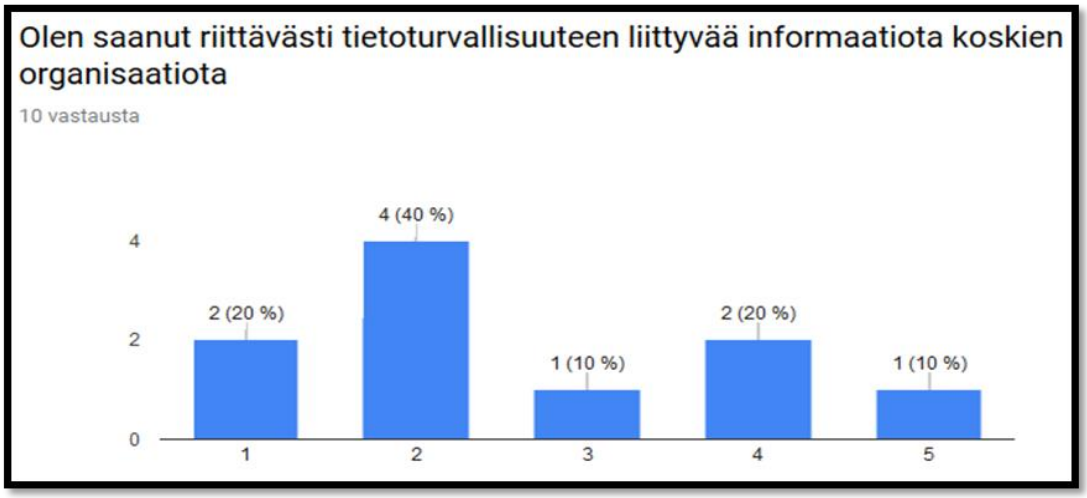

Kuvio 6: Väittämä: ”Koen, että olen saanut tarpeeksi koulutusta tietoturva-asioista”

Väittämässä selvitetään vastaajan tietämystä organisaation säännöistä omien laitteiden käytöstä. Vastaajista kaksi (2) vastasi ”täysin samaa mieltä” Neljä (4) vastasi neljä, eli kokivat lievää epävarmuutta säännöstä. Yksi (1) vastasi kolme, eli koki kohtalaista epävarmuutta säännöstä. Kolme (3) vastasi kaksi, eli kokivat kohtalaisen suurta epävarmuutta säännöstä.



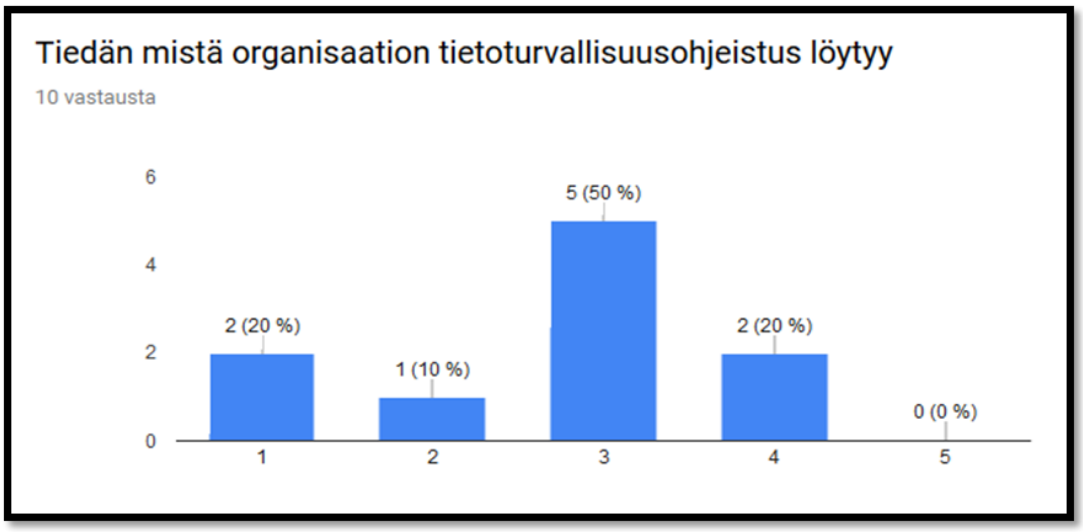

Kuvio 7: Väittämä ”tunnen organisaation säännöt omien laitteiden käytöstä”

Väittämässä kysytään, onko vastaaja saanut mielestään tarpeeksi informaatiota organisaation tietoturva-asioista. Yksi (1) vastasi viisi ”Täysin samaa mieltä” Kaksi (2) vastasi 4 ja Yksi (1) vastasi kolme. Vastaajista neljä (4) vastasi kaksi ja kaksi(2) vastasi 1. Vastauksissa oli suuri hajautuma, kolme vastaajista koki saaneensa tarpeeksi tai lähes tarpeeksi tietoa organisaation tietoturva asioista. Yksi oli neutraali ja kuusi vastaajaa koki ettei ole saanut tarpeeksi tai lähes tarpeeksi tietoa organisaation tietoturva-asioista.



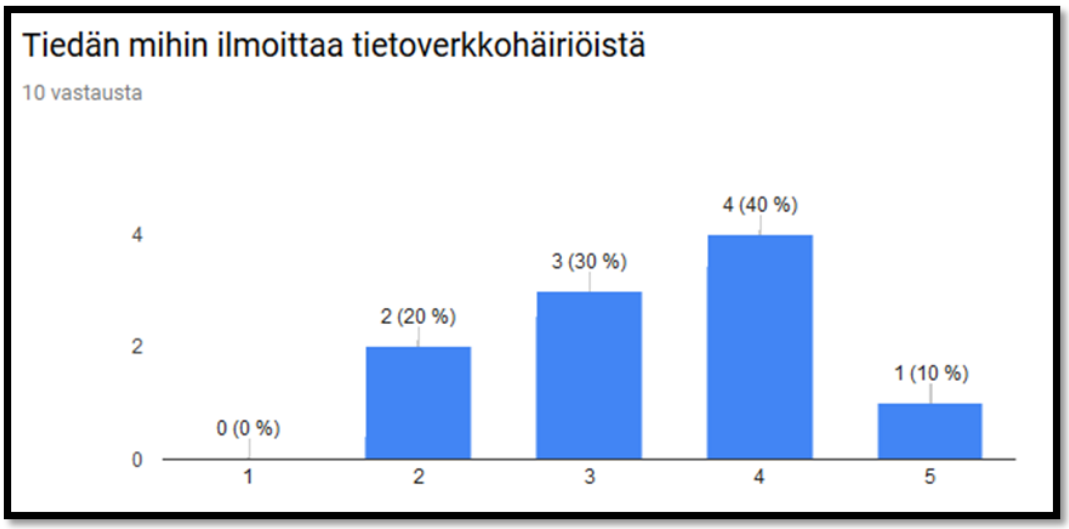

Kuvio 8: Väittämä ”Olen saanut riittävästi tietoturvallisuuteen liittyvää informaatiota koskien organisaatiota”

Kysymyksessä tiedustellaan, tietääkö vastaaja mistä organisaation tietoturvaohjeistus löytyy. Kaksi (2) vastaaja vastasi 4. Viisi vastasi (5) kolme. Yksi (1) vastasi kaksi ja kaksi (2) vastasi 1 ”täysin eri mieltä”.



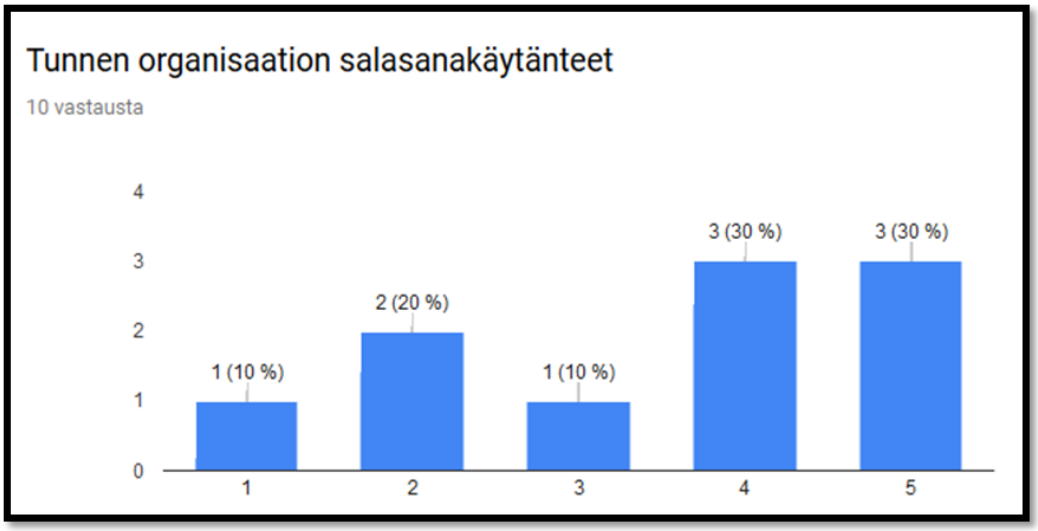

Kuvio 9: Väittämä ”Tiedän mistä organisaation tietoturvallisuusohjeistus löytyy”

Kysymyksessä tiedustellaan tietääkö vastaaja mihin ilmoittaa, jos havaitsee tietoverkkohäiriön. Yksi (1) vastasi 5 ”täysin samaa mieltä. Neljä (4) vastasi 4. Kolme vastasi (3) ja kaksi vastasi 2. Viisi (5) vastaajaa valitsi vaihtoehdot 5 tai 4, eli tiesivät täysin tai melkein varmasti minne ilmoitetaan. Kolme (3) vastajaa valitsi vaihtoehdon kolme, eli olivat jokseenkin epävarmoja minne ilmoitus tehdään. Kaksi (2) vastaajaa valitsi 2, eli olivat epätietoisia minne imoitus tulee tehdä.



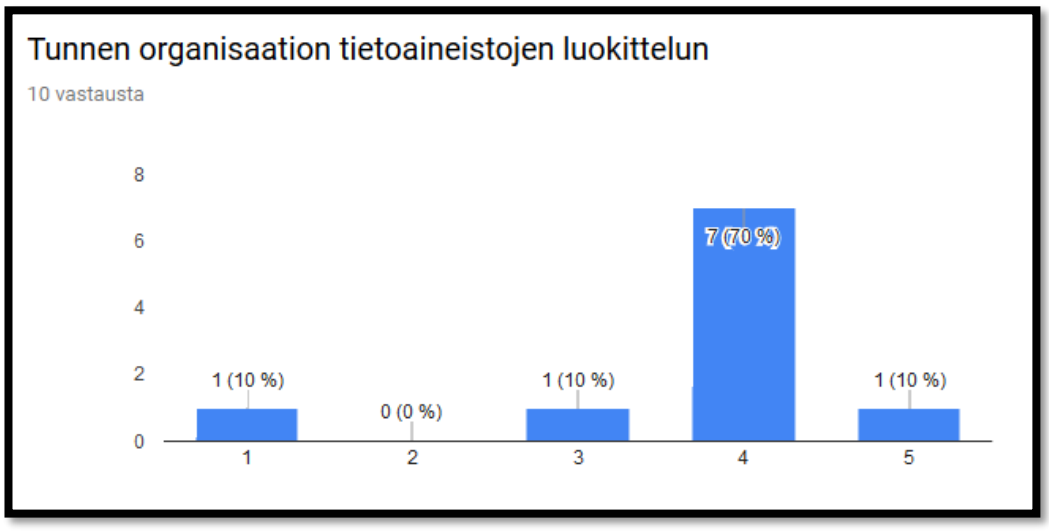

Kuvio 10: Väittämä ”Tiedän mihin ilmoittaa tietoverkkohäiriöistä”

Väittämässä kysytään tunteeko vastaaja organisaation salasanakäytänteet. Kolme vastaajaa vastasi 5 ”Täysin samaa mieltä”, kolme (3) vastasi 4. Yksi (1)vastasi kohtaan 3 ja kohtaan 2 vastasi kaksi (2) vastaajaa. Täysin eri mieltä oli yksi (1) vastaaja.



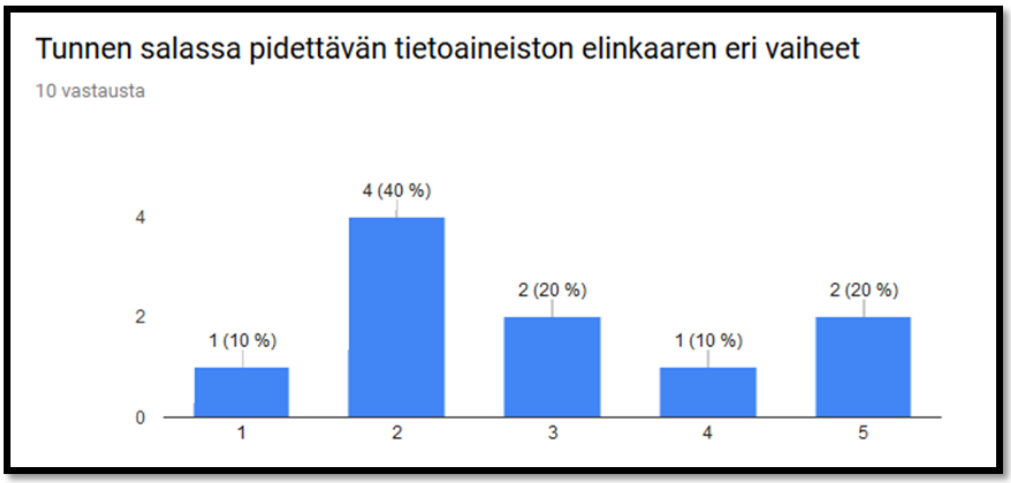

Kuvio 11: Väittämä ”Tunnen organisaation salasanakäytänteet”

Väittämässä kysytään tunteeko vastaaja organisaation tietoaineiston luokittelun. Vastaajista yksi (1) vastasi viisi ”täysin samaa mieltä”, seitsämän (7) vastasi 4. Yksi (1) vastasi kolme ja yksi (1) vastasi 1 ”täysin eri mieltä”



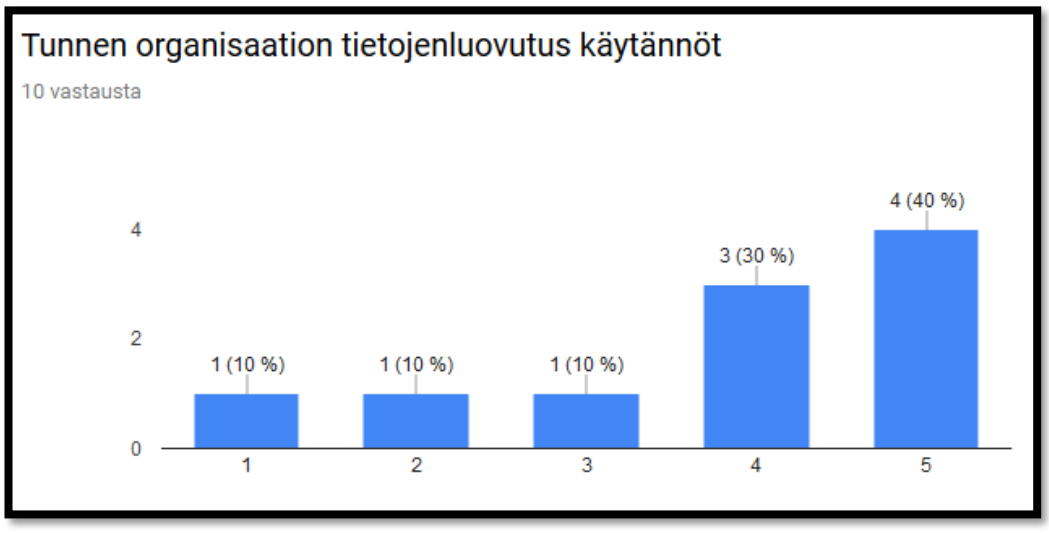

Kuvio 12: Väittämä ”Tunnen organisaation tietoaineiston luokittelun”

Väittämässä kysytään tietääkö vastaaja salassa pidettävän tietoaineiston elinkaaren eri vaiheet. Kaksi (2) vastasi 5 ”täysin samaa mieltä”, yksi (1) vastasi 4 ja kaksi (2) vastasi kolme. Neljä (4) vastaajaa valitsi vaihtoehdon kaksi ja yksi(1) vastaaja valitsi 1 ”täysin eri mieltä”



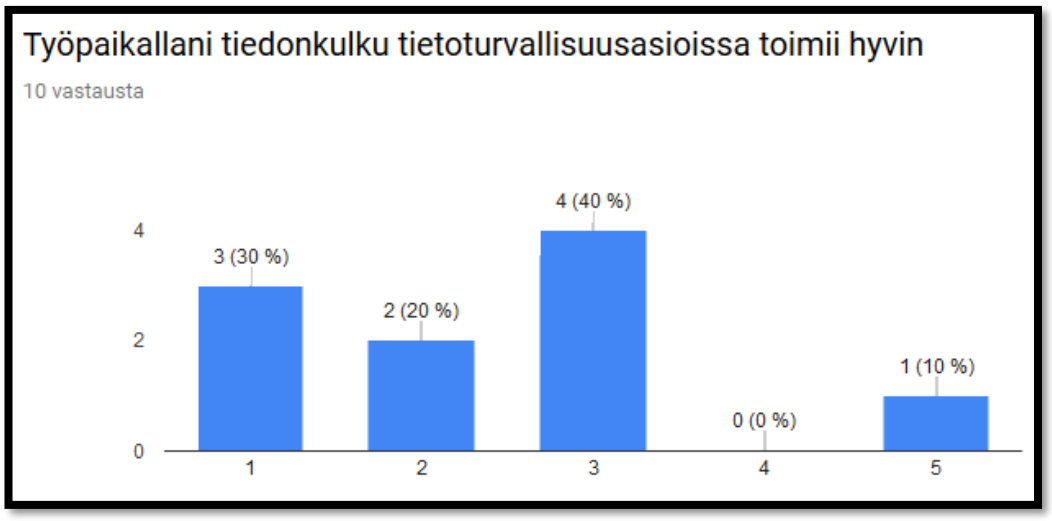

Kuvio 13: Väittämä ”tunnen salassa pidettävän tietoaineiston elinkaaren eri vaiheet”

Väittämässä kysytään tunteeko vastaaja organisaation tietojenluovutus käytänteet. Vastaajista neljä (4) vastasi 5 ”täysin samaa mieltä”, kolme (3) vastasi 4. Kohtiin yksi, kaksi ja kolme vastasi kuhunkin yksi vastaaja(1).



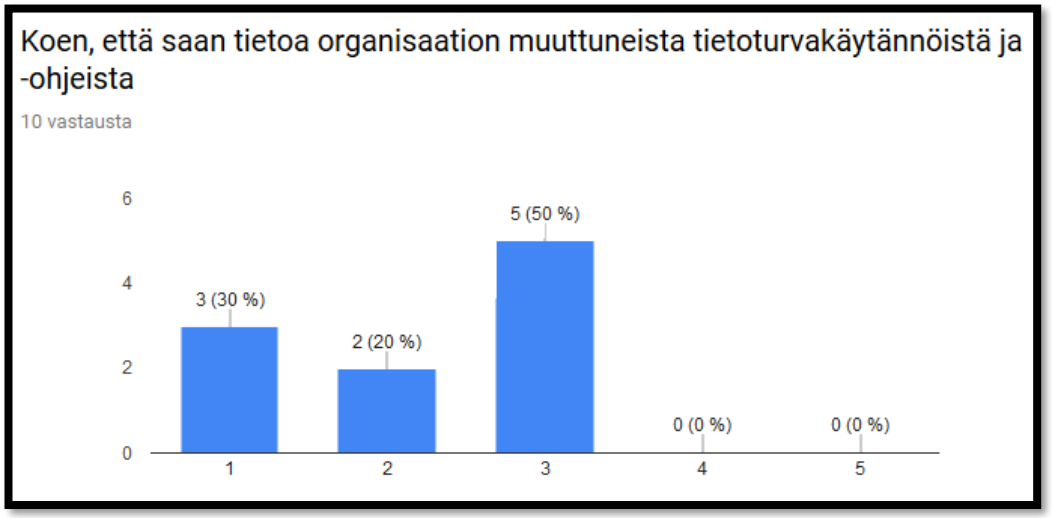

Kuvio 14: Väittämä ”tunnen organisaation tietojenluovutuskäytännöt”

Väittämässä kysytään toimiiko työpaikalla tiedonkulku tietoturvallisuusasioissa hyvin. Vastaajista yksi (1) vastasi 5 ”täysin samaa mieltä”. Neljä vastasi 3, kaksi (2) vastasi kaksi ja kolme (3) vastasi 1 ”täysin eri mieltä”.



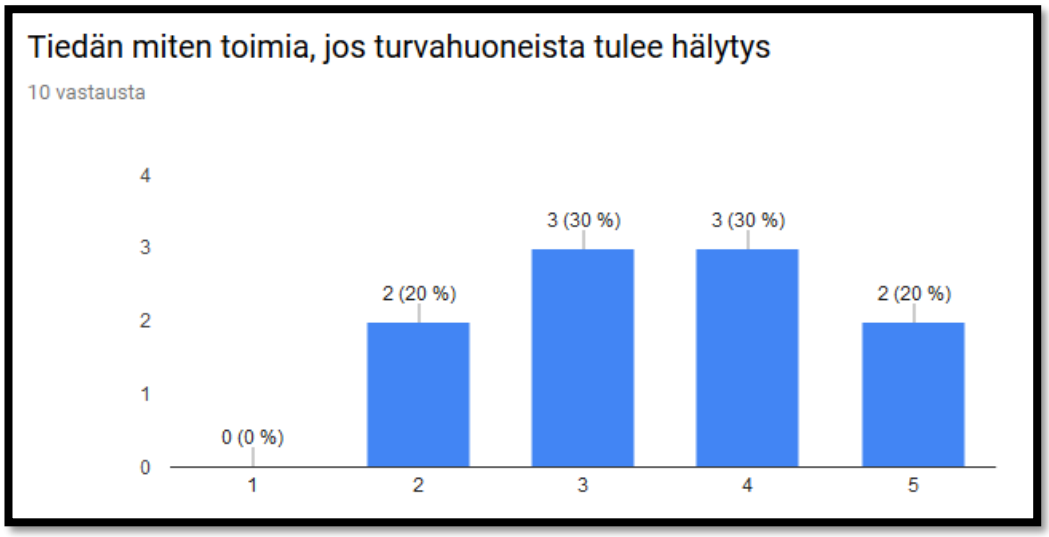

Kuvio 15: Väittämä ”työpaikallani tiedonkulku tietoturvallisuusasioissa toimii hyvin”

Väittämässä kysytään kokeeko vastaaja saavansa tietoa, jos tietoturvakäytänteet tai -ohjeet muuttuvat. Vastaajista viisi (5) vastasi kolme, kaksi (2) vastasi kaksi ja kolme (3) vastasi 1 ”täysin eri mieltä”.



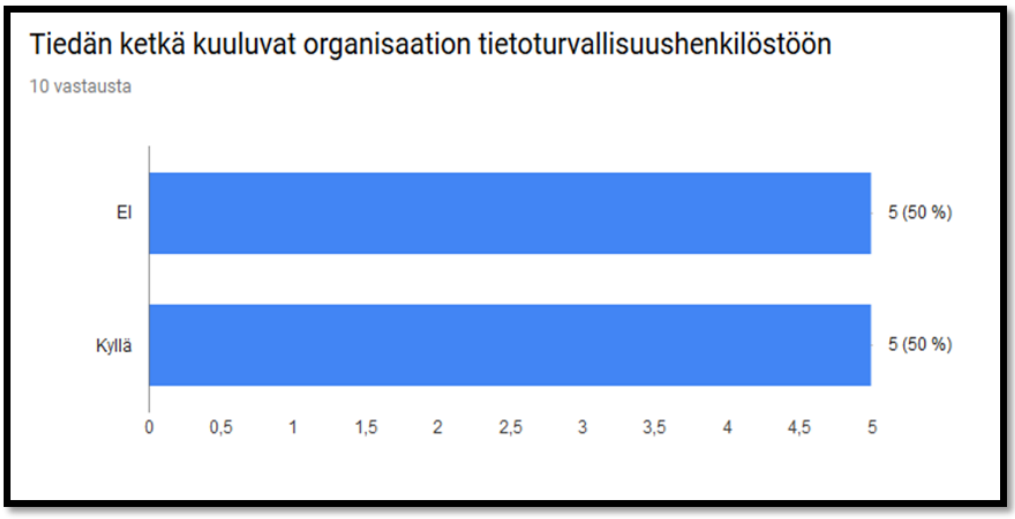

Kuvio 16: Väittämä ”koen , että saan tietoa organisaation muuttuneista tietoturvakäytänteistä ja – ohjeista”

Väittämässä kysytään tietääkö vastaaja, kuinka toimia turvahuoneista tulevissa hälytyksissä. Kaksi (2) vastaajaa vastasi 5 ”täysin samaa mieltä, kolme vastasi (3) 4. Kolme (3) vastaajaa valitsi vaihtoehdon 3 ja kaksi (2) vastaajaa vastasi 2.




Kuvio 17: Väittämä ”tiedän miten toimia, jos turvahuoneista tulee hälytys”

Kysymyksessä kysyttiin, tietääkö vastaaja ketkä kuuluvat organisaation tietoturvahenkilöstöön. Vastaajista puolet (5) kertoivat tietävänsä ja puolet(5) vastasivat etteivät tiedä.




Kuvio 18: Väittämä "Tiedän ketkä kuuluvat organisaation tietoturvallisuushenkilöstöön"

## 6.2 Kyselytutkimuksen avoimet kysymykset

Kysymyksessä koskien työpaikan suurimpia tietoturvaongelmia kävi ilmi, että henkilöstöllä ei ole yhteistä mielipidettä siitä, mitkä olisivat suurimipia ongelmia. Muutamassa vastauksessa todettiin, että tietoturvaongelmat johtuivat henkilöstöstä. Kysymykseen vastasi kymmenen (10) vastaajaa, joista yksi (1) hylättiin tyhjänä, vastaaja oli vastannut pisteellä.

”Välinpitämättömyys ja liian kaaottinen kokonaisuus”

”Käyttäjät ovat aaseja”

Yksi tekijä, joka edisti työpaikan tietoturvongelmia koettiin olevan organisaation koulutuksen puute.

” Minulle ei ole kerrottu tietoturva-asioista oikeastaan ollenkaan koko urani (12v.) aikana”

” Ei tiedotusta tai jatkuvaa koulutusta. Palveluntuottajia ei kouluteta organisaation kautta ollenkaan. Tietoturvallisuuden johtaminen ja implementointi on hyvin heikkoa”

Kysymyksessä ”miten parantaisit tietoturvatietämystä työpaikallasi” nousi esiin kaksi teemaa; tietoturvakoulutus ja ajantasaiset ohjeet. Kysymykseen vastasi seitsemän (7) vastaajaa, joista yksi (1) hylättiin tyhjänä.

”Kouluttamalla ja tekemällä tiedotuksesta tavan.”

” Perehdyttämällä, ajantasaisilla tiedotuksilla/ohjeilla”

” *Kouluttamalla väkeä, ajamalla päähän että tietoturvallisuus on kaikkien asia, rakentamalla kunnolliset ohjeet, seuraamalla että niitä seurataan ja poistamalla poikkeukset sekä ristiriidat*.”

Kysymyksessä ” Mistä tietoturvallisuuteen liittyvistä asioista kaipaisit koulutusta?” havaittiin että yleinen tietoturvallisuuden kertauskoulutus oli suurin kaivattu koulutus, joka mainittiin viidessä yhdeksästä vastauksessa. Yksi vastaus hylättiin tyhjänä.

”*Sellanen snadi kertauskoulutus vois olla jees*”

”*Kaikesta yleisesti. Säännöllisesti*.”

Myös kohdeorganisaation tietoturvakäytänteistä toivottiin koulutusta.

”*Yleisistä organisaation käytännöistä*”

”*Tämän hetken uhkista ja mahdollisesti muuttuneista ohjeistuksista*”

Kysymykseen ”Millä keinoin mielestäsi omaa tietoturvallisuustietoisuuttasi voitaisiin parantaa?” vastasi 6 vastaajaa, joista neljä hyväksyttiin. Yksi vastaaja vastasi tyhjää ja toinen kommentoi vastaustilannetta. Kolme vastaajaa kertoi koulutuksen olevan olevan keino parantaa omaa tietoturvatietoisuutta.

”*Kouluttamalla ja informoimalla*”

”*Säännölliset koulutukset/kertaukset*”

Kolmessa vastauksessa mainittiin keinoksi parantaa omaa tietoturvatietoisuutta perehdyttäminen ja organisaation tunteminen.

”*Kokonaisuuden hahmottamisella ja koulutuksella*”

”*Perehdyttämällä*”

### 6.3 Havainnoinnin tulokset

Havainnoinin tuloksissa ei vastata kaikkiin havainoinnissa perehdyttyihin aiheisiin, vaan luodaan kokonaiskuva havainnoinnin tuloksista. Havainnointi suoritettiin normaalien työvuorojen aikana, eikä siitä infomoitu havainnoinnin kohteita. Havainnoinnin tulokset kirjattiin välittömästi muistiin.

Vuoronvaihtojen yhteydessä henkilöstö käy läpi päivän tapahtumia suullisesti vuoroon tulevan henkilöstön kanssa ja työvuoron aloittava henkilöstö myös lukee läpi päivän työvuororaportin. Työvuororaportit kirjoitetaan Word-tiedostoon, joka kattaa yhden vuorokauden tapahtumat. Valvomon toiminta on käynnissä ympäri vuorokauden vuoden jokaisena päivänä, joka aiheuttaa tilanteen, jossa henkilöstöllä voi olla useiden päivien mittaisia vapaa jaksoja. Vaikka vuoroon tuleva henkilöstö saapui vuoroon useamman päivän tauolta ei se muuttanut vuoron vaihdon toimintaa. Henkilöstö luki vain edeltävän vuoron raportin. Täten vuoroon saapuvalla hen-

kilöstöllä saattaa olla puutteita edellisten vuorokausien tapahtumista. Havainnoinnin aikana havaittiin kahden (2) henkilön lukevan vanhempia kuin edellisen vuorokauden raportit.

Havainnoinnin aikana valvomoon tuli yksi kirjallinen ja yksi suullinen toimintaohje, suulliset toimintaohjeet ovat tilapäisohjeita jotka ovat voimassa vain lyhyen ajan. Kirjallinen ohje lisättiin kohteen sisäisten toimintaohjeiden kansioon. Ohjeen saapumista ei kirjattu työvuororaporttiin, eikä siitä tehty tiedotetta valvomon henkilökunnalle. Suullisesta toimintaohjeesta kirjattiin päivittäistiedote, joka lisättiin muiden tilapäisten toimintaohjeiden joukkoon kirjoitusalustalle.

Havainnoinnin aikana organisaation tiloihin pyrki useita huolto- ja korjaus yms. henkilöitä, joilla tulee olla henkilöturvaselvitys tehtynä hyväksytysti tiloihin päästäkseen. Kolmessa tapauksessa henkilöä ei löytynyt valvomoon toimitetulta listalta. Virkamiesten selvittelyn kautta, kaikissa kolmessa tapauksessa löytyi turvaselvitys ja henkilöt pääsivät kohteeseen töihin.

Omien laitteiden käyttöä havaittu päivittäin älypuhelinten merkeissä. Muita laitteita käytössä muun muassa tablettja ja kannettavia tietokoneita, näiden käyttötarkoitus oli havaintojen perusteella hiljaisten ajankohtien viihdekäyttöä. Ei havaintoja ulkoisten muistien yms. käytöstä kohteessa.

# 7 Tutkimustulosten analysointi

Tutkimuskohteen henkilökunta on turvallisuusalan ammattilaisia, joka vaikuttaa myös tietoturvallisuuden osaamiseen. Palveluntuottajan tuottama palvelu on luokiteltu vaativaksi kohteeksi, jossa yksin toimiminen vaatii, että henkilö on työskennellyt kohteessa kokeneemman kollegan valvonnassa vähintään yhden vuoden ajan. Tänä aikana uudelle työntekijälle ehtii siirtymään myös paljon, niin kutsuttua hiljaistatietoa kohdeorganisaatiosta ja sen toimintatavoista.

Tutkimustuloksista kävi ilmi että tietoturvallisuuden perustaso oli hyvä, mutta tiedoissa organisaation tietoturvaohjeista ja käytännöissä oli puutteita. Tietoturvallisuuden toimintatapojen tuntemukseen liittyvissä kysymyksissä vastauksien mediaani oli korkea. Puutteet puolestaan ilmenivät siten, että väittämissä joissa käsiteltiin aiheita, jotka liityivät organisaation tietoturvaohjeiden ja -käytänteiden tuntemukseen, oli suurin vastausjakauma. Myös mediaanilla tarkasteltuna organisaation tietoturvaohjeiden ja -käytänteitä käsittelevät väittämät saivat usein arvon neljä tai alle. Kyselytutkimuksen avointen vastauksien osiossa henkilöstö mainitsi perehdytyksen ja ohjeet seitsemän kertaa kysymyksissä, joissa kysyttiin henkilöstön mielipidettä siitä, mitkä ovat tärkeimpiä kehityskohteita koskien tietoturvallisuutta.

Kirjallisuusaineistosta havaittiin että tietoturvatietoisuudessa koulutus on tärkessä roolissa. Varsinkin kyselyn avoimien vastauksien osiossa henkilöstön mielestä koulutus olisi tärkein keino parantaa omaa ja koko henkilöstön tietoturvatietoisuutta. Koulutus mainittiin, tai oikeammin jatkuvan koulutuksen puute mainittiin myös työpaikan suurimpana tietoturvallisuutta uhkaavana tekijänä.

Tutkimuksessa havaittiin, että viestinnässä on henkilöstön mielestä parannettavaa. Palveluntuottajan sisäinen viestintä sekä palveluntuottajan ja kohdeorganisaation välinen viestintä tietoturvallisuus asioissa koettiin rittämättömäksi. Vastaajat kokivat, että palveluntuottajan sisäinen tiedonkulku tietoturvallisuusasioissa on korkeintaan välttävää. Henkilöstö koki myös että kohdeorganisaatiolta ei viestitä palveluntuottajaa muuttuneista tietoturvaohjeista ja käytänteistä. Kysyttäessä ”miten parantaisit tietoturvallisuutta työpaikallasi” kolme vastaajaa mainitsi viestinnän ja tiedotuksen parhaaksi tavaksi parantaa työpaikan tietoturvaa.

# 8 Kehitysehdotuksia

Opinnätetyön tavoitteena oli tutkia palveluntuottajan tietoturvatietoisuuden tasoa ja pohtia parannusehdoituksia tutkimustuloksien perusteella.Tutkimustuloksista havaittiin että suurimmat puutteet palveluntuottajan tietoturvallisuustietoisuuden nykytilassa liittyvät säännöllisen koulutuksen puutteeseen, organisaation tietoturvaohjeiden ja käytänteiden tuntemukseen sekä viestintään. Tässä luvussa pohditaan keinoja parantaa näitä kolmea osa-aluetta.

Palveluntuottaja on sitoutunut kouluttamaan henkilöstöään viisi työpäivää vuodessa, eli 40 tuntia kalenterivuoden aikana. Osa koulutustunneista menee lakisääteisiin koulutuksiin ja osa organisaation erityspiirteistä johtuviin pakollisiin koulutuksiin. Pakollisten koulutusten jälkeen jää vuodessa noin 2 työpäivää palveluntuottajan valitsemiin koulutuksiin. Näistä jäljelle jäävistä koulutuspäivistä suosittelisin organisaatiota vaatimaan palvelun tuottajaa suuntaamaan ainakin osan kohti tietoturvakoulutusta.

Säännöllisellä koulutuksella saadaan henkilöstön tieturvallisuustietoisuuden taso vastaamaan valtioneuvoston periaatepäätöstä, jossa kaikilla työntekijöillä on riittävä tietoturvatietämys tehtävien hoitoon. Säännöllistä koulutusta tulee myös kehittää ja arvioida ettei siitä muodostu itseään toistavaa. Tutkimuksessa havaittiin, että useissa vastauksissa oli suurta hajontaa, joka kertoo henkilöstön tietoturvatietämyksen suurista eroista. Koulutus tulisi siis aloittaa tietoturvallisuuden perusteista, jotta koko henkilöstön perustietämys saataisiin lähemmäksi samaa tasoa.

Tietoturvallisuden peruskoulutus voidaan toteuttaa luentotyylisesti, mutta myöhemmissä koulutuksissa voisi käyttää myös verkko-opetusta, tietoiskuja ja tarinankerrontamenetelmää, missä kerrotaan tarinoiden avulla miten tietoturvallisuus on menetetty ja pohditaan yhdessa miten kyseistä uhkaa voidaan torjua. Tarinan kerrontaa voi suorittaa hyvinkin yksinkertaisesti, esimerkiksi omista tietoturvallisuuden opinnoista yksi parhaiten mieleen jääneistä tavoista oppia oli tietoturvatestaajan kertomukset, kuinka organisaatioihin on päästy tunkeutumaan sisälle ja aiheutettu kohteelle tietoturvan menetys. Kertomuksien herättämät mielikuvat herättävät pohtimaan omia työtapoja, joilla edesauttaa tietoturvallista toimintaa. Kun koulutusta on annettu tietoturvatietämyksen tasoa olisi hyvä myös testata, esimerkiksi järjestämällä koetyyppinen verkkokysely, jolla selvitetään henkilöstön tietoturvaosaamisen taso.

Koulutuksen lisäksi tutkimuksessa ilmeni palveluntuottajan epätietoisuus kohdeorganisaation tietoturvallisuus ohjeisiin. Kohdeorganisaation sisäiset tietoturvaohjeistukset sijaisevat, järjestelmässä, johon palveluntuottajalla on rajoitettu käyttöoikeus. Tästä johtuen järjestelmästä ei saa ladattua dokumentteja palveluntuottajan järjestelmään myönnetyillä käyttö-

oikeuksilla. Tähän ongelmaan nykytilassa näkisin ratkaisuna organisaation tietoturva-asiantuntijan järjestämän perehdytyskoulutuksen palveluntuottajan henkilökunnalle. Haastavaksi perehdytyksen järjestämisen tekee palveluntuottajan tarjoaman palvelun luonne, jonka vuoksi koulutuksia olisi järjestettävä useita. Myös henkilöstön vaihtuvuus aiheuttaa tarvetta satunnaisiin koulutuksiin. Pitkän ajan ratkaisuna tehokkainta olisi löytää malli, jossa perehdytys organisaation tieturvasääntöihin voitaisiin suorittaa verkossa itseopiskeluna.

Kolmas esiin noussut kehittämistä vaativa asia oli viestintä. Palveluntuottajan sisäiseen viestintään ratkaisuna näkisin sisäisen viestinnän hyvien toimintapojen implementoinnin työpaikalla. Näitä toimintatapoja ovat sovitun viestintäkanavan käyttö sekä viestinnässä käytettävä ilmaisu, jota kaikki viestijät ymmärtävät. Hyviin toimintatapoihin viestinnässä sisältyy myös jokaisen vastuu viestiä tiedosta, joka vaikuttaa työyhteisön tehtävien hoitoon. Tämä vaatii palveluntuottajan henkilöstöltä ja johdolta paneutumista asiaan. Pitkäaikaisempana ratkaisuna sisäisen viestinnän kehittämiseen näkisin tietokantapohjaisen tapahtumien raportoinnin käyttöön oton työpaikalla. Nykyinen tekstinkäsittelyohjelmalla suoritettu raportointi ei sisällä mitään sisäistä viestintää tukevia ominaisuuksia. Tietokantapohjaisessa raportointiohjelmassa pystyttäisiin hyödyntämään esimerkiksi henkilökohtaisilla käyttäjätunnuksilla ominaisuutta, joka pakottaisi lukemaan poikkeavat tapahtumailmoitukset pitkän poissaolojakson ajalta. Tämä lisäisi tehokkaasti viestintää ja yleistä tietämystä työpaikan tapahtumista.

Viestintään, tietoturvakoulutukseen ja kohdeorganisaation tietoturvaohjeiden perehdytykseen auttaisi myös koulutusyhteistyö, jossa esimerkiksi organisaation tietoturva-asiantuntija osallistuisi koulutuksen suunnitteluun ja siten koulutukseen pystyttäisiin sisällyttämään perehdytyksen ja organisaation toimintaohjeiden opetusta. Tämä seikka parantaisi myös organisaation ja palveluntuottajan henkilöstön välistä viestintää tietoturva-asioissa, lisäämällä yhteistyötä tietoturvallisuusasoissa.

# 9 Yhteenveto

Tutkimuksen tuloksien perusteella valvomon henkilöstön tietoturvatietoisuuden taso on yleisesti ottaen hyvä. Tämä ilmeni tutkimustuloksien perusteella siten, että alkuperäisen suunnitelman mukaan mediaanin kolme ja alle saaneet vastaukset tulkittaisiin erityistä kehittämistä vaativiksi asioiksi, kuitenkin vastausten perusteella raja-arvo nostettiin arvoon neljä, joka yllätti tutkijan positiivisesti. Valvomon henkilöstön tietoturvatietämyksen tasossa esiintyy kuitenkin vaihtelua, tämä esiintyi hajontana kyselyn vastauksissa varsinkin kysymyksissä, jotka koskivat organisaation sääntöjä. Suurin osa kyselyyn vastanneista henkilöistä tuntee organisaation säännöt hyvin kun taas muutamalla vastaajista esiintyi suurtakin epävarmuutta sääntöjen tuntemuksessa.

Valvomon tietoturvaosaamisen tavoitteena on tutkijan mukaan henkilöstö, joka tuntee kohdeorganisaation tieto-turva ohjeet, ymmärtää mihin kaikkeen tietoturvallisuus vaikuttaa, saa jatkuvaa tietoturvakoulutusta ja pystyy opastamaan ja valvomaan kohdeorganisaation henkilöstön toimintaa tietoturvaan liittyvissä asioissa. Tutkimuksen ajankohtana henkilöstön tietoturva osaamisessa ja kohdeorganisaation ohjeiden tuntemuksessa on puutteita osalla henkilöstöstä.

Tutkimustulosten mukaan palveluntuottajan tietoturvatietoisuuden suurimmiksi puutteiksi nousivat koulutuksen puute, kohdeorganisaation tietoturvaohjeiden tietämys sekä viestintä niin palveluntuottajan sisäinen kuin kohdeorganisaation ja palveluntuottajan välinen. Valvomon tietoturvallisuuden tavoitetason saavuttaminen vaatii sekä kohdeorganisaatiolta että palveluntuottajalta panostusta valvomon henkilöstön kouluttamiseen. Ratkaisuksi näkisin palveluntuottajan ja kohdeorganisaation yhteistyöllä suoritetun tietoturvakoulutuksen, jolla pystyttäisiin vaikuttamaan kaikkiin havaittuihin ongelmiin.

Valvomon tietoturvatietämyksen kehittäminen tulisi aloittaa järjestämällä tietoturvallisuuden perusteet sisältävä koulutus. Koulutuksella saataisiin koko valvomon henkilöstö ymmärtämään mitä tietoturvallisuus on ja mihin kaikkeen se vaikuttaa. Tämän jälkeen kohdeorganisaation tietoturvallisuudesta vastaavan ja valvomon esimiehen tulisi suunnitella perehdytyskoulutus kohdeorganisaation tietoturva ohjeisiin ja käytänteisiin. Perhdytyksen jälkeen valvomon henkilöstön osaamistasoa tulisi mitata, esimerkiksi järjestämällä esimerkiksi kysely verkossa. Mittausten perusteella suunnitellaan vuotuinen kertaus- ja jatkokoulutus, jolla valvomon henkilöstön tietoturvatietoisuutta kehitetään jatkossakin.

Lähteet

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

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2012. 15.-17., painos. Tutki ja kirjoita. Helsinki:Tammi.

Krause, M. & Tipton, H. 2009. Information Security Management Handbook. Volume 3. US: Auerbach Publications

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

Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen-hallittu prosessi. 2006. VAHTI 7/2006. Helsinki: Edita Prima.

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Tampere: Oulun Yliopisto, luonnontieteiden tiedekunta, tietojenkäsittelytieteiden
laitos

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. 3., uudistettu painos. Kehittämistyön menetelmät. Helsinki: WSOYpro.

Tietoturvakouluttajan opas. 2006. VAHTI 11/2006. Valtionvarainministeriö. Helsinki: Edita Prima.

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.

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

Sähköiset lähteet:
Federal Office for Information Security. 2013. IT-Grundschutz-Catalogues. Viitattu 25.5.2017. https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf

Valtiovarainministeriö. viitattu 16.5.2017
http://vm.fi/tieto-ja-kyberturvallisuus

Vähämäki, M. 2015 Tiedon klassinen määritelmä. Viitattu 17.5.2017
http://opinnot.internetix.fi/fi/muikku2materiaalit/lukio/fi/fi1/3_mita_on_tieto_/02_tiedon_klassinen_maaritelma?C:D=1818613&m:selres=1818613)

Haasio, A. & Vakkari, P. 2017 Viestintätieteiden yliopistoverkoston oppimateriaalit. Viitattu 1.6.2017
https://viestintatieteet-wiki.wikispaces.com/Informaatiotutkimuksen+perusteet

Kuviot

Taulukot

Liitteet

Liite 1: Kyselyn saateviesti

Arvon kollegat

Kuten monet teistä varmaankin tietävät opiskelen Laurea ammattikorkeakoulussa tietojenkäsittelyä. Nyt on opinnot siinä vaiheessa, että lopputyö pitäisi toteuttaa. Lopputyössäni tutkin työpaikkamme henkilöstön tietoturvallisuustietämyksen lähtötason ja sen pohjalta pohdin kehitysehdotuksia, jolla tietoturvatietämyksen tasoa voidaan kehittää. Olen laatinut valvomolle Tietoturvatietoisuuden kartoitus kyselyn, jolla lähtötaso selvitetään.
Kaikki kyselyn vastaukset tullaan käsittelemään nimettöminä ja ne ovat luottamuksellisia. Vastauksia käsittelee allekirjoittanut. Osan kyselyn tuloksista tulen esittämään opinnäytetyössäni Laurea-ammattikorkeakoulussa, kuitenkin niin, että organisaatiota ei mainita työssäni.

Kyselyyn vastaaminen kestää noin 5 minuuttia. Arvostaisin kovasti, jos vastaat kyselyyn mahdollisimman pian, koska valmis työ pitäisi esittää jo 23.5.2017.

Kiitos vaivannäöstäsi.

Tuomas

Liite 2: Kyselyn muistutusviesti

Arvon kollegat
Tämä on muistutus työpaikan tieturvakartoituskyselystä
Kuten monet teistä varmaankin tietävät opiskelen Laurea ammattikorkeakoulussa tietojenkäsittelyä. Nyt on opinnot siinä vaiheessa, että lopputyö pitäisi toteuttaa. Lopputyössäni tutkin työpaikkamme henkilöstön tietoturvallisuustietämyksen lähtötason ja sen pohjalta pohdin kehitysehdotuksia, jolla tietoturvatietämyksen tasoa voidaan kehittää. Olen laatinut valvomolle Tietoturvatietoisuuden kartoitus kyselyn, jolla lähtötaso selvitetään.
Kaikki kyselyn vastaukset tullaan käsittelemään nimettöminä ja ne ovat luottamuksellisia. Vastauksia käsittelee allekirjoittanut. Osaa kyselyn tuloksista tulen esittämään opinnäytetyössäni Laurea-ammattikorkeakoulussa, kuitenkin niin, että organisaatiota ei mainita työssäni.

Tällä hetkellä vastausprosentti on 40%

Kyselyyn vastaaminen kestää noin 5 minuuttia. Arvostaisin kovasti, jos vastaat kyselyyn mahdollisimman pian, koska valmis työ pitäisi esittää jo 23.5.2017.

Kiitos vaivannäöstäsi.

Tuomas