OPINNÄYTETYÖ

VIRPI STENBERG 2012

ROVANIEMEN KAUPUNKIKONSERNIN TIETO-TURVAN VERKKOKOULUTUKSEN JÄRJESTÄMINEN JA KOULUTUKSEN ARVIOINTI

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

TIETOJENKÄSITTELYN KOULUTUSOHJELMA

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC ROVANIEMEN AMMATTIKORKEAKOULU

LUONNONTIETEIDEN ALA

Tietojenkäsittelyn koulutusohjelma

Opinnäytetyö

ROVANIEMEN KAUPUNKIKONSERNIN TIETOTURVAN VERKKOKOULUTUKSEN JÄRJESTÄMINEN JA KOULUTUKSEN ARVIOINTI

Virpi Stenberg

2012

Toimeksiantaja Rovaniemen kaupunki

Ohjaaja Eija Turunen

Hyväksytty _____ 2012 _____

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

Luonnontieteiden ala
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön tiivistelmä

Tekijä Virpi Stenberg Vuosi 2012

Toimeksiantaja Rovaniemen kaupunki

Työn nimi Rovaniemen kaupunkikonsernin tietoturvan verkko-koulutuksen järjestäminen ja koulutuksen arviointi

Sivu- ja liitemäärä 53 + 29

Rovaniemen kaupunki järjesti henkilöstölleen tietoturvakoulutusta verkko-oppimisympäristössä vuosina 2010 - 2011. Opinnäytetyöni käsittelee Rovaniemen kaupungin tietoturvakoulutuksen järjestämisen taustaa, koulutuksen sisältöä sekä koulutuksen organisointia ja toteutusta, johon osallistuin.

Opinnäytetyön teoriaosuus muodostuu tietoturvan ja verkko-oppimisen määritelmistä ja niihin liittyvistä käsitteistä.

Opinnäytetyön tavoitteena oli arvioida toteutetun tietoturvakoulutuksen vaikuttavuutta järjestämällä arviointikysely ja sen perusteella selvittää koulutuksen suorittaneiden käsityksiä tietoturvakoulutuksen toteutuksesta, sisällöstä, käytettävyydestä ja vaikuttavuudesta yksilön tietoturvakäyttäytymisen muutokseen.

Arvioinnissa ja johtopäätöksissä kiinnitetään huomiota siihen, miten ja millä keinoin organisaation tietoturvakoulutusta tulisi kehittää. Tämän opinnäytetyön pohjalta voidaan laatia kehittämissuunnitelma Rovaniemen kaupungin tietoturvakoulutuksen järjestämisestä tulevaisuudessa.

Avainsana(t) Tietoturva, koulutus, verkko-oppiminen, vaikuttavuus, arviointi

Rovaniemen ammattikorkeakoulu
University of Applied Sciences
LUC

School of Business and Administration
Business Information Technology

Abstract of Thesis

Author Virpi Stenberg Year 2012

Commissioned by City of Rovaniemi
Subject of thesis Arranging and evaluating of web-based security training in the city of Rovaniemi
Number of pages 53 + 29

The city of Rovaniemi organized security training for staff in web-based learning environment in the years 2010 - 2011. The thesis deals with the background of organizing the information security training, the training content, as well as the organisation and implementation of training for the city of Rovaniemi.

The theoretical part of thesis consists of information security and e-learning definitions and the related concepts.

The aim of this thesis was to evaluate the effectiveness of this implemented information security training on the behaviour of the individual. By organizing the completed assessment questionnaires it was determined how and what changes the individuals made to their own security in the e-learning environment and how usable and effective this was.

The evaluation and conclusions draw attention to how and by what means the organization's information security training should be developed. On the grounds of this thesis this will help to formulate a development program for the city of Rovaniemi for information security training in the future.

Key words Information security, training, e-learning, effectiveness, evaluation

SISÄLTÖ

TAULUKKO- JA KUVIOLUETTELO

1 JOHDANTO

Tämän opinnäytetyön runkona toimivat vuoden 2012 alussa tekemäni yhteenveto tietoturvakoulutuksen järjestämisestä Rovaniemen kaupunkikonsernissa sekä koulutuksen jälkeen toteuttamani arviointi sen vaikuttavuudesta.

Koulutuksen vaikuttavuus voidaan mieltää ja sitä voidaan tutkia monella eri tavoin riippuen yhteyksistä. Tässä opinnäytetyössä vaikuttavuuden arviointi perustuu koulutukseen osallistujien omiin mielikuviin koulutuksesta saadusta hyödystä ja sen hyödyntämisestä omassa työssään koulutuksen jälkeen. Koulutuksesta saatava hyöty riippuu monista eri tekijöistä, kuten henkilön motivaatiosta, oppimisesta, opetustavasta sekä opitun asian soveltamisesta omaan työhön.

Opinnäytetyön teoriapohja muodostuu tietoturvan ja verkko-oppimisen määritelmistä sekä niihin liittyvistä käsitteistä. Työn keskeisin aineisto käsittää tietoturvakoulutuksen järjestämisen ja sen onnistumisen arvioinnin. Arvioimalla järjestettyä koulutusta ja henkilöstön osallistumista siihen, voidaan muodostaa kuva tietoturvallisuuden tietoisuuskasvatukseen paneutumisesta.

Tämän opinnäytetyön toimeksiantajana oli Rovaniemen kaupunki.

2 OPINNÄYTETYÖN LÄHTÖKOHDAT, TAVOITTEET, RAJAUKSET JA KOHDEORGANISAATIO

2.1 Lähtökohdat

Opinnäytetyöni aihe sai alkunsa vuoden 2010 alussa, kun Rovaniemen kaupunki otti käyttöönsä web-pohjaisen tietoturvakoulutusympäristön. Tässä vaiheessa osallistuin koulutuksen suunnitteluun, toteutukseen ja koulutuksesta saatujen tulosten analysointiin. Vuoden 2012 alussa tein näiden pohjalta yhteenvedon koulutuksen taustasta, toteutuksesta ja arvioin koulutustuloksia järjestelmästä koostettujen raporttien perusteella. Yhteenvedossa ei kuitenkaan arvioitu koulutuksen vaikuttavuutta eikä koulutuksen jatkokehittämistä, joka on tärkeä osa koko organisaation tietoturvaosaamisen ja -koulutuksen kehittämisprosessia.

Vuoden 2012 lopulla tein kyselyn, jossa keskeisintä oli arvioida toteutetun tietoturvakoulutuksen vaikuttavuutta. Kyselyssä vastaajia pyydettiin arvioimaan tietoturvakoulutuksen toteutusta, käytettävyyttä, sisältöä ja sen merkitystä. Tavoitteena oli lisäksi selvittää, miten koulutuksen toteutus oli onnistunut ja miten tietojen, taitojen ja tietoturvatietoisuuden kehittyminen on muuttunut toteutetun koulutuksen jälkeen.

2.2 Tavoite

Tämä opinnäytetyö keskittyy järjestetyn tietoturvakoulutuksen tulosten ja vaikuttavuuden arviointiin. Tavoitteena muodostaa käsitys tietoturvakoulutuksen nykytilasta ja tarpeista. Työn pohjalta voidaan löytää ja valmistella ehdotuksia ja toimenpiteitä tietoturvakoulutuksen kehittämiseksi Rovaniemen kaupunkikonsernissa. Näitä kehitystarpeita pyritään löytämään, kysymällä koulutukseen osallistuneilta työntekijöiltä heidän kokemuksiaan ja mielipiteitään.

2.3 Rajaukset

Rovaniemen kaupunkikonsernilla tarkoitetaan tässä työssä Rovaniemen kaupungin ja sen liikelaitosten palveluksessa olevaa henkilöstöä. Työn ulkopuolelle on rajattu kaupungin omistamat tytäryhteisöt, yhdistykset ja säätiöt, kuntayhtymät sekä osakkuus- ja yhteisyhteisöt. Tytäryhteisöistä ei ole kuitenkaan rajattu pois Napapiirin Residuum Oy:tä, jonka henkilöstö osallistui tietoturvakoulutuksen suorittamiseen.

Tässä työssä ei myöskään arvioida Rovaniemen kaupungin terveys-, sosiaali- ja päivähoidonpalvelukeskuksen henkilöstön koulutusta, koska heille vastaava koulutus on järjestetty Lapin sairaanhoitopiirin Uula -hankkeen kautta.

Työssä on keskitytty lähinnä käytetyn opetusmenetelmän ja sen sisällön arviointiin, ottamatta kantaa tietoturvan toteuttamisen teknisiin menetelmiin ja -ratkaisuihin.

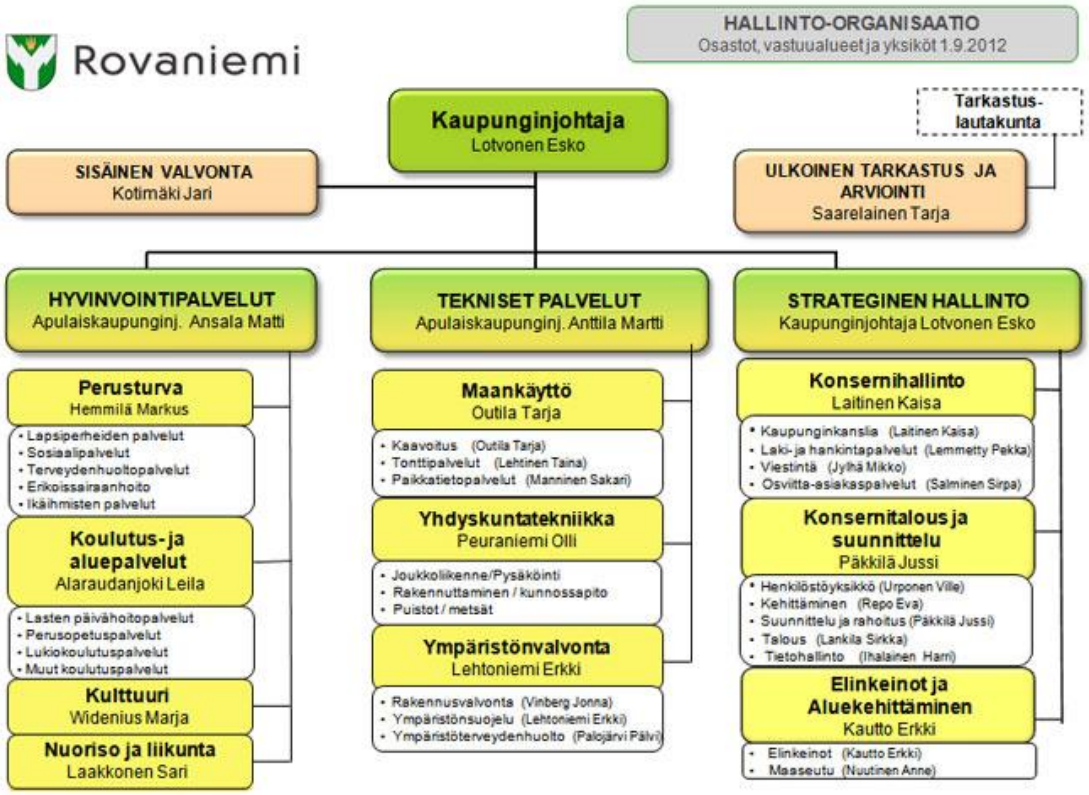
2.4 Kohdeorganisaatio

Rovaniemen kaupungin palveluksessa oli vuoden 2011 lopussa yhteensä 3 506 henkilöä, (Rovaniemen kaupungin henkilöstöraportti 2011) jotka työskentelevät noin 150 eri toimipisteessä. Rovaniemen kaupungilla on käytössä arviolta 250 erilaista tietojärjestelmää, ohjelmaa tai sovellusta sekä lähes 3000 työasemaa.

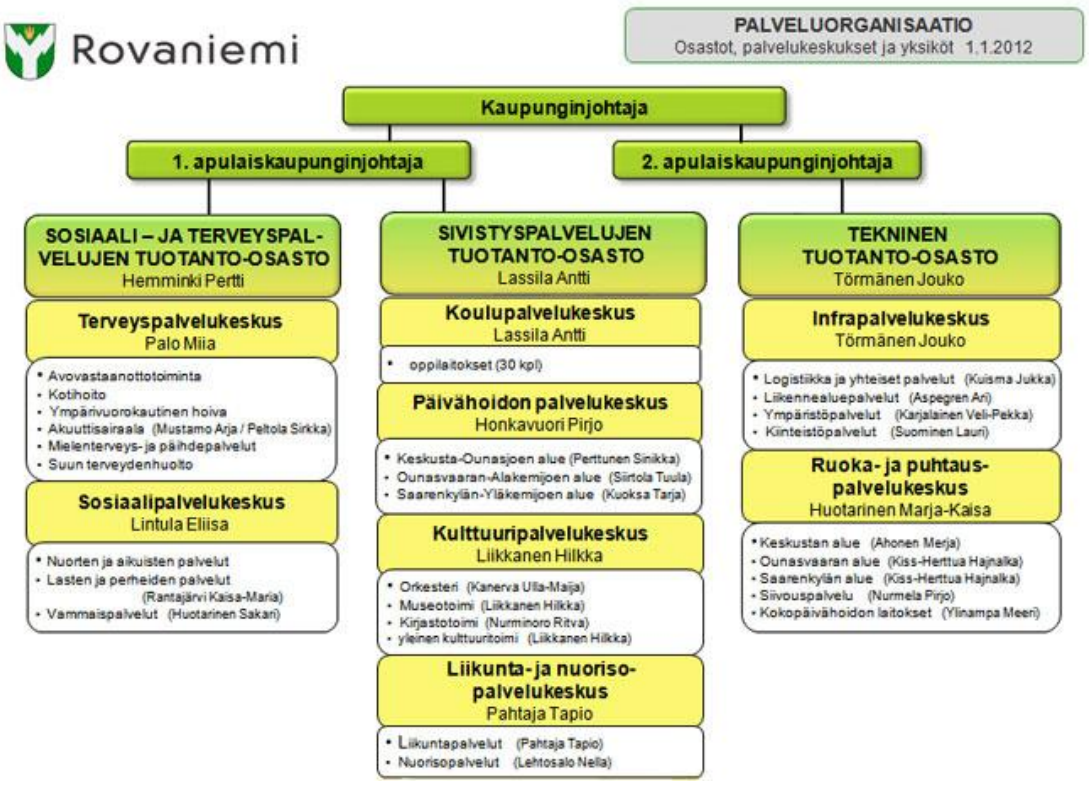
Rovaniemen kaupungin organisaatio muodostuu hallinto- ja palveluorganisaatiosta. Hallinto-organisaatio (kuvio 1) vastaa demokraattisesta päätöksenteosta ja toiminnan ohjaamisesta sekä palvelujen järjestämisestä kuntalaisten perusoikeuksien ja palvelutarpeiden mukaisesti.

Palveluorganisaation (kuvio 2) tuotanto-osastot tuottavat tai hankkivat hallinto-organisaation kanssa hyväksymänsä palvelusopimuksen mukaiset palvelut kunnan asukkaille.

Hallinnon järjestäminen sekä toiminnan ja talouden ohjaaminen perustuu sopimusohjausjärjestelmään, jossa palvelusopimuksilla määritellään järjestettävien, tuotettavien tai ostettavien palvelujen laatu, määrä ja hinta.



Kuvio 1. Rovaniemen kaupungin hallinto-organisaatiokaavio (http://www.rovaniemi.fi/suomeksi/Paatoksenteko/Hallinto-organisaatio)



Kuvio 2. Rovaniemen kaupungin palveluorganisaatiokaavio (http://www.rovaniemi.fi/suomeksi/Paatoksenteko/Palveluorganisaatio)

3 TIETOTURVA

3.1 Tietoturvan merkitys

Tietoturva sisältää joukon toimintoja ja osa-alueita, joihin jokainen voi vaikuttaa omalla toiminnallaan. Se ei ole pelkästään organisaation johdon, tietojärjestelmien ylläpitäjien tai tietohallinnon asia. Organisaation jokaisen työntekijän tulee ymmärtää oma roolinsa tietoturvallisen organisaation ylläpitäjänä. Tämä ei toteudu, mikäli organisaatiossa ei ole laadittu tarkoituksenmukaisia ohjeita ja panostettu henkilökunnan kouluttamiseen.

Rovaniemen kaupungissa on laadittu tietoturvapolitiikka, jonka tarkoituksena on varmistaa Rovaniemen kaupungin toiminnan jatkuvuus ja laatu sekä kuntalaisen ja työntekijän oikeusturvan toteutuminen. Tietoturvapolitiikka on kaupungin johdon kannanotto tietoturvan toteuttamiseen Rovaniemen kaupunkikonsernissa. Rovaniemen kaupungin tietoturvapolitiikassa on määritelty tietoturvan tavoitteet, vastuut, tietoturvatyön organisointi ja toteutuskeinot. Se kuvaa myös tietoturvan seurannan ja tiedottamisen yleisperiaatteet. (Rovaniemen kaupungin tietoturvapolitiikka KH 23.4.2012 § 163.)

Tieto- ja viestintäyhteiskunnan kehittymisen myötä myös työelämässä tarvittavat tiedot, taidot ja haasteet ovat lisääntyneet. Työelämän muutosten tahdissa pysyminen edellyttää jatkuvaa osaamisen kehittämistä. Tieto- ja viestintäteknisten ympäristöjen kehittyminen ja monimutkaistuminen asettaa omat haasteensa tietoturvalle, joka on Nykäsen (2011, 13) mukaan hyvin keskeinen tekijä organisaation kokonaisturvallisuuden ja liiketoiminnan tarpeiden tukemisessa.

Tietoturva koostuu pienistä päivittäisistä teoista ja sen heikoin lenkki on usein ihminen. Tietoturvan tulee olla osa organisaatiokulttuuria, jossa kaikki ymmärtävät sen merkityksen ja osaavat työskennellä ja vaikuttaa sen toteutumiseen (Nykänen 2011, 13).

3.2 Tietoturvan toteuttaminen Rovaniemen kaupunkikonsernissa

Rovaniemen kaupunkikonsernin tietoturvan toteuttamisen perustana on kaupungin tietoturvapolitiikka, josta on tiedotettu koko organisaatiolle. Kaikkiin palvelusopimuksiin tulee sisällyttää tietoturvaan liittyvät vaatimukset, velvoitteet ja häiriötilanteiden toimintamallit sekä määritellä vastuuhenkilöt läpi koko

palveluketjun. (Rovaniemen kaupungin tietoturvapolitiikka KH 23.4.2012 § 163.)

”Tietoturvan hyvä hallinta edellyttää toiminnan jatkuvaa seurantaa, pitkäjänteistä suunnittelua ja resursointia erilaisten uhkatilanteiden varalta. Tietoturvan toteuttaminen vaatii sovittujen ohjeiden ja toimintatapojen noudattamista, koulutusta ja viestintää” (Rovaniemen kaupungin tietoturvapolitiikka KH 23.4.2012 § 163).

Rovaniemen kaupunkikonsernin peruskäyttäjän tietoturvaohje sisältää jokaisen käyttäjän kannalta vähimmäistiedot tietoturvallisesta toiminnasta ja jokaisen käyttäjän pitää lukea ja noudattaa siinä annettuja ohjeita. Kaupunkikonserni edellyttää, että henkilöstö osallistuu järjestettäviin tietoturvakoulutuksiin ja turvallisuusharjoituksiin. (Rovaniemen kaupungin tietoturvapolitiikka, KH 23.4.2012 § 163.)

Kaupungin tietoturvan kehittämistä ja ylläpitoa koordinoi tietohallinto yhdessä kaupunginjohtajan asettaman tietoturvatyöryhmän kanssa, johon itsekin kuulun. Tietoturvatyöryhmän tehtävänä on laatia tietoturvaan liittyvät esitykset, ohjeistukset ja toimintamallit kaupungin johtoryhmän ja kaupunginhallituksen hyväksyttäväksi. Tietoturvakehitystyön tavoitteena on sisällyttää tietoturva luonnolliseksi osaksi kaupungin toimintaa ja palveluja. Kaupungin johto, esimiehet ja työntekijät yksilötasolla ovat vastuussa tietoturvan toteuttamisesta ja varmistamisesta tietoturvapolitiikan mukaisesti. (Rovaniemen kaupungin tietoturvapolitiikka, KH 23.4.2012 § 163.)

3.3 Tietoturvan määrittely

Valtionvarainministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä on määritellyt tietoturvallisuuden seuraavasti: Tietoturvalla tarkoitetaan tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaista suojaamista sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. (VAHTI 3/2007, 13.)

Tietoturvan keskeiset käsitteet ja perustat ovat saatavuus, luottamuksellisuus ja eheys.

Saatavuus tarkoittaa, että tiedot ja palvelut ovat niiden henkilöiden käytettävissä, joilla on siihen oikeus, eivätkä tiedot ole tuhoutuneet vikojen tai muun toiminnan seurauksena.

Luottamuksellisuus tarkoittaa, että tiedot ovat vain niiden henkilöiden käytössä, joilla on siihen oikeus eivätkä tiedot joudu vääriin käsiin.

Eheys puolestaan tarkoittaa, että tiedot ovat luotettavia, oikeita ja ajantasaisia, eivätkä muutu vikojen tai muun toiminnan seurauksena.

Jotta nämä edellä mainitut kolme perustetta saavutettaisiin, tulee organisaation tietoturvan ohjekokonaisuus kattaa kaikki tietoturvallisuuden kahdeksan osa-aluetta.

3.4 Tietoturvallisuuden osa-alueet

3.4.1 Tietoturvallisuuden osa-alueet käyttäjän näkökulmasta

Valtionhallinnossa on tehty Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI toimesta opas julkishallinnon tietoturvakoulutuksen järjestämisestä (VAHTI 6/2003), jonka valmisteluun on osallistunut myös kunnallishallinto. Opasta voidaan näin ollen hyödyntää valtionhallinnon lisäksi myös kunnallishallinnossa.

Oppaassa on nostettu esiin asioita kustakin kahdeksasta osa-alueesta, jotka tulee sisällyttää julkishallinnon organisaation tietoturvan ohjekokonaisuuteen. Seuraavassa tarkastelen näitä osa-alueita ja nostan esiin niitä asioita, jotka vaikuttavat kullakin osa-alueella erityisesti henkilöstön koulutukseen ja ohjeistukseen. Näiden pohjalta voidaan laatia kustakin osa-alueesta yksityiskohtaisemmat tietoturvaohjeet henkilöstölle.

3.4.2 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus on organisaation keskeinen perusta ja lähtökohta tietoturvalliseen toimintaan. Käytännössä tämä tarkoittaa johdon hyväksymiä periaatteita, kuten organisaation tietoturvapolitiikkaa, jossa on määritelty tietoturvan pääperiaatteet, vastuunjaot, tarkoitukseen varatut resurssit sekä riskien arviointi.

Hallinnollinen turvallisuus luo lähtökohdat organisaation tietoturvallisiin toimintatapoihin. Tämän pohjalta laaditaan mm. erilaiset tietoturvaohjeet ja

huomioidaan tarpeet organisaation henkilöstön koulutukseen. (VAHTI 6/2003, 39.)

Henkilöstön tulee olla tietoinen ohjeistuksista ja erityisesti niistä ohjeista, jotka säätelevät heidän omaa työtänsä. Myös tietoturvavastuisiin on kiinnitettävä huomiota ja henkilöstöä koskevat vastuut tulee määritellä, kouluttaa ja ohjeistaa, jotta jokainen työntekijä on tietoinen omasta vastuustaan ja kykenee toimimaan vastuun edellyttämällä tavalla. (VAHTI 6 /2003, 40.)

3.4.3 Henkilöstöturvallisuus

Henkilöstö on organisaation suurin voimavara, mutta samalla myös riski organisaation tietoturvalle. Henkilöstö voi vaarantaa organisaation tietoturvaa joko tahallisesti, mutta usein myös tahattomasti ja näin ollen henkilöstöturvallisuuden osa-aluetta ei tule väheksyä. Pääpainona tulee olla välttää riskit ennakkoon ja varautua niihin oikeanlaisilla toimenpiteillä (VAHTI 3/2007, 57).

Henkilöstöturvallisuudessa on syytä huomioida ainakin seuraavia asioita: tietoturvavelvoitteet henkilön työ- tai virkasopimuksessa, lainsäädännön velvoitteet, salassapitositoumukset, käyttöoikeuksien vastaavuus henkilön työtehtäviin ja avain- ja varahenkilöjärjestelyt.

Edellä mainittuihin asioihin on syytä kiinnittää huomiota jo henkilöstövalinnoissa, mutta myös silloin kun työntekijän työsuhde päättyy syystä tai toisesta. Työntekijän mukana kulkeutuu aina organisaation tietoja. Työnantajan on aina varmistettava, että näitä tietoja ei pääsisi kulkeutumaan organisaation ulkopuolelle. Myös kulkuluvat, avaimet, käyttäjätunnukset väärinkäytettyinä ja muut organisaation turvallisuutta uhkaavat riskit on pyrittävä estämään.

Henkilöstöturvallisuuteen voidaan vaikuttaa henkilöstön motivoinnilla, ohjeistuksella ja koulutuksella. Näin saadaan ennaltaehkäistyä lukuisia tietoturvauhkia. Henkilöstön on tiedostettava oma roolinsa tietoturvan kannalta niin työpaikan sisällä kuin sieltä poistuessaankin.

3.4.4 Fyysinen turvallisuus

Fyysinen turvallisuus tarkoittaa niitä toimenpiteitä, joilla organisaatio suojaa toimitilojaan ja siellä olevia laitteistoja fyysisiltä tapaturmilta tai vahingoittamisyrityksiltä. Fyysinen turvallisuus on laaja-alaista ja koostuu monesta eri osatekijästä, joten se on myös vaikeasti hallittavaa.

Organisaatio vastaa fyysisen turvallisuuden toteutumisesta muun muassa toimitilalukituksilla, kulunvalvontasäännöillä, hälytysjärjestelmillä, henkilö- ja vierailijakorttien käyttämisellä, toimitiloihin saapuvien vieraiden ohjaamisella sekä toimitiloissa olevien tietovälineiden turvallisuudesta huolehtimalla.

Henkilöstöä on ohjeistettava ja koulutettava niistä periaatteista ja toimenpiteistä, joilla organisaation fyysinen turvallisuus taataan. Ohjeissa voidaan ottaa kantaa ovien lukitsemiseen, tietovälineiden ja salassa pidettävien asiakirjojen säilyttämiseen, organisaation omistamien laitteiden käsittelyyn niin organisaation omissa toimitiloissa kuin sen ulkopuolellakin.

Henkilöstöä on tiedotettava myös heihin kohdistuvasta mahdollisesta valvonnasta organisaation toimitiloissa. ”Mikäli organisaation toimitilaturvallisuudesta ja fyysisestä turvallisuudesta vastaavat eri henkilöt kuin tietoturvallisuudesta, on vastuunjako oltava selkeästi käyttäjien tiedossa” (VAHTI 6/2003, 43).

3.4.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella pyritään varmistamaan tietoturvan keskeiset perustat eli tietoverkoissa välitettävien tietojen saatavuus, luottamuksellisuus ja eheys. Käytännössä ne ovat joukko toimenpiteitä, joilla varmistetaan tietojen turvallisuus niiden liikkuessa järjestelmästä toiseen joko organisaation sisällä tai eri organisaatioiden välillä (VAHTI 6/2003, 43).

Henkilöstölle tämä näkyy esimerkiksi sähköpostin, Internetin ja etäyhteyksien turvallisena käyttönä. Sähköpostin, Internetin ja etäyhteyksien turvallinen käyttö määritellään organisaation omilla periaatteilla, ohjeilla ja säännöillä, joista henkilöstön on oltava tietoinen.

On olennaista, että jokainen työntekijä ymmärtää sähköpostin käyttöön liittyvät velvoitteet, rajoitukset ja säädökset. Rovaniemen kaupungin tietoturvapolitiikkaan on kirjattu esimerkiksi se, että työntekijät huolehtivat yhteistyössä esimiestensä kanssa siitä, että heidän työtehtävissään käsittelemät, organisaatiolle kuuluvat tiedot, ovat joka tilanteessa organisaation käytettävissä, ellei niitä muilla määräyksillä ole määrätty hävitettäväksi. (Rovaniemen kaupungin tietoturvapolitiikka, KH 23.4.2012 § 163.) Tämän lisäksi käyttäjille on laadittu erilliset ohjeet sähköpostin ja kommunikaatiovälineiden tietoturvaperiaatteista.

Tänä päivänä Internetin tarjoamat palvelut ja tiedonlähteet ovat tulleet yhä suuremmaksi osaksi organisaatioiden toimintaa ja sen tarjoamia palveluita. Henkilöstölle on näin mahdollistettava turvallinen pääsy organisaation sisäverkosta myös Internetiin. Koska Internetiä voidaan käyttää myös muuhun kuin työtehtäviin, on huolehdittava, että henkilöstö tietää organisaation periaatteet Internetin käyttöön. Internetin käytön periaatteet on määriteltävä ja ohjeistettava niistä henkilöstöä. Esimerkiksi Rovaniemen kaupungin Internetin käytön tietoturvaperiaatteissa on määritelty, että Internet-järjestelmät on tarkoitettu kaupungin viestintään ja palveluista tiedottamiseen, sähköisten palvelujen tarjoamiseen ja henkilökohtaisten työtehtävien hoitamiseen. Työtehtävien hoitamiseen tarvittavien aineistojen lataaminen Internetistä on tekijänoikeuksien ja lisenssiehtojen puitteissa sallittu, mutta muussa tapauksessa se on kielletty.

Etäyhteyksien käyttö voi liittyä tietojärjestelmien etäkäyttöön tai etätyöskentelyyn. Etäkäytöstä on kysymys silloin, kun organisaation tietoverkkoa tai sen osaa käytetään tietoliikenneyhteyden välityksellä organisaation ulkopuolelta. Etätyöllä puolestaan tarkoitetaan työn tekemistä muualla kuin työntekijän vakituisessa toimipisteessä. (VAHTI 6/2003, 45.)

Etäkäyttöoikeuden saaneelle työntekijälle on oleellista ymmärtää etätyöstä aiheutuvat riskit tietoturvallisuudelle. Etätyössä myös korostuu työntekijän oma vastuu, koska pääsääntöisesti hän vastaa siitä, että luottamukselliset tiedot ovat vain niiden käyttöön oikeutettujen saatavissa (VAHTI 3/2007, 66). Organisaation tulee laatia etäkäyttöoikeuksista periaatteet sekä ohjeet ja varmistettava työntekijän sitoutuminen organisaation tietoturvaperiaatteisiin allekirjoitetulla sopimuksella.

3.4.6 Laitteistoturvallisuus

Laitteistoturvallisuus pitää sisällään teknisten laitteiden käytettävyyden, toimintavarmuuden, kokoonpanon, kunnossapidon sekä laadunvarmistuksen. Laitteistoturvallisuuden keskeinen tavoite on tarjota organisaation henkilöstölle mahdollisuus tehdä laitteiden avulla työtä tietoturvallisesti ja ilman, että niiden käytöstä aiheutuu kohtuuttomasti häiriötä tai keskeytyksiä.

Laitteistoturvallisuudessa on syytä ottaa huomioon ainakin laitteiden hankintaan, asennukseen, käyttöön, huoltoon, takuuseen, ylläpitoon sekä käytöstä

poistoon liittyvät seikat (VAHTI 3/2007, 63). Organisaatiossa on hyvä luoda selkeä toimintaprosessi kuinka edellä mainitut toimenpiteet hoidetaan ja kenen vastuulla se on. Myös omien laitteiden tuominen töihin ja liittäminen organisaation tietojärjestelmiin, laitteisiin tai tietoverkkoon voi aiheuttaa suuren tietoturvariskin. Kun edellä mainitut prosessit on hyvin määritelty ja henkilöstö on tietoinen toimintatavoista kunkin prosessin osalta, voidaan saavuttaa hyvin ylläpidetty, laadukas ja toimintavarma tietotekninen toimintaympäristö.

3.4.7 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus käsittää organisaatiossa käytettävien käyttöjärjestelmien ja käytettävien sovellusten ja ohjelmistojen turvallisuuden. Organisaation ohjelmistoturvallisuudesta huolehditaan käytännössä ohjelmistojen ajantasaisella päivittämisellä, käyttäjäoikeuksien ja lisenssien ylläpidolla sekä ehkäisemällä viruksien ja haittaohjelmien leviämistä.

Henkilöstölle tämä tarkoittaa, että suojauskeinoista on huolehdittu siten, että ohjelmistojen pääsynvalvontamekanismi on määritelty, ohjelmistojen tapahtumatietoja seurataan riittävässä määrin, ohjelmistoille on laadittu tarkoituksenmukainen käyttödokumentaatio ja tarpeettomien tai tietoturvaa uhkaavien ohjelmiston lataaminen työasemaan on estetty.

Henkilöstöä tuleekin ohjeistaa ja kouluttaa toimimaan oikein tietoturvaa uhkaavissa tilanteissa, kuten esimerkiksi silloin, kun haitallinen virus on saastuttanut työaseman. Henkilöstöä tulee myös ohjeistaa varmuus- ja suojakopioiden ylläpidosta ja riskeistä mitä Internetistä ladatut ohjelmat voivat aiheuttaa koko organisaation toimintaan. Henkilöstölle tulee myös tiedottaa organisaation käyttöoikeus- ja pääsynvalvontamenettelyistä ja työntekijän tulee noudattaa työntehtävissä sallittavia valtuuksia. Henkilöstön on oltava tietoinen organisaatiossa käytettävistä tietoturvarikkomusten havainnointimenetelmistä ja seuraamuksista. (VAHTI 6/2003, 47.)

3.4.8 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden tarkoituksena on tiedon elinkaaren eri vaiheessa (luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi, tuhoaminen) taata sen käytettävyys, eheys ja luottamuksellisuus (VAHTI 6/2003, 48).Se koskee kaikkea organisaation merkittävää tietoa riippumatta siitä missä muodossa tieto on. Tietoaineistoturvallisuu-

den muuttumattomuuden takaamiseksi tärkeimpiä keinoja ovat tiedon luokittelu, tietovälineiden asianmukainen hallinta, käsittely, säilytys ja hävittäminen (VAHTI 6/2003, 48).

Henkilöstön on tärkeää ymmärtää mitä virheellisen tiedon leviäminen jatkokäsittelyyn tai päätösten tekeminen virheellisin tiedoin vaikuttaa organisaation toimintaan. Tallennetun tiedon ja tietojärjestelmien suojaaminen vahingoilta, vahingoittamiselta ja menetyksiltä koskettaa koko henkilöstöä. Tietoaineistoturvallisuus koskettaa myös muuta kuin tietojärjestelmiin tallennettua tietoa. ”Asiakirjojen virallisuus ei riipu viestintä- ja käsittelyvälineestä tai asiakirjan fyysisestä muodosta. Sähköpostitse lähetettävä ja vastaanotettava asiakirja voi olla yhtä virallinen kuin paperimuotoinen asiakirja, jos se liittyy virka-asian hoitamiseen” (VAHTI 6/2003, 49).

Organisaation henkilöstön kouluttamisen ja ohjeistamisen kannalta on tärkeää tehdä käsittelysäännöt tiedoille, joilla ne pystytään luokittelemaan eri ryhmiin, kuten julkinen ja salainen. Myös luokitellun tiedon välittämiseen tietojärjestelmissä ja Internetissä on oltava pelisäännöt, jotta salassa pidettävää tietoa ei leviä vääriin käsiin. Viranomaisen toimintaa säätelee laki viranomaisen toiminnan julkisuudesta (621/1999) ja sen nojalla annettu asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999). Viranomaisten asiakirjat ovat julkisia, jollei toisin ole säädetty.

Tietoaineistoturvallisuuden erityinen osa on tietosuoja ja sitä säätelee suurelta osin henkilötietolaki (523/1999). Mikäli organisaatio pitää henkilörekisteriä, on sen tehtävä tarvittavat tekniset ja hallinnolliset toimenpiteet, jotta henkilön yksityisyys on suojattu valtuudettomalta tai henkilöä vahingoittavalta käytöltä. Kaikki henkilörekisteriä ja henkilötietoja käsittelevät henkilöt tulee kouluttaa ja ohjeistaa huolellisesti henkilötietojen käsittelyyn, luovuttamiseen ja käyttöön liittyvissä asioissa. Myös tietojen salaamiseen tulee tässä kiinnittää huomiota.

Varmuuskopiointi sekä suoja- ja turvakopiointi ovat osa tietoaineistoturvallisuutta. Varmuuskopioinnin tavoitteena on varmistaa tietojen käytettävyys esimerkiksi siinä tilanteessa, kun tietojärjestelmä on toimimaton. Suoja- ja turvakopioinnista puhutaan puolestaan silloin, kun halutaan säilyttää jokin tietoaineisto, mutta sitä ei ole tarve tai järkevää arkistoida. (VAHTI 6/2003, 50.)

Arkistoinnilla puolestaan tarkoitetaan sitä osaa tietoaineistoturvallisuudessa, jossa tietojen tallentaminen on pitkäaikaista tai pysyvää. Sillä varmistetaan tietojen käytettävyys. Julkishallinnossa arkistointia säätelee arkistolaki (831/1994). Organisaatio voi toteuttaa tätä esimerkiksi laatimalla arkistolain vaatimukset täyttävän arkistointisuunnitelman ja ohjeistaa henkilöstöä sen noudattamiseen.

Yksi osa tietoaineistoturvallisuutta on tietoaineiston käytöstä poistaminen ja hävittäminen, joka koskee missä tahansa muodossa olevaa tietoa. Käytöstä poistosta ja hävittämisestä on olemassa Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje (VAHTI 2/2000) jota voidaan hyödyntää myös kuntaorganisaatiossa. Erityistä huomiota on kiinnitettävä salassa pidettävien asiakirjojen käytöstä poiston ja hävittämisen ohjeistamisessa, jotta organisaatiolle hyödyttömäksi käynyt tieto ei joudu ulkopuolisten käsiin (VAHTI 6/2003, 51).

3.4.9 Käyttöturvallisuus

Käyttöturvallisuus on se osa tietoturvaa, joka pitää sisällään tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn sekä sen tuki-, ylläpito-, kehittämis- ja huoltotoimenpiteisiin liittyviä ratkaisuja. Käyttöturvallisuudella huolehditaan turvallisesta ja luotettavasta tietoteknisestä käyttöympäristöstä. (VAHTI 6/2003, 51.)

Käyttöturvallisuuteen liittyvät myös käyttäjätunnuksien ja salasanojen, PIN-koodien käyttö ja hallinnointi. Henkilöstöä on ohjeistettava miten tietojärjestelmiä käytetään ja mikä on henkilökohtainen vastuu, kun käyttäjä kirjautuu tietoverkkoon tai -järjestelmään omalla käyttäjätunnuksellaan. Henkilöstön tulee myös tietää, että käyttöoikeuksien saaminen perustuu työtehtäviin ja ne poistuvat työsuhteen päättyessä. Olennainen osa käyttöturvallisuutta on myös seuranta ja valvonta, jotta tietoturvariskejä pystytään myös mahdollisimman pitkälle ennaltaehkäisemään. Henkilöstön tulee olla tietoinen mitä toimintaa organisaatiossa seurataan tai valvotaan ja millä välineillä. (VAHTI 6/2003, 51.)

4 VERKKO-OPPIMINEN

4.1 Verkko-oppimisympäristö käsitteenä

Tennon (2011, 53) mielestä verkko-oppimisympäristöä ei voida käsittää pelkästään johonkin tiettyyn fyysiseen tilaan tai tietoverkkoon rajattuna ympäristönä, vaan se on ympäristö, jossa opiskelija on. Verkko-oppimisympäristön erottaa tavanomaisesta toimintaympäristöstä se, miten opetus ja oppiminen kyseisessä ympäristössä organisoidaan ja osa niistä syntyy oppimis- ja työskentelytapojen kautta (Tenno 2011, 53). Verkko-oppimisympäristö voidaan myös nähdä virtuaalisena tilana, jossa on opiskelijalle tarvittavat puitteet ja resurssit. Resursseina voidaan pitää kaikkea teknologisia, sosiaalisia, kognitiivisia ja episteemisiä ratkaisuja. (Tenno 2011, 53.)

Verkko-oppimisympäristöllä tarkoitetaan tässä opinnäytetyössä kokonaan tietoverkoissa toteutettua koulutusta, joka oli luonteeltaan suunnitelmallista. Oppimiselle oli määritelty tavoitteet ja oppisisällöt oli erikseen suunniteltu. Oppimista myös seurattiin ja arvioitiin.

4.2 Verkko-oppimisympäristö oppimistilana

Tarkastelen tässä luvussa oppimisen edellytyksiä työelämälähtöisessä koulutuksessa verkko-oppimisen näkökulmasta. Verkko-oppiminen tarkoittaa tässä oppimistoimintaa, jossa hyödynnetään tieto- ja viestintätekniikkaa ja työskentely on tavoitteellista ja ohjattua, mutta silti itsenäisesti tapahtuvaa oppimista. (Tenno 2011, 28.)

Tennon (2011, 26) mukaan verkko-oppimisessa pätevät samat lainalaisuudet kuin muussakin oppimisessa ja keskeistä siinä on pikemminkin käsitteellinen muutos, joka painottaa enemmän sosiaalisen toiminnan merkitystä oppimisessa.

Vaikka tieto- ja viestintätekniikka on tarjonnut jo suhteellisen pitkään uusia työvälineitä opetukseen ja opiskeluun, on niiden käyttö ainakin kuntaorganisaatioissa ollut vähäistä. Verkko-oppimisympäristöt tarjoavat kuitenkin tänä päivänä myös organisaatioille ja työnantajille mahdollisuuksia kouluttaa henkilöstöään uudella ja usein myös kustannustehokkaammalla tavalla. Opetuksen siirtäminen verkkoon ei saa kuitenkaan olla itsetarkoitus tai työtapojen

kopiointia uuteen konseptiin, vaan sen tulee perustua perusteltuihin ja huolellisesti arvioituihin ratkaisuihin.

Etenkin työelämälähtöisissä koulutuksissa on otettava huomioon henkilöstön olemassa olevat taidot ja tiedot. Vanhat tiedot ovat usein uuden oppimisen edellytys, mutta ne saattavat olla myös este sille, mikäli ne ovat ristiriidassa uuden tiedon kanssa. ”Mitä enemmän ihmisellä on elämänkokemusta, sitä enemmän on myös vakiintuneita ajattelu- ja toimintamalleja” (VAHTI 11/2006, 13).

Koulutuksen kannalta tämä on haasteellista, koska uusi asia on kytkettävä käytännön kokemukseen, joko uuteen tai vanhaan. Uutta oppiessaan ihminen pyrkii omaksumaan tietoa jo olemassa olevan tiedon perusteella ja tekee siitä omat tulkintansa käsitystensä, odotustensa ja ominen tavoitteidensa pohjalta. (VAHTI 11/2006, 14.)

Työelämälähtöistä koulutusta suunniteltaessa on myös otettava huomioon, että työntekijän tavoitteena on usein hankkia tietoa käytännön ongelmien ratkaisuun ja koulutuksesta tulisi saada jotain, joka auttaa häntä kehittämään omaa työtänsä. Mikäli koulutusta ei koeta työn kannalta hyödylliseksi, sitä ei koeta myöskään merkitykselliseksi.

Tämän lisäksi jokaisella on oma oppimistyylinsä ja kaikki opetusmenetelmät eivät sovi kaikille. Motivaation merkitystä ei myöskään pidä väheksyä. Sillä on keskeinen merkitys siinä, miten työntekijä suhtautuu koulutukseen tai ponnistelee kohti tavoitteita. Hyvä motivaatio luo edellytykset myös hyvälle oppimistulokselle. Se auttaa ponnistelemaan kohti tavoitteita ja edesauttaa näin ollen myös oppimista.

4.3 Verkko-oppimisympäristö henkilöstökoulutuksen välineenä

Rovaniemen kaupungin henkilöstön kehittämisen haasteena on turvata henkilöstön osaamistaso huolimatta siitä, että kaupungin palveluksesta poistuu eläkkeelle jäännin seurauksena yhä suurempi määrä henkilöstöä tulevina vuosina (Rovaniemen kaupungin henkilöstöraportti 2011). Myös talouden näkymät asettavat kuntasektorille omat haasteensa henkilöstön osaamisen kehittämisessä. Henkilöstökoulutuksen kriittiset tekijät ovat riittävän rahoituksen varmistaminen ja kytkeminen organisaation strategiaan. Tulevaisuudes-

sa myös koulutukseen käytettävän ajan varmistaminen on entistä tärkeämpää.

Tämä tilanne edellyttää myös kriittistä tarkastelua henkilöstön kouluttamisen ja kehittämisen osalta, jotta osaamisen taso ja motivaatio säilytetään koko työuran ajan. Ennusteiden mukaan ikärakenteen muutos ja kansainvälistymisen vaikutus henkilöstökoulutukseen tulee lisääntymään. Myös työn sisällön muutokset, tieto- ja viestintätekniikan kehitys ja verkko-oppimisen mahdollisuudet tulevat vaikuttamaan henkilöstökoulutuksen kehitykseen tulevaisuudessa.

Kuntaorganisaatioissa verkko-oppimisen soveltamista henkilöstökoulutuksen välineenä on toteutettu varsin vähäisessä määrin tai ainakin enemmän kokeiluluontoisina hankkeina. Tämä vaatisikin tarkempaa selvitystä, koska verkko-oppimisen tulisi tarjota lisäarvoa ja uusia mahdollisuuksia organisaatiolle eikä kustannuksissa säästäminen saisi olla keskeinen motiivi sen soveltamiselle. Yhtenä syynä verkko-oppimisen soveltamiseen henkilöstökoulutuksen välineenä saattaakin olla kokemusten vähäisyys ja pelko siitä että alun investointikustannukset saattaisivat nousta korkeiksi.

Tärkeimpiä verkko-oppimiseen kohdistuvia odotuksia on varmasti uudenlaisten oppimismuotojen käyttöönotto, erityisesti ajasta ja paikasta riippumaton opiskelun mahdollisuus, joka korostuu tulevaisuudessa etätyömahdollisuuksien kehittyessä. Vapaus tulisikin nähdä sekä työntekijän mahdollisuutena joustavaan opiskeluun että organisaation etuna, kun opiskelussa voidaan hyödyntää työn suvantovaiheita. Odotuksia kohdistuu myös oppimisen sisällöllisten tavoitteiden parempaan saavuttamiseen, sosiaalisen vuorovaikutteisuuden lisääntymiseen ja sähköisen viestinnän kehittämiseen. (Valtionvarainministeriön työryhmämuistioita 6/2002, 17.)

Tämä Rovaniemen kaupungin henkilöstölle verkko-oppimisympäristössä toteutettu tietoturvakoulutus, josta kerron seuraavaksi, osoitti kuitenkin, että uhkakuvista huolimatta, uusi koulutusmuoto koettiin ainakin tässä yhteydessä varsin toimivaksi henkilöstökoulutuksen välineeksi.

5 ROVANIEMEN KAUPUNGIN TIETOTURVAKOULUTUS

5.1 Yleistä

Tässä kappaleessa selvitän Rovaniemen kaupungin tietoturvakoulutuksen järjestämisen taustaa, koulutuksen sisältöä sekä koulutuksen organisointia ja toteutusta, johon osallistuin vuosina 2010 – 2011. Olen arvioinut erillisessä yhteenvedossa koulutustuloksia, josta otan vain keskeisimmät havainnot mukaan tähän tarkasteluun.

5.2 Koulutuksen taustaa

Granite Partners Oy ja ePohjois-Suomi ovat tehneet puitesopimuksen web-pohjaisen tietoturvallisuuden koulutusympäristön käyttöoikeudesta. ePohjois-Suomi (ePS) on Oulun, Kuusamon ja Rovaniemen kaupunkien tietohallinnon yhteistyöverkosto. Koulutusympäristöä on räätälöity asiakaskohtaisesti. Sopimuksen option perusteella ePS-kaupunkien työyksiköt ovat voineet halutessaan hyödyntää sopimuksen koulutuksia hintaan 1,20 €/käyttäjä/vuosi. Rovaniemen kaupunginjohtaja linjasi päätöksellään (15.12.2008 § 559), että Rovaniemen kaupunki ottaa koulutusympäristön käyttöön, koulutuksen suorittaminen on pakollista ja koulutuksen voi suorittaa työaikana.

Rovaniemen kaupungin tietohallinto teki sopimuksen koulutusympäristön käyttöoikeudesta ajalle 1.1.2010 – 31.12.2010. Koulutuksen kohderyhmä oli kaupungin ja sen liikelaitosten henkilöstö, joilla oli käyttäjätunnukset Rovaniemen kaupungin tietoverkkoon. Arvioitu käyttäjämäärä oli tuolloin yhteensä 1700 henkilöä. Koulutus suunniteltiin järjestettäväksi kertakoulutuksena sillä hetkellä palveluksessa olevalle henkilöstölle, pois lukien sosiaali-, terveys- ja päivähoidon palveluiden henkilöstö, jolle sama koulutus järjestetään muun tahon toimesta. Koulutus hyväksyttiin osaksi Rovaniemen kaupungin koulutustyöryhmän koordinoimaa keskitettyä koulutusta, josta myös koulutuskustannukset maksettiin.

Kaupunki sai halutessaan jatkaa käyttöoikeutta vuoden kerrallaan puitesopimuksessa määriteltyä vuosihintaa vastaan. Koulutusta jatkettiinkin vielä 1.1.2011 – 31.12.2011 välisen ajan ja koulutusympäristön tuloksia päätettiin tarkastella vuoden 2011 lopussa.

5.3 Koulutuksen sisältö

Koulutus toteutettiin web-pohjaisella verkkokoulutusalustalla, jossa työntekijä pystyi ajasta ja paikasta riippumatta suorittamaan tietoturvallisuuden peruskoulutuksen. Koulutusmateriaalin sisältö oli laadittu yhteistyössä järjestelmän toimittajan ja ePS-kaupunkien yhteisen tietoturvavastaavan kanssa. Koulutusmateriaaliin koottiin kattava tietopaketti tietoturvan perusteista. Teoreettisen tarkastelun lisäksi oppimateriaalissa perehdyttiin kaupungin omiin tietoturvaperiaatteisiin ja toimintatapoihin.

Koulutus koostui seuraavista osa-alueista: alkutesti, tietoturvan perusteet, käytännön ohjeet, yhteenveto ja lopputesti. Koulutusympäristössä olivat myös koulutuksen suorittamisen ja koulutusympäristössä navigoinnin käyttöohjeet sekä sivukartta.

Perusteet osiossa käsiteltiin tietoturvan keskeisiä käsitteitä ja tietoturvan osa-alueita. Käytännön ohjeissa tutustuttiin käytännön tietoturvaongelmiin ja kaupungin toimintatapoihin, jotka on kuvattu tietoturvapolitiikassa, tietoturvaperiaatteissa ja tiettyihin kokonaisuuksiin liittyvissä ohjeissa. Lisäksi osana käytännön ohjeita oli kattava paketti ajankohtaisesta tietoturvaa uhkaavasta ilmiöstä sosiaalisesta krakkeroinnista. Sosiaalinen krakkerointi tarkoittaa tietoturvaan kohdistuvia hyökkäyksiä, joissa hyökkääjä sosiaalisia taitojaan hyväksikäyttäen yrittää saada organisaation tietoja haltuunsa.

Yhteenveto jakautui Digitoday.fi -lehden tietoturva-aiheisiin uutislinkkeihin, lyhyeen kertausosioon ja yhteenvetoon Rovaniemen kaupungin peruskäyttäjän tietoturvaohjeista.

Koulutusmateriaali piti sisällään alkutestin, jonka suorittaminen oli pakollista, jotta koulutuksessa pääsi etenemään. Alkutesti piti sisällään 10 kysymystä tietoturvan eri osa-alueilta. Koulutusmateriaalissa oli lisäksi pieniä välikyselyitä, joilla työntekijä pystyi testaamaan osaamistaan. Varsinainen lopputesti oli suoritettava, jotta koulutus katsottiin hyväksytysti suoritetuksi. Lopputestissä oli kysymyksiä koulutusympäristön teoriaosuuden eri osa-alueilta. Hyväksyttyyn suoritukseen vaadittiin vähintään 12 oikeaa vastausta 20 kysymyksestä.

Koulutuksen jälkeen työntekijä pystyi tulostamaan itselleen todistuksen hyväksytystä suorituksesta sekä yhteenvedon Rovaniemen kaupungin perus-

käyttäjän tietoturvaohjeista. Hyväksyttyä lopputestiä ei voinut suorittaa uudelleen, mutta sen sijaan hylätyn suorituksen pystyi suorittamaan niin monta kertaa, että sen läpäisi.

5.4 Koulutuksen organisointi ja toteutus

Koulutus organisoitiin Lapin sairaanhoitopiirin Uula -hankkeessa toteutetun vastaavan koulutuksen pohjalta. Tietohallintokoordinaattorit Virpi Stenberg ja Elmi Marjomaa sekä palvelussuhdesihteeri Marjo Hettula organisoivat koulutusympäristön käyttöönoton, ohjeistuksen ja viestinnän yhteistyössä nimettyjen esimiesten/ryhmävastaavien kanssa.

Koulutus toteutettiin kahdessa vaiheessa, joista ensimmäisenä koulutettiin Rovaniemen kaupungin ja liikelaitosten henkilöstö pois lukien sosiaali- ja terveyspalvelukeskuksen sekä päivähoidon henkilöstö, jolle sama koulutus toteutettiin Lapin Sairaanhoitopiirin hallinnoiman Uula -hankkeen toimesta. Koulupalvelukeskuksen henkilöstön työajoista johtuen koulupalvelukeskuksen henkilökunnan koulutus päätettiin toteuttaa toisessa vaiheessa opettajien kesälomien jälkeen syksyllä 2010.

Toteuttamista varten koulutusympäristöön tehtiin organisaatioryhmät, jotka puolestaan jaettiin osastoihin, joille nimettiin vastuuhenkilöt eli ryhmävastaavat. Pääsääntöisesti osastojen tai yksiköiden esimiehet toimivat ryhmävastaavina. Jokaiselle organisaatioryhmälle nimettiin lisäksi alueellinen vastuuhenkilö sekä yksi koko kaupunkiorganisaation vastuuhenkilö. Organisaatioryhmiin ja osastoihin jakamisen tarkoituksena oli, että esimiehet /ryhmävastaavat tietävät oman alueensa työntekijät ja näin koulutusympäristöön rekisteröityneiden seuranta oli helpompaa. Tämä mahdollisti myös osastokohtaisten raporttien saamisen koulutustuloksista. Ryhmien vastuuhenkilöille pidettiin neljä samansisältöistä infotilaisuutta ennen koulutuksen aloittamista.

Ensimmäiset infotilaisuudet ryhmävastaaville järjestettiin 6.5.2010 sekä 10.5.2010 ja niihin osallistui yhteensä 28 henkilöä. Toisen vaiheen infotilaisuudet koulupalvelukeskuksen henkilöstölle järjestettiin 29.9.2010 sekä 4.10.2010 ja niihin osallistui yhteensä 26 henkilöä.

Infotilaisuuksissa käytiin läpi koulutuksen käyttöönoton taustaa, tietoturvan merkitystä, ryhmävastaavien oikeuksia ja velvollisuuksia sekä koulutuksen käytännön toteutusta ja aikataulua.

Infotilaisuuksien jälkeen laitettiin kaupungin sisäiseen intranetiin ohjeistusmateriaali sekä linkit varsinaiseen koulutusympäristöön rekisteröitymistä varten. Nämä tulivat kaupungin keskitetyn koulutuksen sivustolle, jossa ne olivat henkilöstön saatavilla koko koulutuksen keston ajan.

5.5 Koulutusympäristöön rekisteröityminen

Koulutuksen aloittamiseksi tuli valita intranetissä olevista organisaatiolinkeistä omaa organisaatiota vastaava linkki, josta pääsi rekisteröitymään ja tilaamaan tunnukset koulutusympäristöön. Rekisteröitymisajaksi sovittiin noin kaksi viikkoa. Linkkejä molempien vaiheen koulutuksessa oli yhteensä neljä. Käyttäjät ohjeistettiin kirjallisesti oikean linkin valitsemisessa. Organisaatiolinkin valittuaan, käyttäjälle avautui alasvetovalikko, josta löytyivät sen organisaatioryhmän alle lisätyt osastot. Mikäli käyttäjä tunsi oman organisaationsa ja sen eri osastot ja yksiköt, ei oikean linkin ja osaston valitsemisessa ollut ongelmia. Tässä vaiheessa todettiin myös, että kaikki eivät tienneet omaa paikkaansa organisaatiossa ja muutama käyttäjä oli ohjeistuksesta huolimatta rekisteröitynyt väärän organisaatiolinkin tai väärän osastovalinnan kautta.

Ryhmävastaavien tehtävänä oli rekisteröitymisvaiheen päätyttyä tarkastaa, että oman vastuualueen työntekijät ovat rekisteröityneet koulutusympäristöön. Tehtävän hoitamiseksi, ryhmävastaaville oli annettu koulutusympäristön hallintaoikeudet tarkastella oman vastuualueensa rekisteröityneitä henkilöitä. Vaikka ryhmävastaaville kerrottiin tämän vaiheen tärkeydestä, huomattiin koulutuksen kuluessa paljon osastokohtaisia eroja tehtävän suorittamisessa. Koulutuksen loppuvaiheessa todettiinkin, että infotilaisuuksissa ja ryhmävastaavien ohjeistuksessa tämän vaiheen tärkeyttä olisi ollut syytä korostaa nykyistä enemmän.

5.6 Koulutusympäristöön kirjautuminen

Rekisteröitymisen jälkeen koulutusympäristö lähetti käyttäjän sähköpostiin tunnuksen, salasanan ja linkin varsinaiseen koulutusympäristöön tai vaihtoehtoisesti käyttäjä pystyi tulostamaan Pdf -tiedoston, josta tiedot löytyivät.

Mikäli sähköpostiosoitteessa oli virhe tai se ei muuten vastannut täysin olemassa olevaa (rovaniemi.fi) sähköpostiosoitetta, ei käyttäjä saanut koulutusympäristöstä tunnuksia sähköpostiinsa.

Ilmeisesti käyttäjillä oli ongelmia kirjautumisen kanssa, koska koulutuksen edetessä huomattiin, että muutamilla käyttäjillä oli useita tunnuksia, toisin sanoen he olivat rekisteröityneet koulutusympäristöön useaan kertaan. Mahdollisesti tähän vaikutti se, että jos rekisteröitymisen ja ensimmäisen kirjautumisen välillä oli pitkä aika, koulutusympäristön lähettämät kirjautumistiedot olivat kadonneet ja käyttäjä rekisteröityi uudelleen. Toinen mahdollinen selitys useille tunnuksille oli se, että vaikka kirjautumistiedot tulivat linkkeineen sähköpostiin, käyttäjä yritti kirjautua koulutusympäristöön rekisteröitymislinkin kautta ja huomaamattaan teki uusia rekisteröitymisiä.

5.7 Koulutuksen suorittaminen

Koulutuksen suorittamiseen oli sovittu aikaa kahdelle ensimmäiselle ryhmälle neljä kuukautta ja kahdelle seuraavalle ryhmälle (koulupalvelukeskuksen henkilöstö) kaksi kuukautta. Koulutusajan loppuvaiheessa otettu etenemisraportti osoitti, että osa oli aloittanut koulutuksen, mutta osalla se oli yhä kesken. Ryhmävastaaville lähetettiin tästä sähköpostiviesti, että he muistuttaisivat työntekijöitä koulutuksen suorittamisesta. Tässä vaiheessa todettiin myös, että kaikki eivät vielä olleet rekisteröityneet koulutusympäristöön. Koulutusympäristö lähetti automaattimuistutuksia koulutuksen suorittamisesta niille, jotka olivat rekisteröityneet. Ryhmävastaavien rooli korostui tässä vaiheessa, koska koulutusympäristö ei lähettänyt automaattimuistutuksia rekisteröitymättömille. Toisaalta ne käyttäjät, joilla oli useampia tunnuksia koulutusympäristöön, saivat muistutusviestejä, vaikka olivatkin jo suorittaneet yhdellä tunnuksella koulutuksen.

Syksyllä 2010 otetun etenemisraportin pohjalta koulutusympäristöstä siivottiin pois ylimääräisiä tunnuksia, patisteltiin koulutusympäristöön rekisteröitymättömiä rekisteröitymään ja seurattiin etenemistä ylipäänsä. Myös vääristä organisaatiolinkeistä kirjautuneita siirrettiin oikeisiin osastoihin. Tässä vaiheessa yhteydenottojen määrä vastuuhenkilöihin päin lisääntyi jonkin verran ja koulutuksen suoritusaikaa päätettiin pidentää vuoden 2010 loppuun saakka.

Vuoden 2011 syksyllä kehotettiin intranetissä niitä käyttäjiä, jotka eivät olleet vielä suorittaneet koulutusta, tekemään se viimeistään 18.11.2011 mennessä. 13.12.2011 lähetettiin vielä sähköpostia niille käyttäjille, jotka olivat rekisteröityneet koulutusympäristöön, mutta joilta puuttui vielä suoritus tai sen osa. Tämän jälkeen tehtiin vielä vertailu voimassa olevista käyttäjätunnuksista ja työsuhteista, jossa todettiin, että osa käyttäjätunnukset omaavista henkilöistä ei ollut lainkaan rekisteröitynyt koulutusympäristöön, eikä näin ollen ole suorittanut koulutusta. Heitä muistutettiin asiasta vielä sähköpostitse 20.12.2011.

5.8 Koulutuksen tulosten arviointi

Koulutusympäristöön rekisteröityi yhteensä 1297 kaupungin työntekijää. Rekisteröityneiden työntekijöiden osalta voidaan todeta, että vuoden 2011 lopussa 1253 henkilöä (97 %) oli suorittanut lopputestin, 19 henkilöä (1 %) oli tehnyt alkutestin ja 25 henkilöä (2 %) oli rekisteröitynyt koulutusympäristöön, mutta ei ollut aloittanut koulutuksen suorittamista lainkaan.

Vuoden 2011 lopussa koulutusympäristöön rekisteröitymättä ja koulutuksen suorittamatta olevia käyttäjätunnuksen omaavia työntekijöitä oli yhteensä 259.

Koulutuksen hyväksytysti suorittaneiden määrä oli 1093 työntekijää vuoden 2010 lopulla ja vuoden 2011 lopussa 1253 työntekijää. 2009 vuoden lopulla tehdyn käyttäjätunnustarkistuksen yhteydessä tunnuksia kaupungin tietoverkkoon oli yhteensä 1678 kappaletta. Tarkkaa arviota koulutuksen suorittamatta jättäneistä henkilöistä oli vaikea saada, koska isossa organisaatiossa henkilöstömäärä elää koko ajan.

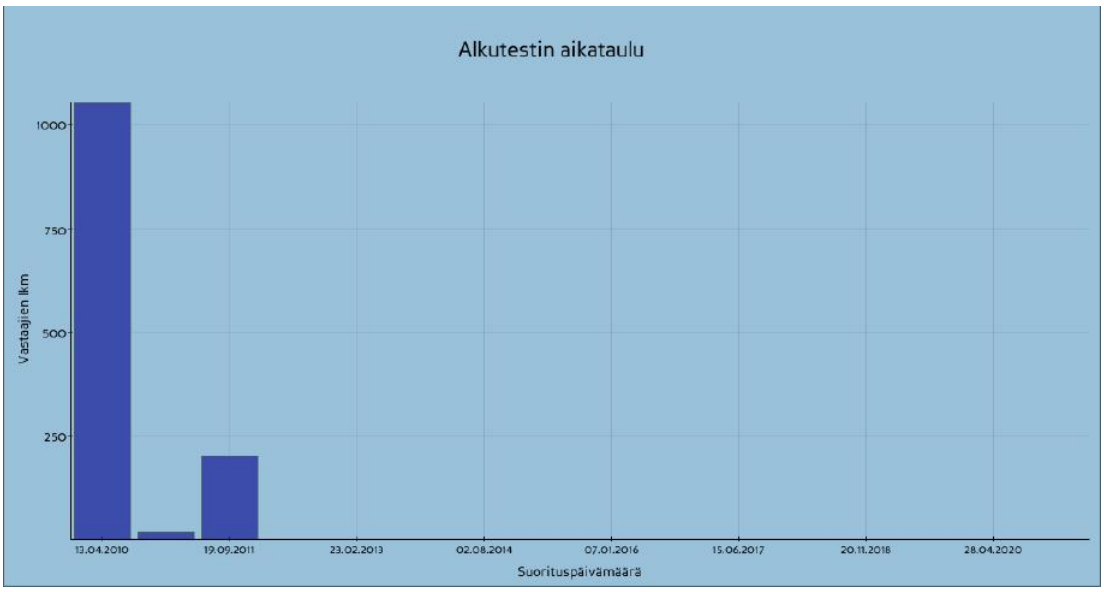
Seuraavassa taulukossa (Taulukko 1) näkyvät koulutusympäristöön rekisteröityneiden työntekijöiden tulokset organisaatiotasolla. Siinä näkyvät myös koulutuksen suorittaneiden henkilöiden lukumäärät ja prosenttiosuudet. Lisäksi siitä selviävät alku- ja lopputestin suorittaneiden keskiarviot prosentteina sekä koulutuksen lopputestissä hylättyjen määrät prosentteina. Taulukon ensimmäisessä sarakkeessa näkyy myös päivämäärä milloin koulutusympäristö on otettu käyttöön kussakin kaupungin organisaatioryhmässä.

Organisaatio / Toteutus	Hlö	Suoritti	Alku-testi KA	Lopputesti KA	Lopputesti hylättyjä*
Rovaniemi: Alaluokkien koulut / 2010-09-13	258	98 %	70 %	75 %	13 %
Rovaniemi: Hallinto / 2010-04-13	142	96 %	75 %	79 %	9 %
Rovaniemi: Liikelaitokset ja konserniyhtiöt / 2010-04-13	112	99 %	68 %	72 %	15 %
Rovaniemi: Lukiot / 2010-09-13	81	99 %	74 %	79 %	5 %
Rovaniemi: Muut koulut ja koulutoimisto / 2010-09-13	55	96 %	72 %	80 %	2 %
Rovaniemi: Tekninen tuotanto-osasto / 2010-04-13	174	93 %	63 %	67 %	27 %
Rovaniemi: Tuotantopalvelut / 2010-04-13	219	97 %	72 %	76 %	12 %
Rovaniemi: Yläluokkien koulut ja yhtenäiset perus-koulut / 2010-09-13	256	95 %	71 %	78 %	7 %
Yhteensä	1297	97 %	70 %	75 %	13 %

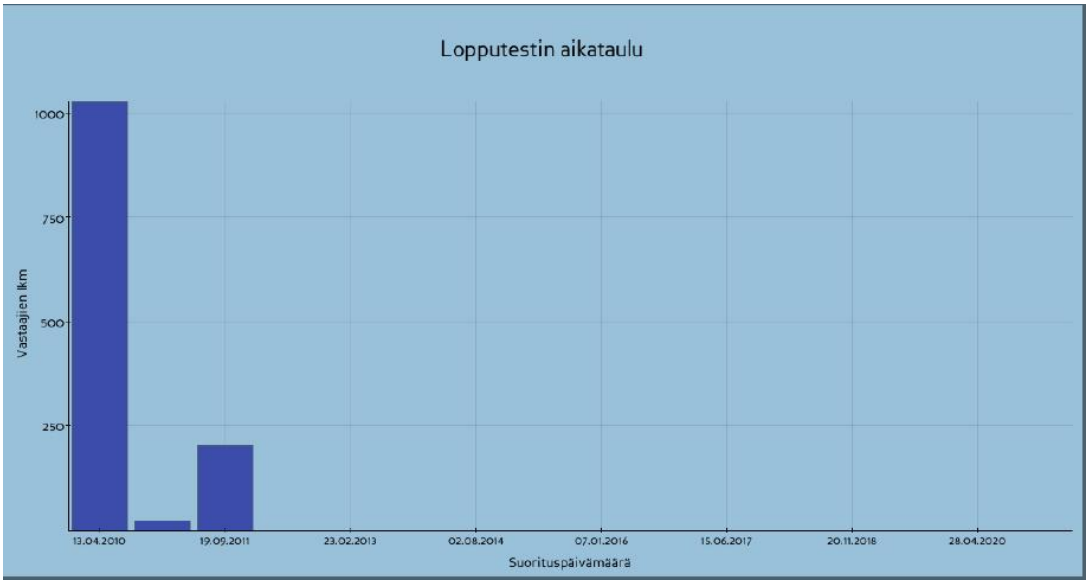
*) Hylättyjen osuus kaikista yrityksistä

Taulukko 1. Koulutusympäristöön rekisteröityneiden tulokset organisaatiotasolla

Alku- ja lopputestien suorittamisen aikataulun graafiset pylväät (Kuviot 3 ja 4) osoittavat vastaajien lukumäärät eri ajankohtina. Loppuraportin mukaan eniten suorituksia on ollut heti koulutusympäristöön rekisteröitymisen jälkeen sekä siinä vaiheessa, kun koulutusympäristö on muistuttanut käyttäjää koulutuksen suorittamisesta.

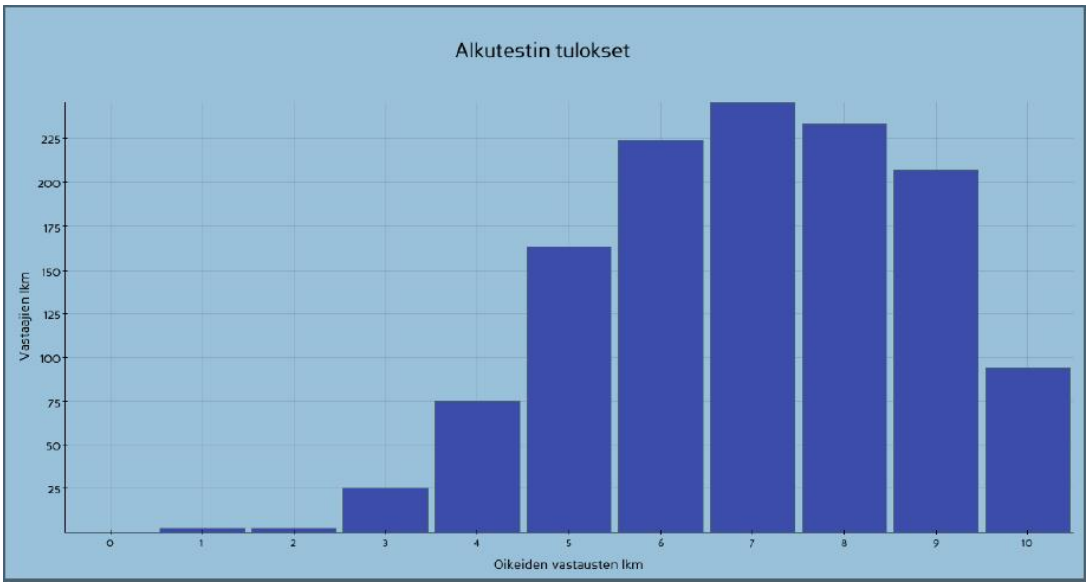


Kuvio 3. Alkutestin suorittamisen aikataulu



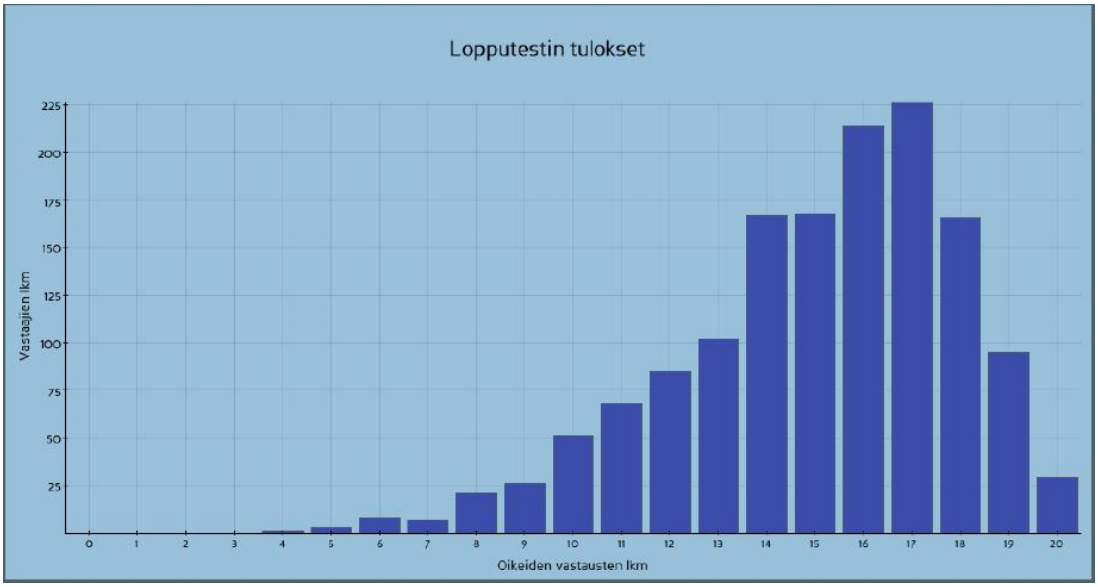
Kuvio 4. Lopputestin suorittamisen aikataulu

Seuraavissa alku- ja lopputestin tulosjakaumien graafisissa pylväissä (Kuviot 5 ja 6) verrataan oikeiden vastausten lukumäärää vastaajien lukumäärään siten, että kuinka moneen kysymykseen on lukumääräisesti vastattu oikein.



Kuvio 5. Alkutestin tulosjakauma pylväinä

Alkutestissä oli kymmenen kysymystä, joista kaikkiin vastasi oikein 94 henkilöä. Suurin osa eli 252 henkilöä vastasi oikein seitsemään alkutestin kysymykseen.



Kuvio 6. Lopputestin tulosjakauma pylväinä

Lopputestissä oli 20 kysymystä, joista kaikkiin vastasi oikein 29 henkilöä. Lopputestissä suurin osa eli 227 henkilöä vastasi oikein seitsemääntoista kysymykseen kahdestakymmenestä.

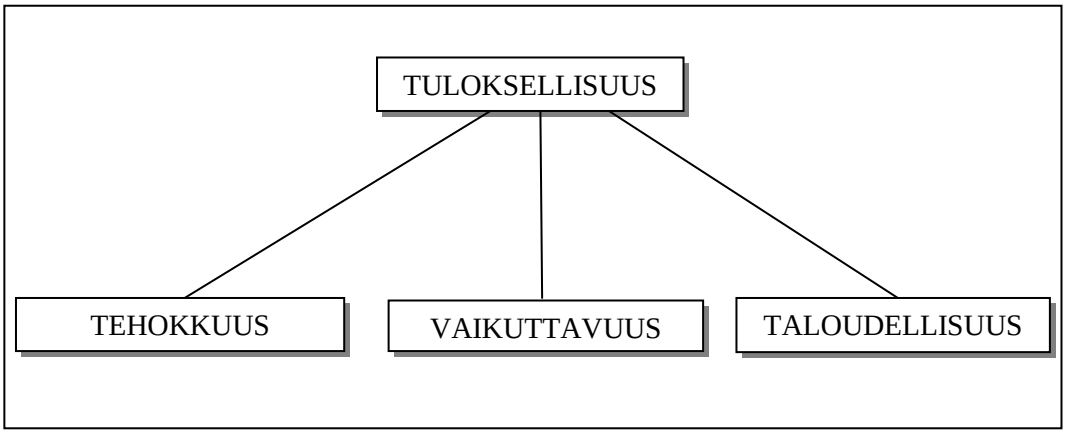
6 TIETOTURVAKOULUTUKSEN VAIKUTTAVUUDEN ARVIOINTI

6.1 Yleisesti arvioinnista

Erilaisissa yhteyksissä arvioinnilla tarkoitetaan erilaisia asioita, eikä arvioinnista ole mahdollista esittää yhtä yleistä tai yksiselitteistä määritelmää. Koulutustulosten tavoitteiden saavuttamisen ja onnistumisen arvioinnin mittaaminen on varsin haasteellista. Mielestäni sitä kuitenkin tulisi tehdä, jos arviointi on toiminnan kannalta tarkoituksenmukaista ja hyödyllistä. Tärkeintä ei niinkään ole se mitä menetelmiä siinä käytetään, vaan miten sen tuloksia pystytään hyödyntämään lyhyellä tai pitkällä aikavälillä, suoraan tai välillisesti käytännön työtä kehitettäessä.

Tietoturvakouluttajan oppaassa (VAHTI 11/2006, 39) sanotaan, että koulutuksen arviointi on haasteellista myös siitä syystä, että arviointi voi kohdistua monelle tasolle, eivätkä käytetyt mittarit välttämättä kerro sitä mitä halutaan mitata. VAHTI:n (2006, 39) mukaan tietoturvakoulutusten hyödyllisin mittari olisi selvittää, miten hyvin tiedot, taidot ja asenteet näkyvät käytännön työtehtävissä koulutuksen jälkeen. Muita mittareita voisivat olla esimerkiksi tietoturvavahinkojen tilastointi ja määrämuotoinen arviointi. Palautetta on syytä kuitenkin pyytää ja arviointia suorittaa, ainakin mikäli on aikomus muuttaa asioita sen perusteella.

Valtionhallinnossa on tuloksellisuuden arviointijärjestelmän pohjalta laadittu opetushallintoa varten tuloksellisuuskäsite. (Opetushallitus 1998, 19.) Tuloksellisuuskäsitettä (Kuvio 7) vapaasti mukaillen: koulutus on ***tuloksellista*** silloin, kun organisaation ja yksilön oppimiselle asetetut tavoitteet on saavutettu. ***Tehokasta*** se on silloin, kun opetusjärjestelyjen toimivuus, joustavuus ja ajoitus ovat mahdollisimman tarkoituksenmukaiset ja opetuksen laatu on hyvä. ***Vaikuttavaa*** silloin, kun sen tuottamat tulokset laadullisesti ja määrällisesti edistävät yksilön henkistä kasvua sekä yhteiskunnan, kulttuurin ja työelämän kehitystä. ***Taloudellista*** se on puolestaan silloin, kun resurssit on kohdistettu tavoitteiden kannalta optimaalisesti ja resurssien määrä on tarkoituksenmukainen. (Opetushallitus 1998, 20 – 21.)



Kuvio 7. Tuloksellisuuskäsite (Opetushallitus 1998, 20)

Tässä arvioinnissa on tarkoitus selvittää tietoturvakoulutukseen osallistujien omia mielikuvia tietoturvakoulutuksen toteutuksesta, käytettävyydestä, sisällöstä ja sen vaikuttavuudesta yksilön tietoturvakäyttäytymisen muutokseen. Tavoitteena on lisäksi selvittää, miten koulutuksen toteutus oli onnistunut ja miten tietojen, taitojen ja tietoturvatietoisuuden kehittyminen on muuttunut toteutetun koulutuksen myötä.

6.2 Arviointimenetelmästä

Arviointi toteutettiin 5. – 9.11.2012 välisenä aikana. Arviointi toteutettiin verkkokyselynä Webropol analysointi- ja kyselytyökalun avulla. Arvioinnin kohteena olivat kaikki Rovaniemen kaupungin ja sen liikelaitosten työntekijät, jotka olivat suorittaneet tietoturvakoulutuksen hyväksytysti vuosien 2010 - 2012 välisenä aikana. Vastaajille lähetettiin sähköpostilla linkki kyselyyn ja vastausaikaa oli viisi päivää.

Arviointikysely koostui kolmesta eri sivusta, jossa ensimmäisellä sivulla kysyttiin vastaajien taustatietoa. Taustatietokysymykset olivat pääsääntöisesti vaihtoehto- tai monivalintakysymyksiä. Kysymyksistä neljä ensimmäistä olivat pakollisia. Arviointikyselyn toinen sivu keskittyi tietoturvakoulutusympäristön käytettävyyden, sisällön sekä vaikuttavuuden arviointiin. Näissä kysymysryhmissä oli mahdollista antaa arvio kysymyksiin vaihtoehtovastauksella, jotka määriteltiin ja arvotettiin seuraavasti: en osaa sanoa = 1, täysin eri mieltä = 2, osittain eri mieltä = 3, osittain samaa mieltä = 4, täysin samaa mieltä = 5. Kolmannella sivulla vastaajilta pyydettiin sanallisia kommentteja ja arvioita, jotka arvioinnin tuloksissa on käsitelty pääosin kohdassa 6.3.6. Tietoturvakoulutuksen kehittäminen.

Kysely lähetettiin 1237 henkilölle ja heti tämän jälkeen tuli sähköpostijärjestelmän kautta viesti, että 152 henkilön sähköpostiosoite ei ole voimassa. Tämä tarkoitti käytännössä sitä, että kyseiset henkilöt eivät olleet enää kaupungin palveluksessa tai olivat virka- tai työsuhdevapaalla. Tämän jälkeen poistin heidän osoitteensa vastaajaryhmästä ja lopullisia kutsuja kyselyyn lähti 1085. Kyselyyn vastasi yhteensä 224 Rovaniemen kaupungin palveluksessa olevaa henkilöä.

Vastaajien määrä vaihtelee hieman kysymyksittäin, sillä vastaaminen oli pakollista vain neljässä ensimmäisessä taustatietokysymyksessä.

Tulosten arvioinnin olen jakanut kyselyn mukaisesti alaotsikoihin, joissa tarkastelen ja arvioin kyselyn tuloksia kunkin sivun kysymysryhmän keskeisempien tulosten näkökulmasta. Tarkemmat tulokset löytyvät tämän opinnäytetyön liitteenä.

6.3 Arvioinnin tulokset

6.3.1 Taustatiedot vastaajista

Kyselyyn vastasi yhteensä 224 henkilöä. Vastausprosentti kaikista kyselykutsun saaneista oli 20,6 %. Vastaajista 55,8 % oli naisia ja 44,2 % miehiä. Vastaajista valtaosa (61,6 %) oli iältään 50 vuotta tai enemmän. Vastaajista vain 8,0 % oli alle 35-vuotiaita. Loput 30,4 % vastaajista sijoittui ikäryhmään 35 - 49 vuotta. Taustatiedoissa kysyttiin myös mihin henkilö sijoittui Rovaniemen kaupunkiorganisaatiossa. Lähes puolet (47,8 %) kyselyyn vastanneista työskentelee sivistyspalvelujen tuotanto-osastolla.

Vastaajista suurin osa (87,1 %) oli tietoinen Rovaniemen kaupungille laaditusta tietoturvapolitiikasta sekä siihen liittyvistä ohjeistuksista. Henkilöstö myös tiesi mistä ohjeet löytyvät.

Rovaniemen kaupungin kaikilla työntekijöillä ei ole käytössään henkilökohtaista työasemaa. Verkkokoulutusympäristö mahdollisti koulutuksen suorittamisen myös muualla kuin työpaikalla. Siitä huolimatta lähes kaikki (83,3 %) olivat suorittaneet koulutuksen työpaikalla. Vain 7,3 % vastaajista oli suorittanut koulutuksen muualla kuin työpaikalla.

Ennen varsinaisen koulutuksen järjestämistä, tehtiin koulutustestausta muutamien käyttäjien kanssa ja tässä vaiheessa arvioitiin myös keskimääräistä aikaa, joka koulutuksen suorittamiseen meni. Testausvaihe osoitti, että koulutuksen suorittamiseen meni aikaa yhdestä kahteen tuntiin. Myös arviointi tuki tätä näkemystä, koska 40,7 % vastaajista vastasi käyttäneensä koulutukseen aikaa yhdestä kahteen tuntiin. Huomionarvoista tässä on silti, että yli puolet (50,2 %) vastaajista oli suorittanut koulutuksen alle tunnissa.

Taustatiedoissa haluttiin myös selvittää oliko vastaaja saanut tukea ja perehdytystä koulutuksen suorittamiseen ja jos oli, niin keneltä hän oli saanut tukea ja perehdytystä. Tuen määrän riittäväksi arvioi 26,5 % vastaajista. 29,6 % vastaajista oli saanut jonkin verran tukea ja 39,0 % vastaajista ilmoitti, ettei ollut saanut lainkaan tukea koulutuksen suorittamiseen.

Vastaajat ilmoittivat saaneensa tukea niin esimieheltä (20,4 %) kuin työkavereiltaan (32,2 %). Koska vastaajaryhmässä on mukana myös esimiehiä/ryhmävastaavia, on perehdytystä saatu myös ryhmävastaaville järjestetyistä infotilaisuuksista. Usealle myös kirjalliset ohjeet olivat olleet riittävä tuki- ja perehdytysmateriaali aiheeseen. Kysymyksessä oli mahdollista valita useampi vastausvaihtoehto, joten prosenttimäärien yhteenlaskettu arvo oli yli sata.

Seuraavaksi kysyttiin keneltä tai mistä vastaaja oli saanut tietoa koulutuksen suorittamisesta. Myös tässä kohtaa oli mahdollista valita useampi vastausvaihtoehto, joten prosenttimäärien yhteenlaskettu arvo oli yli sata. Koulutuksen suorittamisesta tiedotettiin muun muassa kaupungin intranetissä ja infotilaisuuksissa. Osalle henkilöstöä lähetettiin myös henkilökohtaista sähköpostia. 49,1 % vastaajista oli saanut tiedon esimieheltään, 48,2 % vastaajista tiedotteesta työpaikallaan tai intranetissä, 7,2 % vastaajista ilmoitti saaneensa tiedon muualta, kuten esimerkiksi vastaajan sähköpostiin tulleesta kehotuksesta koulutuksen suorittamiseen.

Lopuksi taustatiedoissa vielä pyydettiin vastaajia kertomaan, miksi he olivat suorittaneet koulutuksen. Vastausvaihtoehtoina oli, että vastaaja koki asian tärkeäksi, esimies tai joku muu edellytti tai jokin muu syy ja mikä se oli. Myös tässä kysymyksessä oli mahdollista valita useampi vastausvaihtoehto, joten prosenttimäärien yhteenlaskettu arvo oli yli sata. Koska koulutus oli pakollis-

ta, oli suurin osa vastaajista (60,3 %) luonnollisesti vastannut suorittaneensa koulutuksen, koska esimies tai joku muu edellytti. Siitä huolimatta myös melkein puolet (45,5 %) vastaajista oli myös vastannut suorittaneensa koulutuksen, koska oli kokenut asian tärkeäksi.

6.3.2 Tietoturvakoulutusympäristön käytettävyys

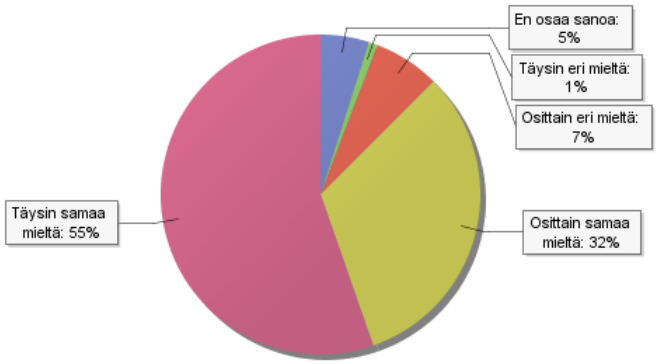
Kansainvälinen standardointijärjestö (ISO) määrittelee standardissaan ISO 9241 käytettävyyden kokonaisuudeksi, jolla voidaan kuvata kuinka hyvin käyttäjät pystyvät käyttämään käyttämiään työvälineitä tietyssä ympäristössä tiettyjen työtehtävien suorittamiseen, jotta he saavuttavat tavoitteensa. Käytettävyydestä puhuttaessa voidaankin tässä yhteydessä puhua ihmisen ja koneen vuorovaikutuksesta. Englanninkielessä termin käytettävyys (usability) kulkeekin usein termi ihminen-tietokone (Human-Computer Interactio, HCI), kun puhutaan sovellusten käytettävyydestä. (Kuutti 2003, 12 - 15.)

Käytettävyyden arvioinnin tavoitteena on mitata, kuinka käyttökelpoinen jokin järjestelmä on sitä käyttävälle ihmiselle. On mahdollista, että käyttöön liittyy usein joukko ihmisen tietoisia ja tiedostamattomia tarpeita, joita hän pyrkii järjestelmän avulla tyydyttämään. Tarpeiden huomioiminen on tärkeää, mikäli halutaan arvioida järjestelmän todellista käyttökelpoisuutta. (Mielonen – Hintikka 1998, 12.)

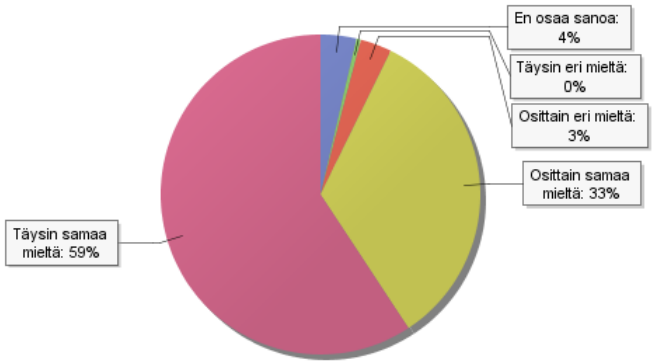
Mielosen ja Hintikan (1998, 12) mukaan käytettävyysarviointi olisi tehtävä niiden käyttäjien kanssa, jotka käyttävät järjestelmää tiettyjen tehtävien suorittamiseen. Arvioinnissa voitaisiin näin huomioida kuinka helposti, nopeasti, virheittä ja vaivattomasti järjestelmän käyttö onnistuu suhteessa tavoitteisiin.

Käytettävyyttä voidaan arvioida useilla eri menetelmillä. Käytetyin ja tunnetuin näistä lienee Nielsenin 10 heuristisen säännön kokoelma (Kuutti 2003, 49). Tässä työssä ei ole kuitenkaan tarkoitus arvioida käytettävyyttä tieteenalan tai suunnittelun näkökulmasta, vaan käytettävyyttä arvioidaan siitä näkökulmasta, miten vastaajat kokivat koulutusympäristön käytön. Vastaajilta kysyttiin muun muassa kuinka he kokivat koulutusympäristöön rekisteröitymisen, siihen kirjautumisen sekä siellä navigoinnin. Lisäksi kysyttiin, olivatko vastaajat löytäneet koulutusympäristön käyttöön laaditut ohjeet helposti.

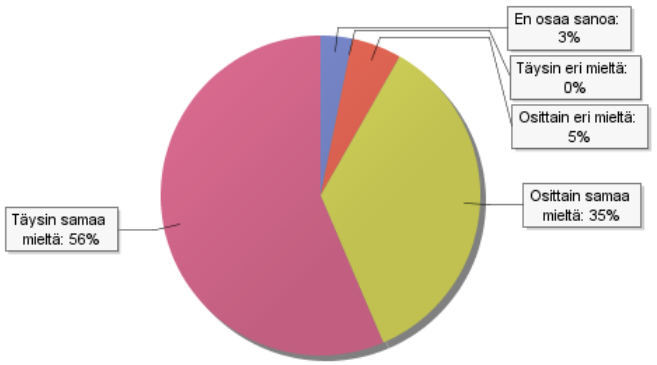
Seuraavissa kuvioissa (Kuviot 7, 8, 9 ja 10) näkyvät käytettävyyden eri osa-alueiden arvioinnin vastausprosentit. Jokaisen osa-alueen kysymyksissä vastaajat olivat pääsääntöisesti täysin samaa mieltä tai osittain samaa mieltä. Tästä voidaan päätellä, että lähes 90 % vastaajista oli sitä mieltä, että koulutusympäristö oli helppokäyttöinen eikä koulutusympäristön käytettävyyden suhteen näin ollen ollut ongelmia.



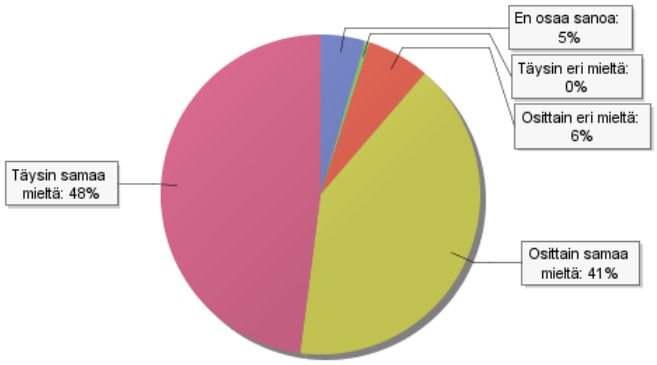
Kuvio 7. Koulutusympäristöön rekisteröityminen oli vaivatonta



Kuvio 8. Koulutusympäristöön kirjautuminen oli vaivatonta



Kuvio 9. Koulutusympäristössä navigointi oli vaivatonta

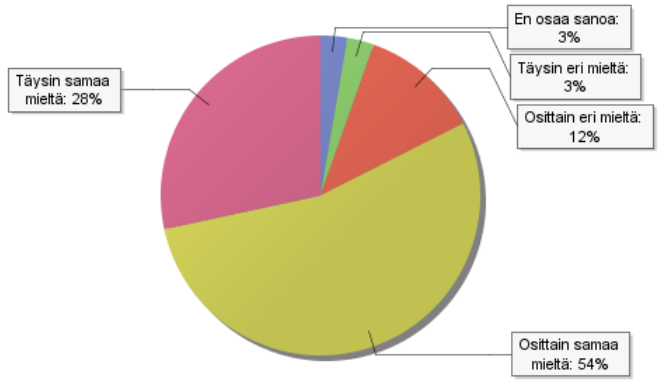


Kuvio 10. Koulutusympäristön ohjeet löytyivät vaivattomasti

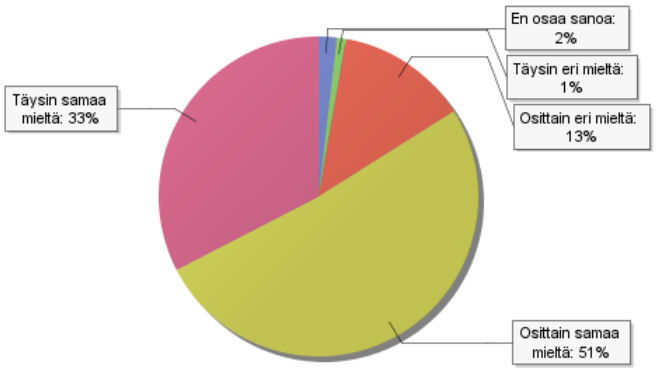
6.3.3 Tietoturvakoulutuksen sisältö

Tässä kysymysryhmässä vastaajia pyydettiin arvioimaan tietoturvakoulutuksen sisältöä ja siinä oli keskeistä myös arvioida tukivatko opetusmateriaali ja -menetelmät vastaajan oppimista. Vastaajia pyydettiin arvioimaan seuraavia osa-alueita: koulutusmateriaalin ymmärrettävyys ja luettavuus, koulutusmateriaalissa esiintyneet käsitteet ja esimerkit, koulutusmateriaalin teoriaosuuden hyöty alku- ja lopputestissä esitettyihin kysymyksiin sekä koulutusmateriaalin ja opetusmenetelmien hyöty henkilön oppimiselle.

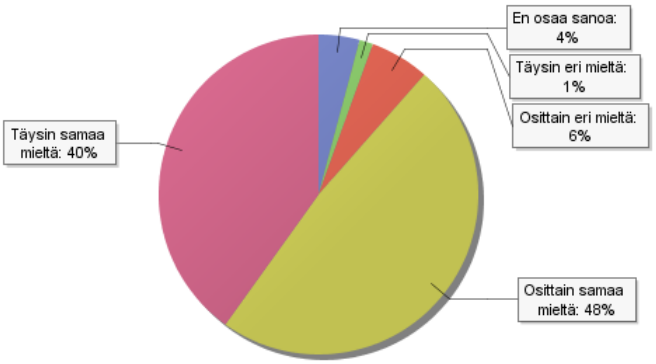
Myös tämän kysymysryhmän osa-alueiden vastaustuloksista (Kuviot 11, 12, 13, 14 ja 15) voidaan päätellä, että vastaajat olivat pääsääntöisesti sitä mieltä, että opetusmenetelmät olivat olleet tarkoituksenmukaisia ja koulutusmateriaalin oli sisältö selkeää. Koska sisältö oli räätälöity Rovaniemen kaupungin työntekijöille, saatiin koulutuksen aikana myös tästä positiivista palautetta.



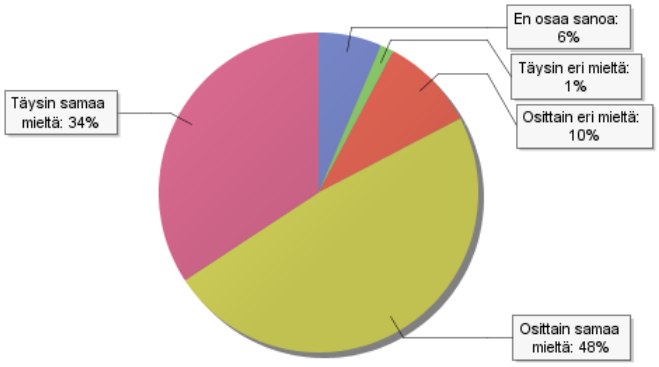
Kuvio 11. Koulutusmateriaali oli selkeää ja helppolukuista



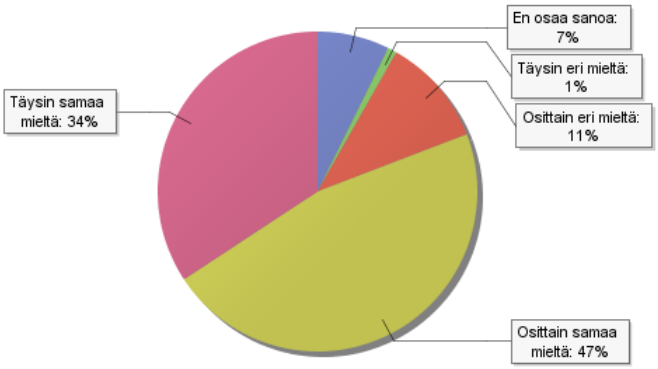
Kuvio 12. Ymmärsin koulutusmateriaalissa olevat käsitteet tai löysin niille tarvittaessa selityksen sanastosta



Kuvio 13. Koulutusmateriaalissa esiintyneet esimerkit auttoivat ymmärtämään käsiteltävän asian paremmin



Kuvio 14. Löysin koulutusmateriaalin teoriaosuudesta vastaukset alku- ja lopputestin kysymyksiin



Kuvio 15. Koulutusmateriaali ja opetusmenetelmät tukivat oppimistani

6.3.4 Asennoituminen tietoturvakoulutusta kohtaan

Tässä kysymysryhmässä oli tavoitteena arvioida koulutuksen tarkoituksenmukaisuutta ja henkilön motivaatiota koulutuksen suorittamiseen, joka vaikuttaa olennaisesti asennoitumiseen koulutusta kohtaan.

Nykänen (2011, 21) korostaa ihmisen henkilökohtaisen asenteen ja motivaation vaikutusta tietoturvaan sitoutumisessa. Tämä tulisi ottaa huomioon koulutuksen suunnittelussa. Mikäli koulutus ei sisällä selkeästi työntekijän omiin työtehtäviin liittyviä oheistuksia ja toimintamalleja, hän ei välttämättä myöskään ymmärrä niiden sisältöä suhteessa omiin työtehtäviin. Henkilön on usein vaikea ymmärtää tietoturvan merkitystä, jos jokapäiväiset käytännöt ovat liian kaukana ohjeistuksista (Nykänen 2011, 22). Nykäsen (2012, 23) mukaan koulutuksen asiakokonaisuuden sitomisella henkilökohtaisiin työtehtäviin on todettu olevan merkittävä vaikutus henkilöstön motivaatioon ja asennoitumiseen koulutukseen ja sen kautta tietoturvakäyttäytymisen muutokseen.

Mielestäni yksi kyselyyn vastanneista kiteytti asennoitumisen merkitystä tietoturva-asioihin varsin osuvasti: *”Kuulee monesti sanottavan, että pitäisi olla vain yksi salasana, jolla pääsee kaikkiin, ohjelmiin, mihin on oikeudet. Ovien sulkemisesta ja esim. kannettavien salauksesta kuulee vieläkin sanottavan, että miksi pitää olla niin monta salasanaa, kuka näitäkin tarvitsee ja julkisia asioitahan käsittelemme??? ASENNE KOHDALLEEN.”*

Motivaatioon liittyy myös olennaisesti kannustaminen ja palautteen saaminen. Mikäli työntekijä saa palautetta ja häntä kannustetaan, niin todennäköisesti hän on myös motivoituneempi koulutuksen suorittamiseen. Vaikka lähes

80 % vastaajista (Kuviot 16 ja 17) oli motivoitunut ja koki koulutuksen hyödylliseksi työlleen, silti lähes puolet vastaajista koki, etteivät he olleet saaneet riittävästi kannustusta ja palautetta suoritetusta koulutuksesta (Kuvio 18).

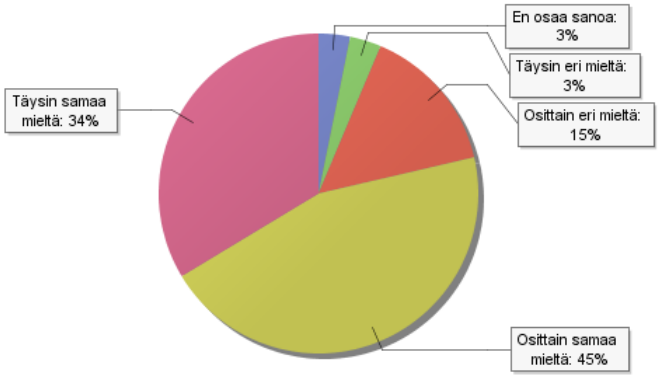
Tämä kävi ilmi myös vapaapalautekysymyksen kohdalla, jossa vastaajilta kysyttiin, että minkälaista palautetta vastaaja toivoisi saavansa koulutuksen suorittamisesta. Usea vastaaja olisi toivonut esimieheltä saatua palautetta. Tämä käy hyvin ilmi myös seuraavista vastaajien vapaapalautteista:

”Lähinnä esimieheltä jonkinlaista huomiointia asian suhteen. Tulisi olo että asia on tärkeä kun siitä esimiehen kanssakin puhuttaisiin/käsiteltäisiin.”

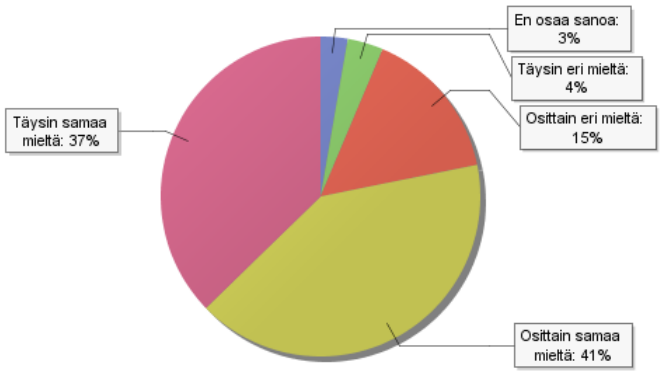
”Kahvitunnilla kyllä keskusteltiin, mutta ei missään virallisesti todettu, että hyvä homma, nyt me osataan.”

”Olisi ollut kiva, jos esimies olis edes kuitannut saamansa tiedon, että olin suorittanut kurssin”

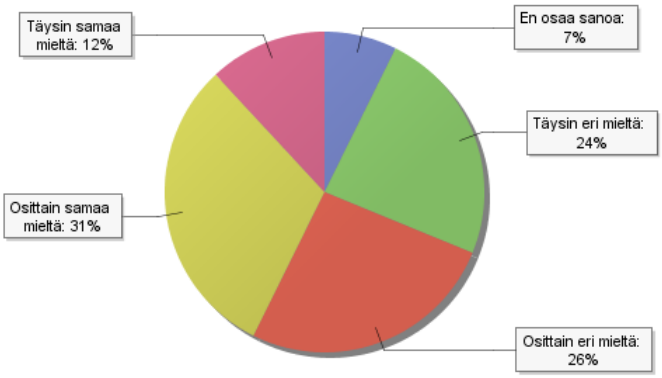
”Lähiesimies antaisi palautteen ihan livenä. Pelkkä softan antama kiitos on turhan kliininen.”



Kuvio 16. Olin motivoitunut koulutuksen suorittamiseen



Kuvio 17. Koulutus oli tarkoituksenmukaista työlleni



Kuvio 18. Minua kannustettiin ja sain palautetta koulutuksen suorittamisessa

6.3.5 Tietoturvakoulutuksen vaikuttavuuden arviointi

Koulutuksen vaikuttavuuden alalla tunnetuin ja käytetyin arviointimalli on Donald Kirkpatrickin (1996) nelivaiheinen malli koulutuksen vaikuttavuudesta. Kirkpatrickin (1996, 54 – 59) mukaan voidaan koulutus jakaa mallin mukaisesti neljään vaiheeseen, joista jokaista voidaan arvioida:

1. Reaktioiden arviointi, jossa arvioidaan millaisia kokemuksia ja tuntemuksia koulutuksesta saatiin.
2. Oppimisen ja osaamisen arviointi, jossa arvioidaan koulutuksessa opittua ja osaamisen tai asenteiden muuttumista.
3. Toiminnan arviointi, jossa arvioidaan miten opittu asia on muuttanut työkäyttäytymistä.
4. Tulosten ja vaikutusten arviointi, jossa arvioidaan mitä vaikutuksia koulutuksella on ollut organisaation taloudellisiin, toiminnallisiin tai laadullisiin tuloksiin.

Tietoturvakoulutuksen vaikuttavuuden arviointiin olin laatinut kysymysryhmään useita eri kysymyksiä, jolla koulutuksen vaikuttavuutta voidaan ainakin osittain arvioida. Tämän kysymysryhmän kohdalla oli myös havaittavissa eniten eroavaisuuksia vastausten suhteen.

Kolmen ensimmäisen kysymyksen vastausten osalta (Kuviot 19. 20. ja 21.) voidaan päätellä, että reilusti yli puolet vastaajista oli sitä mieltä, että koulutus oli ainakin osittain vaikuttanut päivittäisiin tietoturvaan liittyviin toimintatapoihin. Vastaajat myös kokivat osaamisensa ja tietoturvatietoisuutensa kehittyneen koulutuksen myötä. Tästä voidaan päätellä että koulutuksesta on ollut hyötyä ja vaikutusta koko organisaation tietoturvan kehittymiselle.

”Tietoturvakoulutukset ovat tärkeitä, vanhan jo tiedossakin olevan tiedon tärkeys korostuu, tietoturva-asiat eivät ole koskaan liikaa esillä.”

Osa vastaajista kuitenkin koki, että koulutuksesta ei ollut hyötyä tai että koulutuksessa käydyt asiat olivat jo entuudestaan tuttuja ja näin ollen koulutus ei tuonut lisäarvoa työntekijän työn kannalta.

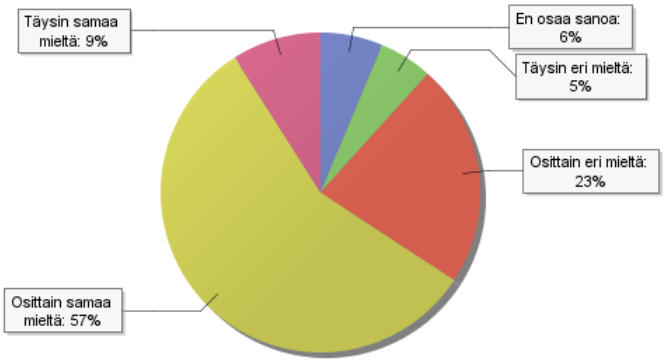
”Nyt koulutus oli vähän läpihuutojuttu”

”Itselle koulutus sinänsä ei tuonut uutta asiaa, mutta on hyvä että koulutusta järjestetään. Voisiko koulutuksen uusijoilla olla vaikeampia tehtäviä, kuin ekakertalaisella? Se voisi lisätä kiinnostusta koulutukseen, kun joutuu jotain miettimään eikä vaan kertaamaan.”

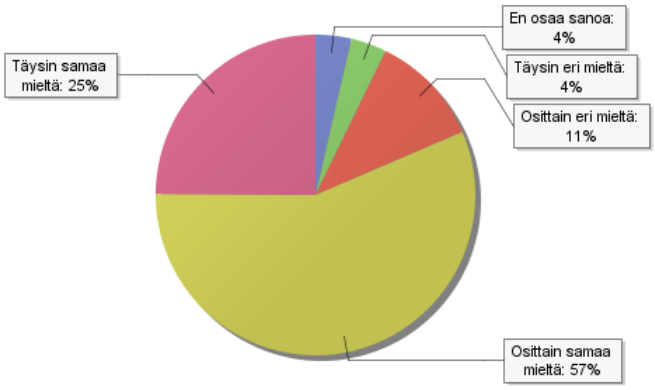
Kohdassa 14. olin monessa kohdin täysin eri mieltä, koska asiat olivat jo entuudestaan tuttuja, joten uutta ei paljoakaan tullut.”

”Koulutuksesta on sen verran aikaa, etten kykene muistamaan materiaaliin liittyviä yksityiskohtia kovin tarkasti. Suuri osa asiasta oli joka tapauksessa jossain määrin tuttua, eikä materiaalin silmäilyyn ja testin tekemiseen kulunut kovin paljon aikaa. Koulutuksen suorittaminen ei juuri rasittanut, mutta ei myöskään tarjonnut paljoakaan uutta työn kannalta.”

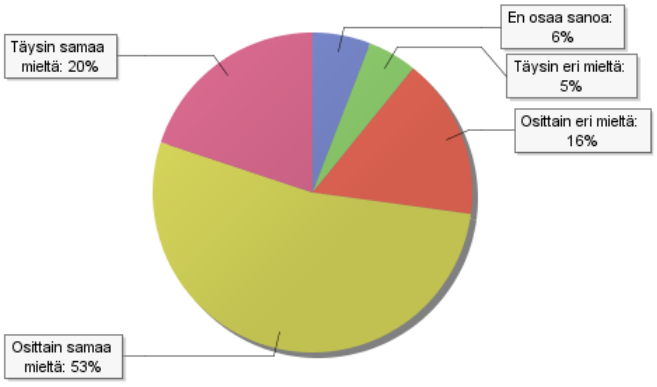
”Koulutus hyvä, mutta minulla oli osaaminen jo ennen koulutusta.”



Kuvio 19. Koulutus vaikutti päivittäisiin tietoturvaan liittyviin toimintatapoihini



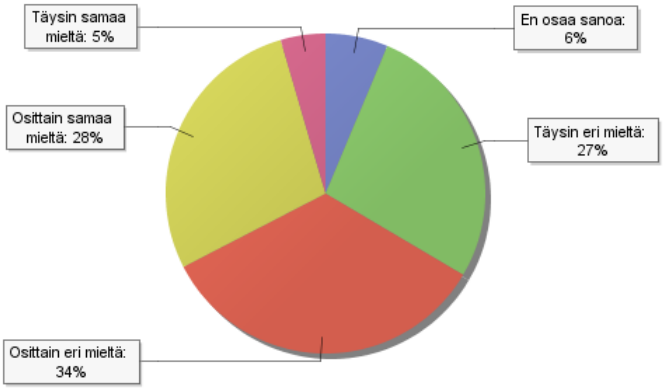
Kuvio 20. Koin oppineeni uutta tietoturvaan liittyvistä asioista



Kuvio 21. Koulutus edisti omaa tietoturvatietoisuuttani ja osaamiseni kehittyi koulutuksen myötä

Kysyttäessä onko vastaajalla ollut riittävästi aikaa kokeilla ja soveltaa uusia tietoturvakäytänteitä työssään, vain 5 % vastaajista oli täysin samaa mieltä ja 28 % vastaajista osittain samaa mieltä (Kuvio 22). Tämä kertoo varmasti paljonkin nykyyhteiskunnan työn vaatimusten lisääntymisestä, jossa työelämän kiire ja hektisyys ovat nousseet yhä keskeisemmiksi ilmiöiksi. Kuitenkin tämä herättää myös kysymyksen, onko työyhteisössä, töiden organisoinnissa, organisaation toimintatavoissa

tai johtamisessa muutoksen paikka? Organisaation ylin johto ja esimiehet toimivat suunnannäyttäjinä ja esimerkkinä tietoturvakulttuurin luomisessa ja tietoturvallisuuden huomioiminen ja johdon sitoutuminen on osa hyvin johdettua organisaatiokulttuuria.



Kuvio 22. Työssäni on riittävästi aikaa kokeilla ja soveltaa uusia tietoturvakäytänteitä

Kysyttäessä onko koulutuksesta ollut hyötyä tai lisäarvoa vastaajan työyhteisölle ja sen tietoturvan kehittämiselle, huomioni kiinnittyi vastaajaryhmään en osaa sanoa, joita oli 14 % vastaajista (Kuvio 23). Oletettavasti tämä kertoo siitä, että työyhteisössä ei ole ylipäänsä herännyt keskustelua koulutuksen suorittamisesta tai sen vaikutuksista toimintatapojen muutokseen. Myös seuraavat vapaapalautteet antavat viitteitä, että keskustelua ei ole syntynyt, mutta opeteltavien asioiden käsittely yhteisesti organisaation omassa työyksikössä olisi hyödyllistä ja toivottavaa.

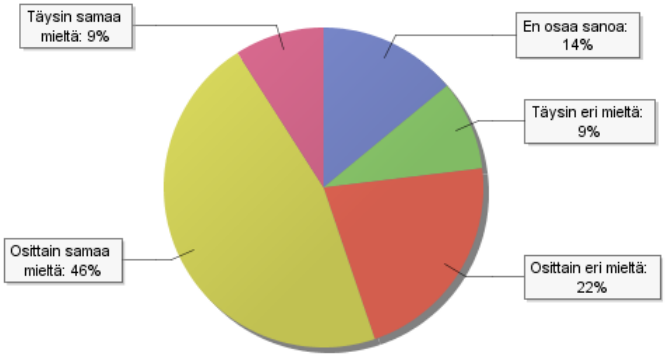
”Koulutuksen jälkeen ydinasioita ja palautetta juuri meidän yksikkömme työssä olisi ollut hyvä käydä läpi henkilöstön yhteisenä koulutusteemana.”

”Oman esimiehen kohdalla ei tullut mitään tietoa ko asiasta. Enkä edes tiedä miten omassa työyksikössäni koulutus suoritettiin. Palautteen käsittely työyksikön kanssa yhdessä olisi hyvä ja toivottava parannus. Olin etulyöntiasemassa koska olin mukana käynnistysvaiheessa, mutta jos en olisi ollut niin kysely olisi tullut ns. puun takaa.”

”Kahvitunnilla kyllä keskusteltiin, mutta ei missään virallisesti todettu, että hyvä homma, nyt me osataan.”

”Verkkokoulutuksen jälkeen palaute kuinka työyhteisö / osasto pärjäsi.”

”Keskustelua yhdessä siitä mitä tuli tehtyä.”



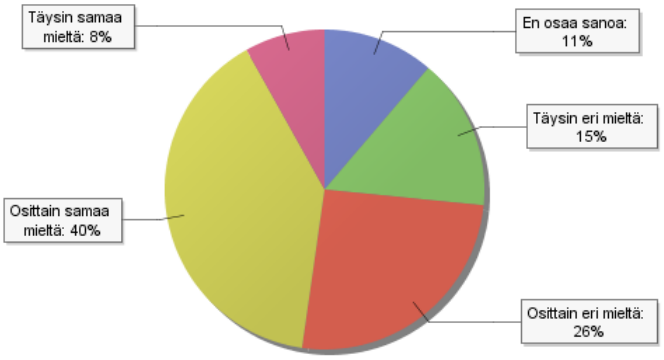
Kuvio 23. Koulutuksesta on ollut lisäarvoa työyhteisölleni ja sen tietoturvan kehittämiselle

Jo tekemässäni yhteenvedossa, totesin, että verkkokoulutusympäristö oli tarkoituksenmukainen niille henkilöille, jotka käyttävät tietokonetta pääsääntöisesti työvälineenään. Myös kyselyssä lähes puolet vastaajista arvioi koulutuksen tuoneen lisää haasteita tietotekniikan käytön suhteen (Kuvio 24). Kaupungilla on myös paljon työtehtäviä, joissa tietokoneen käyttö on vähäistä ja verkkokoulutuksen suorittaminen voi olla haasteellista niille työntekijöille, jotka eivät ole tottuneet tietokoneella työskentelyyn. Tämä käyttäjäryhmä tulee ottaa tulevaisuudessa huomioon ja järjestää tietoturvakoulutusta heille tarkoituksenmukaisella tavalla.

”Henkilöstöä tulisi kannustaa parantamaan tietoteknisiä valmiuksiaan ja taitojaan tukemalla nykyistä enemmän omaehtoista kouluttautumista kursseilla tai oppilaitoksissa. Nykyinen systeemi ei kannusta opiskelemaan.”

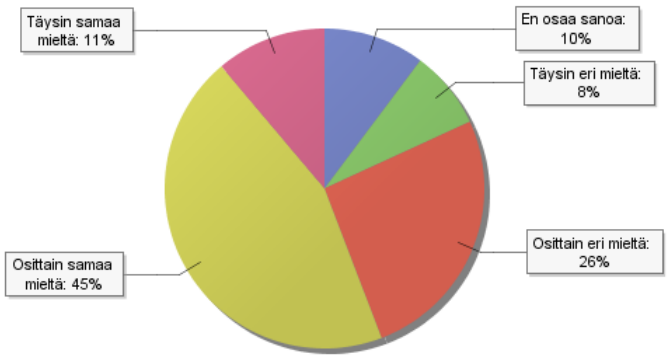
”Tietoturvakoulutus on tarpeellinen asia. Pitäisi kuitenkin muistaa, että kaikki käyttäjät eivät ole "nörttejä" eivätkä välttämättä osaa kaikkia temppuja, joten opetus pitäisi olla sellaista, että välillä käytettäisiin rautalankaa...”

”Monet pitivät kyselyä hankalana ja kiusallisena ja jotkut jopa toivoivat jonkun muun suorittavan sen puolestaan. Ihmiset jotka käyttävät vähän tietokonetta on vaikea omaksua edes perusasioita, kuten tallentamista ja siirtymistä toiselle sivulle.”

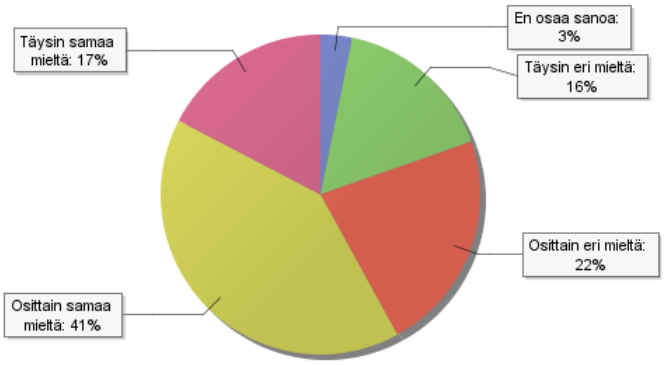


Kuvio 24. Koulutus toi lisää haasteita tietotekniikan käytön suhteen

Kysyttäessä vastaajilta, oliko koulutus tuonut uusia ajatuksia tai uhkakuvia esille henkilön työtä ajatellen tai ovatko salasanan hallintaan liittyvät käytänteet muuttuneet, osittain tai täysin samaa mieltä oli 58 % vastaajista (Kuviot 25 ja 26). Vastaajista reilu kolmasosa oli sitä mieltä, että koulutus ei ole tuonut uusia ajatuksia tai uhkakuvia vastaajan työhön liittyen tai vaikuttanut salasanakäytänteisiin tai niiden huomioimiseen.

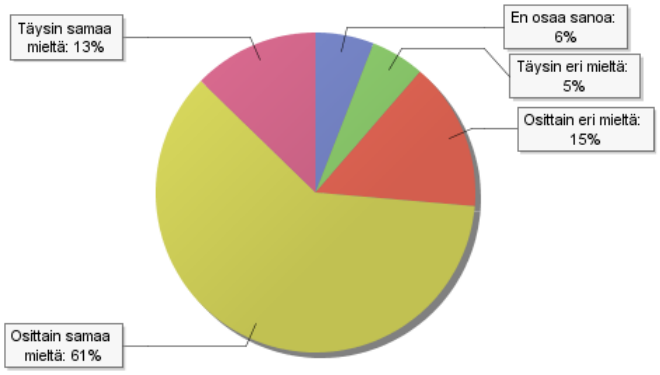


Kuvio 25. Koulutus toi uusia ajatuksia tai uhkakuvia esille työtäni ajatellen

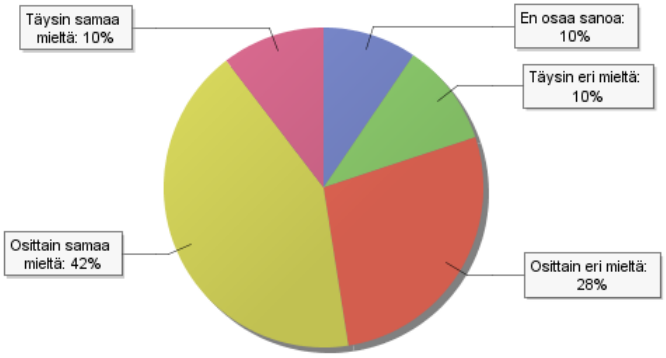


Kuvio 26. Salasanani hallintaan liittyvät käytänteet ovat muuttuneet tai kiinnitän niihin nykyään enemmän huomiota

Oppimisen ja tietoturvakoulutuksen vaikuttavuuden ja merkittävyyden kannalta seuraavat kaksi kuviota (Kuviot 27 ja 28) havainnollistavat hyvin, että koulutuksesta on ollut ainakin osittain hyötyä organisaation tietoturvatietoisuuden kehittymiselle. 74 % vastaajista oli osittain tai täysin samaa mieltä, että hän tunnistaa koulutuksen jälkeen paremmin tietoturvaan liittyviä epäkohtia tai uhkakuvia ja jopa 52 % arveli osaavansa perehdyttää uuden työntekijän tietoturva-asioihin koulutuksen suoritettuaan.



Kuvio 27. Tunnistan nykyään paremmin tietoturvaan liittyviä epäkohtia tai uhkakuvia



Kuvio 28. Koulutuksen suoritettuani osaan perehdyttää uuden työntekijän tietoturva-asioihin

6.3.6 Tietoturvakoulutuksen kehittäminen

Kysyttäessä vastaajilta, että tulisiko tietoturvakoulutusta järjestää säännöllisesti, vastaajista 73,4 % oli samaa mieltä. 26,6 % vastaajista ei osannut sanoa, mutta yksikään vastaajista ei ollut sitä mieltä, ettei koulutusta tulisi järjestää.

43,2 % vastaajista oli sitä mieltä, että koulutusta tulisi järjestää tarpeen mukaan, 25,2 % toivoi koulutusta kerran vuodessa, vain 1,8 % kaksi kertaa vuodessa ja 27 % vastaajista oli sitä mieltä, että koulutus kahden vuoden välein on riittävää. Muissa vaihtoehdoissa (3,6 %) vastaajat ehdottivat muun muassa, että koulutusta tulisi järjestää säännöllisesti aina uusille työntekijöille ja vanhoille työntekijöille kertauksena muutaman vuoden välein.

Vastaajilta kysyttiin myös miten he toivoisivat koulutusta järjestettävän. Yli puolet (53,8 %) oli tyytyväisiä nykyiseen verkkokoulutusmuotoon. 34,1 % vastaajista toivoi kuitenkin sekä verkkokoulutusta että luentoja ja 13 % vastaajista oli sitä mieltä, että luentomuotoinen koulutus sopisi parhaiten. Pieni osa vastaajista oli myös lähi- ja henkilökohtaisen opetuksen kannalla.

”Olen yli 50 ja tietokoneet eivät ole "parhaat ystäväni", joten pitäisin nk yksinkertaista "kädestä pitäen opetusta" parhaana metodina. Meikäläisiä on paljon...”

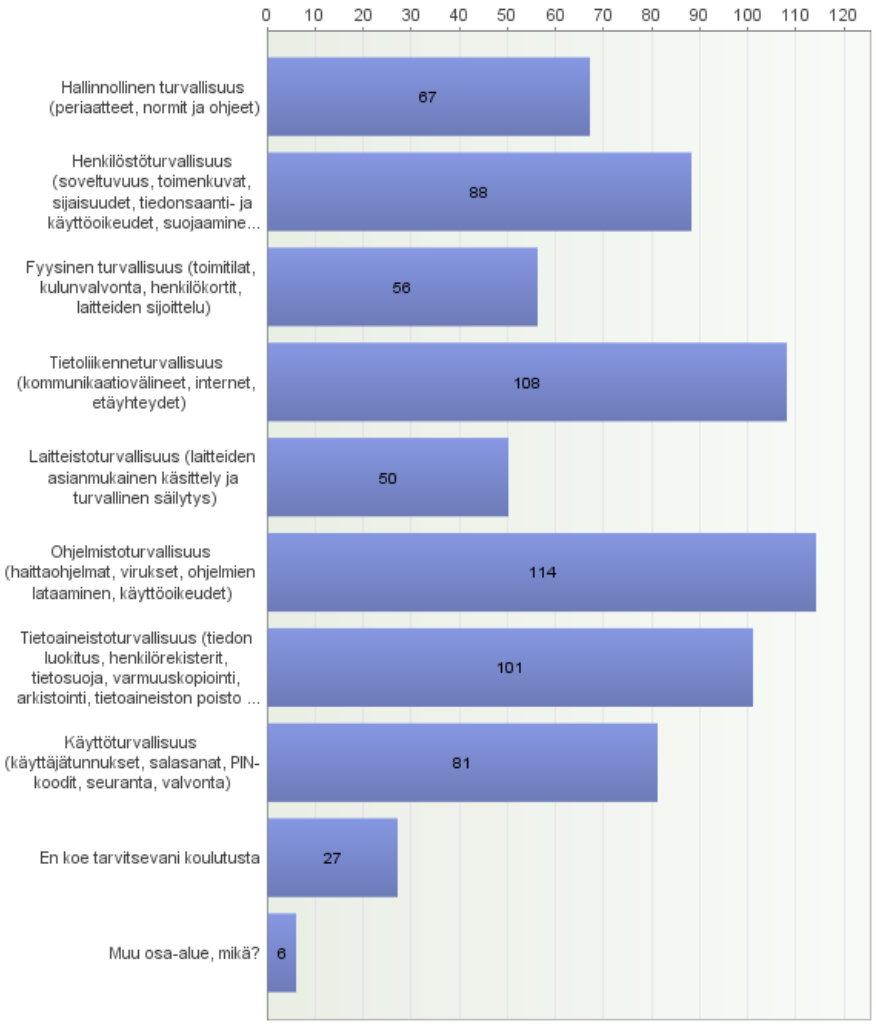
”joku oman alan henkilö puhumaan, että koskettaa...”

*”Pelkkä verkkokoulutus on siitä ikävä, että koulutuksen kuluessa heräävii*n *kysymyksiin ei saa heti vastausta. Kysymyksiä ei tule esitettyä sitten mitään kautta ja joissain asioissa voi jäädä epätietoiseksi.”*

Aiemmin tämän opinnäytetyön teoriaosuudessa kohdassa 3.4. käsittelin tietoturvan kahdeksaa osa-aluetta ja niiden merkitystä tietoturvan kokonaisvaltaiseen hahmottamiseen ja koulutuksen kehittämiseen. Kysyttäessä tulevaisuuden koulutustarpeita tietoturvan saralta, vastaajilla oli mahdollisuus valita useampia osa-alueita (Kuvio 29).

Mobiililaitteiden käyttö yleistyy nopealla vauhdilla myös julkishallinnon organisaatioissa. Rovaniemen kaupungilla on käytössä jo yli 250 älypuhelinta ja myös tablet-laitteet eli taulutietokoneet tekevät tuloaan. Tämä asettaa suuria haasteita tietoturvalle. Myös tietoaineistoturvallisuuteen on kiinnitettävä tulevaisuudessa enemmän huomiota, kun tietojärjestelmiä ja -ohjelmia hankitaan ns. pilvipalveluina, jolloin organisaatio ei välttämättä voi tietää missä tiedot sijaitsevat, miten niiden suojaamisesta on huolehdittu ja miten tieto liikkuu.

Tämä voidaan päätellä myös kyselyyn vastanneiden yhdeksi huolenaiheeksi, koska iso osa vastaajista vastasi tulevaisuuden koulutustarpeista kysyttäessä juurikin tietoliikenne- ja tietoaineistoturvallisuuden osa-alueet. Suurin osa henkilöstön koulutustarpeesta kohdistui kuitenkin ohjelmistoturvallisuuteen, mikä on ymmärrettävää, kun tietojärjestelmien ja ohjelmien määrä lisääntyy koko ajan. Tästä voidaan myös päätellä, että koulutuksen sisältö ja määrä eivät välttämättä vastaa kasvavaan kysyntään.



Kuvio 29. Mihin tietoturvan osa-alueisiin toivoisit tulevaisuudessa koulutusta?

Lopuksi kysyttäessä vastaajilta, että miten parantaisit koulutusta ja mitä tulevaisuudessa pitäisi tehdä, saatiin paljon konkreettisia kehittämistoiveita, jotka koskivat niin koulutuksen sisältöä kuin opetusmenetelmiäkin.

”Koulutuksessa pitäisi ottaa huomioon enemmän myös sitä todellisuutta, että monikaan ei juuri tiedä mitään tietoturvasta. Voisko olla joku yleispätevä paketti, jonka jokainen taho voisi liittää perehdytyskansioihin työpaikoilla, myös liikelaitokset, osakeyhtiöt.”

”Verkkokoulutuksessa on hankalaa esittää kysymyksiä ja monet ei kehtaa jättää viestiä vaan olisi helpompi kysyä ja saada vastaus suoraan. Olen lähiopetuksen kannalla tai verkkokoulutus puheyhteydellä.”

”Tämän kurssin suorittaminen oli pakkopulla ja käytetty menetelmä (ohjelma) oppimisen kannalta kehnohko. En oppinut juuri mitään uutta. Suoritin vain

pakkopullan, mikä ei edistä myönteistä suhtautumista tietoturva-asioihin. Arvelen kuitenkin olevani aika "tietoturvallinen".”

”Nykyisessä kyselyssä on muutama kysymys, jossa "oikea" vastaus riippuu siitä, miten kysymyksen tulkitsee. Kannattaisi päästä testikysymyksissä eroon tulkinnanvaraisuudesta. Jotain tietoturvallisuuskoulutusta voisi olla paikallaan järjestää myös pienryhmissä, jossa asioita voisi yhdessä tekemällä oppia. Pelkkä verkkokoulutus kun helposti jää yhden kerran asiaksi.”

”Eritasoinen koulutus eri toimenkuvan omaaville työntekijöille (osastot).”

7 POHDINTA JA JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tavoitteena oli arvioida toteutetun tietoturvakoulutuksen vaikuttavuutta järjestämällä arviointikysely ja sen perusteella selvittää koulutuksen suorittaneiden käsityksiä tietoturvakoulutuksen toteutuksesta, sisällöstä, käytettävyydestä ja vaikuttavuudesta yksilön tietoturvakäyttäytymisen muutokseen. On kuitenkin arviointitulostenkin perusteella sanottava, että koulutuksen arviointi olisi pitänyt tehdä huomattavasti aiemmin. Arviointikyselyssä usea vastaaja olikin kiinnittänyt tähän huomiota ja tämä varmasti vaikutti osaltaan myös kyselyyn vastanneiden määrään.

Kuitenkin tämä työ saavutti sille asetetut tavoitteensa ja kyselyyn vastanneiden määrä oli tarkoitukseen nähden riittävä, sillä vastauksista saatiin kattava otos tietoturvakoulutuksen osallistuneiden näkemyksistä koulutuksen toteuttamisen ja koulutuksen vaikuttavuuden arviointiin.

Tietoturvakoulutuksen suorittaminen nykyisellä verkko-oppimisalustalla koettiin pääsääntöisesti hyväksi koulutusmuodoksi, joskin muunlaistakin opetusmuotoa rinnalle kaivattiin. Myös koulutusympäristön käytettävyys ja koulutuksen sisältö koettiin tarkoituksenmukaisiksi, vaikkakin se asetti myös haasteita vähemmän tietokonetta käyttäneille. Vastaajat kokivat myös oppineensa uutta ja tiedostaneensa tietoturvan merkityksen paremmin koulutuksen suoritettuaan. Koulutuksen suorittamiseen toivottiin kuitenkin jonkin verran enemmän kannustusta ja tukea esimiehiltä. Myös palautteen saaminen ja koulutuksessa käytyjen asioiden käsitteleminen yhdessä työyhteisön tai esimiehen kanssa koettiin tärkeäksi.

Tietoturvakoulutuksen kehittämistoiveet olivat hyvin konkreettisia ja näiden pohjalta myös koulutuksen sisältöä tulisi miettiä nykyistä tarkemmin. Koulutuksen sisällön kehittäminen vastaamaan henkilön työtehtäviä tai toimenkuvaa, vaikuttaa todennäköisesti positiivisesti myös henkilön motivaatioon ja asennoitumiseen koulutukseen. Motivaatioon liittyy myös olennaisesti kannustaminen ja oikeanlainen palaute. Mikäli työntekijä saa palautetta ja häntä kannustetaan, niin todennäköisesti hän on myös motivoituneempi koulutuksen suorittamiseen.

Nykyinen koulutusmuoto koettiin pääsääntöisesti hyväksi ja helpoksi tavaksi koulutuksen suorittamiseen, mutta tietoturvakoulutusta tulisi myös kehittää

siten, että erilaisten käyttäjäryhmien tarpeet huomioitaisiin. Tulevaisuudessa voitaisiin räätälöidä erilaisille käyttäjäryhmille sopivia koulutuskokonaisuuksia. Koulutusympäristöön voitaisiin räätälöidä sisältöjä vastaamaan esimerkiksi luottamushenkilöiden, osakeyhtiöiden, johdon, esimiesten ja muiden erityisryhmien tarpeisiin. Koulutusympäristöä voitaisiin jopa laajentaa koulujen opetustoimeen oppilaiden tietoturvakouluttamisen välineeksi.

Tässä tietoturvakoulutuksessa käytetystä koulutusympäristöstä voidaan myös todeta, että mikäli sen käyttöä jatketaan, tulisi koulutusympäristön analysointityökaluja kehittää, sillä järjestelmän tuottamat taulukot ja tunnusluvut eivät kerro tarpeeksi kattavasti ja selkeästi tuloksista.

Yhteenvetona tietoturvakoulutuksen kehittämiseksi haluan esittää myös muutaman henkilökohtaisen näkemyksen:

Rovaniemen kaupungille tulisi laatia tietoturvallisuuden koulutussuunnitelma, jossa otettaisiin huomioon niin koulutettavat asiakokonaisuudet kuin koulutuksen kohderyhmät. Koulutussuunnitelman avulla voitaisiin entistä paremmin ottaa huomioon tietoturvallisuuden kehitys- ja koulutustarpeet ja näin varmistaa tietoturvallisuuden jatkuvuuden hallinta.

Kaupungin ylimmän johdon ja esimiesten sitouttaminen tietoturvakulttuurin kehittämiseen ja ylläpitämiseen on edellytys sille, että myös henkilöstö noudattaa tietoturvaohjeita, osallistuu koulutuksiin ja tiedostaa tietoturvan merkityksen omassa työssään.

Tietoturvallisuus tulee ottaa huomioon osana kaupungin henkilöstösuunnitelmaa sekä toiminta- ja taloussuunnittelua, jotta voidaan varmistaa ja ennakoida kehittämiseen ja ylläpitoon tarvittavat resurssit ja kustannukset kullekin vuodelle.

Kyselytutkimuksen valinta tietoturvakoulutuksen vaikuttavuuden arvioinniksi oli lähtökohtaisesti vaivaton ja helppo tapa kerätä aineistoa ja myös vastausten tulkintaa voidaan näin pitää yhteismitallisena. Myös kyselyyn vastanneet pitivät kyselyä selkänä ja sopivan mittaisena. Kyselyn heikkoudeksi puolestaan koin, että sillä ei välttämättä saada kerättyä syvällistä tietoa, koska yksilön tietoturvatietoisuus on hyvin laaja aihealue ja myös kerätyn tiedon tulkitseminen on subjektiivista. Kuitenkin, koska työskentelen kohdeorganisaa-

tiossa ja voin myös vaikuttaa sen tietoturvan kehittämiseen, koen voivani tulkita tietoa myös tästä näkökulmasta.

Haasteeksi kaikkinensa muodostui vain opinnäytetyöni valmistumiseen rajattu aika ja näin ollen arviointitiedon tulkitseminen jäi osittain vajavaiseksi. Tämä arviointi ja siitä työstetty materiaali antaisi mahdollisuuden tarkempaan tarkasteluun esimerkiksi eri osastojen tai ikäryhmien välillä, mutta tässä opinnäytetyössä tarkastelu rajattiin käsittämään koko organisaation näkökulmaa. Tietoturvakoulutuksen kehittämisen näkökulmasta tarkastelua voisi kohdeorganisaatiossa syventää edellä mainittuun suuntaan jo tekemäni arvioinnin pohjalta.

LÄHTEET

Arkistolaki 831/1994. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1994/19940831.

Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19991030.

Digitoday fi. Osoitteessa http://www.digitoday.fi/page.php?page_id=66&news_id=200415488.

Henkilötietolaki 523/1999. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990523. 15.11.2012.

Kirkpatrick, Donald L. 1996. Evaluating Training Programs: The Four Levels. San Francisco. CA: Berrett- Koehler.

Kuutti W. 2003. Käytettävyys, suunnittelu ja arviointi. Korkeakoulu-sarja. Helsinki: Talentum.

Laki viranomaisen toiminnan julkisuudesta 621/1999. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990621. 15.11.2012.

Mielonen, S. – Hintikka K. 1998. Web-palvelujen käytettävyys ja tuotanto. Osoitteessa http://www2.uiah.fi/mediastudio/pdf/web-kaytettavyys.pdf. 20.11.2012. 17.11.2012.

Nykänen K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Oulun yliopisto. Osoitteessa http://herkules.oulu.fi/isbn9789514295713/isbn9789514295713.pdf. 2.11.2012

Opetushallitus. 1998. Koulutuksen tuloksellisuuden arviointimalli. Helsinki: Yliopistopaino.

Rovaniemen kaupungin henkilöstöraportti 2011. Osoitteessa http://issuu.com/roikaupunki/docs/roi_henkilostoraportti 2011. 15.11.2012.

Rovaniemen kaupunkikonsernin tietoturvapolitiikka KH 23.4.2012 § 163. Osoitteessa http://ktweb.rovaniemi.fi/. 15.11.2012

Tenno T. 2011. Surffaajat ja syventyjät. Verkko-oppimisympäristön pedagogisen rakenteen ja opiskelijoiden toimintaorientaatioiden tarkastelua. Lapin yliopistokustannus. Tampere: Juvenes Print.

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2003. Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. VAHTI 6/2003. Valtiovarainministeriö.

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2006. Tietoturvakouluttajan opas. VAHTI 11/2006. Valtiovarainministeriö.

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2007. Tietoturvallisuudella tuloksia. VAHTI 3/2007. Valtiovarainministeriö.

Valtionhallinnon tietoturvallisuuden johtoryhmä. 2000. Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje VAHTI 2/2000. Valtiovarainministeriö. Osoitteessa http://www.vahtiohje.fi/web/guest/273. 15.11.2012.

Valtiovarainministeriön työryhmämuistioita. 2002. Osoitteessa http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/06_valtion_tyomarkkinalaitos/26171/26210_fi.pdf. 14.11.2012.

Viranhaltijapäätös 15.12.2008 § 559. Ei julkinen.

LIITTEET

Tietoturvakoulutuksen arviointikysely

Olet osallistunut Rovaniemen kaupungin järjestämään tietoturvakoulutukseen vuosien 2010 - 2012 välisenä aikana.

Teen parhaillaan Rovaniemen ammattikorkeakoulussa työnantajani toimeksiantona opinnäytetyötä. Opinnäytetyöni koskee järjestetyn tietoturvakoulutuksen arviointia ja sen kehittämistä Rovaniemen kaupungissa.

Kyselyn tarkoituksena on arvioida toteutetun tietoturvakoulutuksen vaikuttavuutta selvittämällä koulutuksen suorittaneiden käsityksiä tietoturvakoulutuksen laadinnasta, toteutuksesta, käytettävyydestä ja sen vaikuttavuudesta yksilön tietoturvakäyttäytymisen muutokseen. Tarkoituksena on lisäksi selvittää, miten koulutuksen toteutus on onnistunut ja miten tietojen, taitojen ja tietoturvatietoisuuden kehittyminen on muuttunut toteutetun koulutuksen jälkeen. Arvioinnissa kiinnitetään huomiota myös siihen, tulisiko organisaation tietoturvakoulutusta kehittää ja millä keinoin.

Pääset kyselyyn tästä linkistä
https://www.webropolsurveys.com/R/93AC78038A92BEC8.par

Vastaukset käsitellään täysin luottamuksellisesti. Muistathan, että kyselyn vastausaikaa on vielä perjantaihin 9.11.2012 saakka.

Kiitos vaivannäöstä!

Lisätietoja:
Virpi Stenberg
virpi.stenberg@rovaniemi.fi
puh. 016 322 8118

Tietoturvakoulutuksen arviointikysely

Tämän kyselyn tavoitteena on arvioida Rovaniemen kaupungin henkilöstölle toteutetun tietoturvakoulutuksen vaikuttavuutta selvittämällä koulutuksen suorittaneiden käsityksiä tietoturvakoulutuksen laadinnasta, toteutuksesta, käytettävyydestä ja sen vaikuttavuudesta yksilön tietoturvakäyttäytymisen muutokseen. Tarkoituksena on lisäksi selvittää, miten koulutuksen toteutus on onnistunut ja miten tietojen, taitojen ja tietoturvatietoisuuden kehittyminen on muuttunut toteutetun koulutuksen jälkeen.

1. Vastaajan sukupuoli *

◯ Mies ◯ Nainen

2. Vastaajan ikä *

◯ Alle 35 vuotta

◯ 35 - 49 vuotta

◯ 50 vuotta tai enemmän

3. Vastaajan sijoittuminen kaupungin organisaatiossa *

◯ Hallinto-organisaatio (sisältää: kaupunginjohto, sisäinen tarkastus, kaupunkitarkastaja, hyvinvointipalvelut, tekniset palvelut, strateginen hallinto)

◯ Sivistyspalvelujen tuotanto-osasto (sisältää: koulupalvelukeskus, päivähoidon palvelukeskus, kulttuuripalvelukeskus, liikunta- ja nuorisopalvelukeskus)

◯ Tekninen tuotanto-osasto (sisältää: keskitetyt palvelut, infrapalvelukeskus, ruoka- ja puhtauspalvelukeskus)

◯ Liikelaitokset (sisältää: Napapiirin Vesi, tilaliikelaitos, työterveysliikelaitos)

4. Olen tietoinen kaupungin tietoturvapolitiikasta sekä siihen liittyvistä ohjeistuksista ja tiedän mistä ne löytyvät? *

◯ Kyllä ◯ Ei

5. Missä suoritit tietoturvakoulutuksen?

◯ Työpaikalla

◯ Kotona

◯ Työpaikalla ja kotona

◯ Muualla

6. Arvioi aikaa, joka sinulta kului koulutuksen suorittamiseen

◯ Alle 1 tunti

◯ 1 - 2 tuntia

◯ Yli 2 tuntia

7. Saitko tukea ja perehdytystä koulutuksen suorittamiseen?

◯ Sain riittävästi

◯ Sain jonkin verran

◯ En saanut lainkaan

◯ En osaa sanoa

8. Keneltä sait tukea ja perehdytystä koulutuksen suorittamiseen?

☐ Esimieheltä

☐ Työkaverilta

☐ En keneltäkään

☐ Muualta, mistä?

9. Keneltä tai mistä sait tietoa koulutuksen suorittamisesta?

☐ Esimieheltä

☐ Työkaverilta

☐ Tiedotteesta työpaikalla tai lanssissa

☐ Muualta, mistä?

10. Suoritin koulutuksen, koska...

☐ Koin asian tärkeäksi

☐ Esimies tai joku muu edellytti

☐ Muusta syystä, mistä?

11. Arvioi tietoturvakoulutusympäristön käytettävyyttä

Tämän kysymysryhmän tavoitteena on selvittää tietoturvakoulutusympäristön käytettävyyttä

	En osaa sanoa	Täysin eri mieltä	Osittain eri mieltä	Osittain samaa mieltä	Täysin samaa mieltä
Koulutusympäristöön rekisteröityminen oli vaivatonta	○	○	○	○	○
Koulutusympäristöön kirjautuminen oli vaivatonta	○	○	○	○	○
Koulutusympäristössä navigointi oli vaivatonta	○	○	○	○	○
Koulutusympäristön ohjeet löytyivät vaivattomasti	○	○	○	○	○

12. Arvioi tietoturvakoulutuksen sisältöä

Tämän kysymysryhmän tavoitteena on arvioida tietoturvakoulutuksen materiaalin sisältöä.

	En osaa sanoa	Täysin eri mieltä	Osittain eri mieltä	Osittain samaa mieltä	Täysin samaa mieltä
Koulutusmateriaali oli selkeää ja helppolukuista	○	○	○	○	○
Ymmärsin koulutusmateriaalissa olevat käsitteet tai löysin niille tarvittaessa selityksen sanastosta	○	○	○	○	○
Koulutusmateriaalissa esiintyneet esimerkit auttoivat ymmärtämään käsiteltävän asian paremmin	○	○	○	○	○
Löysin koulutusmateriaalin teoriaosuudesta vastaukset alku- ja lopputestin kysymyksiin	○	○	○	○	○
Koulutusmateriaali ja opetusmenetelmät tukivat oppimistani	○	○	○	○	○

13. Asennoituminen tietoturvakoulutusta kohtaan

Tämän kysymysryhmän tavoitteena on arvioida koulutuksen tarkoituksenmukaisuutta ja henkilön motivaatiota koulutuksen suorittamiseen.

	En osaa sanoa	Täysin eri mieltä	Osittain eri mieltä	Osittain samaa mieltä	Täysin samaa mieltä
Olin motivoitunut koulutuksen suorittamiseen	○	○	○	○	○
Koulutus oli tarkoituksenmukaista työlleni	○	○	○	○	○
Minua kannustettiin ja sain palautetta koulutuksen suorittamisessa	○	○	○	○	○

14. Arvioi tietoturvakoulutuksen vaikuttavuutta

Tämän kysymysryhmän tavoitteena on arvioida koulutuksen vaikutusta oman osaamisen kehittymiseen ja työyhteisön toimintaan.

	En osaa sanoa	Täysin eri mieltä	Osittain eri mieltä	Osittain samaa mieltä	Täysin samaa mieltä
Koulutus vaikutti päivittäisiin tietoturvaan liittyviin toimintatapoihini	○	○	○	○	○
Koin oppineeni uutta tietoturvaan liittyvistä asioista	○	○	○	○	○
Koulutus edisti omaa tietoturvatietoisuuttani ja osaamiseni kehittyi koulutuksen myötä	○	○	○	○	○
Työssäni on riittävästi aikaa kokeilla ja soveltaa uusia tietoturvakäytänteitä	○	○	○	○	○
Koulutuksesta on ollut lisäarvoa työyhteisölleni ja sen tietoturvan kehittämiselle	○	○	○	○	○
Koulutus toi lisää haasteita tietotekniikan käytön suhteen	○	○	○	○	○
Koulutus toi uusia ajatuksia tai uhkakuvia esille työtäni ajatellen	○	○	○	○	○
Salasanani hallintaan liittyvät käytänteet ovat muuttuneet tai kiinnitän niihin nykyään enemmän huomiota	○	○	○	○	○
Tunnistan nykyään paremmin tietoturvaan liittyviä epäkohtia tai uhkakuvia	○	○	○	○	○
Koulutuksen suoritettuani osaan perehdyttää uuden työntekijän tietoturva-asioihin	○	○	○	○	○

15. Tulisiko tietoturvakoulutusta järjestää säännöllisesti

○ Kyllä

○ Ei

○ En osaa sanoa

16. Kuinka usein tietoturvakoulutusta tulisi mielestäsi järjestää?

◯ Kaksi kertaa vuodessa

◯ Kerran vuodessa

◯ Kerran kahdessa vuodessa

◯ Tarpeen mukaan

◯ Muu vaihtoehto, mikä?

15. Tulisiko tietoturvakoulutusta järjestää säännöllisesti

◯ Kyllä

◯ Ei

◯ En osaa sanoa

16. Kuinka usein tietoturvakoulutusta tulisi mielestäsi järjestää?

◯ Kaksi kertaa vuodessa

◯ Kerran vuodessa

◯ Kerran kahdessa vuodessa

◯ Tarpeen mukaan

◯ Muu vaihtoehto, mikä?

17. Millä tavoin toivoisit tietoturvakoulutusta järjestettävän tulevaisuudessa?

☐ Verkkokoulutus

☐ Luennot

☐ Verkkokoulutus ja luennot

☐ Muu vaihtoehto, mikä?

18. Mihin tietoturvan osa-alueisiin toivoisit tulevaisuudessa koulutusta?

- ☐ Hallinnollinen turvallisuus (periaatteet, normit ja ohjeet)
- ☐ Henkilöstöturvallisuus (soveltuvuus, toimenkuvat, sijaisuudet, tiedonsaanti- ja käyttöoikeudet, suojaaminen, koulutus, valvonta)
- ☐ Fyysinen turvallisuus (toimitilat, kulunvalvonta, henkilökortit, laitteiden sijoittelu)
- ☐ Tietoliikenneturvallisuus (kommunikaatiovälineet, internet, etäyhteydet)
- ☐ Laitteistoturvallisuus (laitteiden asianmukainen käsittely ja turvallinen säilytys)
- ☐ Ohjelmistoturvallisuus (haittaohjelmat, virukset, ohjelmien lataaminen, käyttöoikeudet)
- ☐ Tietoaineistoturvallisuus (tiedon luokitus, henkilörekisterit, tietosuoja, varmuuskopiointi, arkistointi, tietoaineiston poisto ja hävittäminen)
- ☐ Käyttöturvallisuus (käyttäjätunnukset, salasanat, PIN-koodit, seuranta, valvonta)
- ☐ En koe tarvitsevani koulutusta
- ☐ Muu osa-alue, mikä?

19. Minkälaista palautetta toivoisit koulutuksen suorittamisesta?

20. Miten parantaisit koulutusta ja mitä tulevaisuudessa pitäisi tehdä?

21. Muu palaute

Tässä voit vapaasti kommentoida niin tietoturvakoulutusta kuin tätä kyselyäkin.

Tietoturvakoulutuksen arviointikyselyn yhteenveto

1. Vastaajan sukupuoli

Vastaajien määrä: 224

	Vastaajan sukupuoli
Mies	44,2%
Nainen	55,8%

2. Vastaajan ikä

Vastaajien määrä: 224

	Vastaajan ikä
Alle 35 vuotta	8%
35 - 49 vuotta	30,4%
50 vuotta tai enemmän	61,6%

3. Vastaajan sijoittuminen kaupungin organisaatiossa

Vastaajien määrä: 224

	Vastaajan sijoittuminen kaupungin organisaatiossa
Hallinto-organisaatio (sisältää: kaupunginjohto, sisäinen tarkastus, kaupunkitarkastaja, hyvinvointipalvelut, tekniset palvelut, strateginen hallinto)	21%
Sivistyspalvelujen tuotanto-osasto (sisältää: koulupalvelukeskus, päivähoidon palvelukeskus, kulttuuripalvelukeskus, liikunta- ja nuorisopalvelukeskus)	47,8%
Tekninen tuotanto-osasto (sisältää: keskitetyt palvelut, infrapalvelukeskus, ruoka- ja puhtauspalvelukeskus)	22,8%
Liikelaitokset (sisältää: Napapiirin Vesi, tilaliikelaitos, työterveysliikelaitos)	8,5%

4. Olen tietoinen kaupungin tietoturvapolitiikasta sekä siihen liittyvistä ohjeistuksista ja tiedän mistä ne löytyvät?

Vastaajien määrä: 224

	Olen tietoinen kaupungin tietoturvapolitiikasta sekä siihen liittyvistä ohjeistuksista ja tiedän mistä ne löytyvät?
Kyllä	87,1%
Ei	12,9%

5. Missä suoritit tietoturvakoulutuksen?

Vastaajien määrä: 222

	Missä suoritit tietoturvakoulutuksen?
Työpaikalla	83,3%
Kotona	9,5%
Työpaikalla ja kotona	5,9%
Muualla	1,4%

6. Arvioi aikaa, joka sinulta kului koulutuksen suorittamiseen

Vastaajien määrä: 221

	Arvioi aikaa, joka sinulta kului koulutuksen suorittamiseen
Alle 1 tunti	50,2%
1 - 2 tuntia	40,7%
Yli 2 tuntia	9%

7. Saitko tukea ja perehdytystä koulutuksen suorittamiseen?

Vastaajien määrä: 223

	Saitko tukea ja perehdytystä koulutuksen suorittamiseen?
Sain riittävästi	26,5%
Sain jonkin verran	29,6%
En saanut lainkaan	39%
En osaa sanoa	4,9%

8. Keneltä sait tukea ja perehdytystä koulutuksen suorittamiseen?

Vastaajien määrä: 211

	Keneltä sait tukea ja perehdytystä koulutuksen suorittamiseen?
Esimieheltä	20,4%
Työkaverilta	32,2%
En keneltäkään	44,5%
Muualta, mistä?	10,9%

Avoimet vastaukset: Muualta, mistä?

- Koulutuksen yhteydessä oli hyvä tietopaketti.
- koulutuksen sivuilta
- infosta
- tutustumalla materiaaliin ko.aiheesta
- tietosuojatyöryhmästä
- nettiohjeista, info koulutuksesta työpaikkakokouksessa ja s-postilla henkilöstöllemme
- Tietohallinnolta
- muistaakseni kaupungilla oli järjestetty perehdytys ja ohjeistusta tuli sähköpostina
- kirjallinen käyttöohje
- koulutuksen mukana tulleista ohjeista
- Ohjeista suorittaessani koulutuksen
- Osasin asiat pääsäätöisesti ennen koulutuksen suorittamista
- Koulutuksen teksteistä
- omilta työntekijöiltä
- tvt -vastaavalta
- Olin mukana ko. koulutksen käynnistyksessä, joten sain pohjatiedon sitä kautta.
- Siitä linkistä, jossa koulutus suoritettiin
- Koulutusohjeet lanssissa
- Info rehtorikokouksessa
- Tietohallinnon järjestämä koulutus
- Tietoturvatyöryhmässä ja tietohallinnolta
- ei ollut tarvetta

9. Keneltä tai mistä sait tietoa koulutuksen suorittamisesta?

Vastaajien määrä: 222

	Keneltä tai mistä sait tietoa koulutuksen suorittamisesta?
Esimieheltä	49,1%
Työkaverilta	12,2%
Tiedotteesta työpaikalla tai lanssissa	48,2%
Muualta, mistä?	7,2%

Avoimet vastaukset: Muualta, mistä?

- infosta
- Sähköposti
- sähköpostiin tulleesta ilmoituksesta
- sähköposti
- tietosuojatyöryhmästä
- Tietohallinnolta
- vastauslomakkeesta tai vastaavasta, en tarkkaan muista.
- sähköposti
- Koulutukseen valmistavassa ennakkoinfossa
- Sähköpostiukaasista, että pitää suorittaa heti tai...
- Sähköpostista
- sähköpostin kautta
- Sähköpostilla patistettiin tekemään.
- Olin mukana ko. koulutksen käynnistyksessä, joten sitä kautta
- sähköpostilla
- sähköpostimuistutus

10. Suoritin koulutuksen, koska...

Vastaajien määrä: 224

	Suoritin koulutuksen, koska...
Koin asian tärkeäksi	45,5%
Esimies tai joku muu edellytti	60,3%
Muusta syystä, mistä?	2,7%

Avoimet vastaukset: Muusta syystä, mistä?

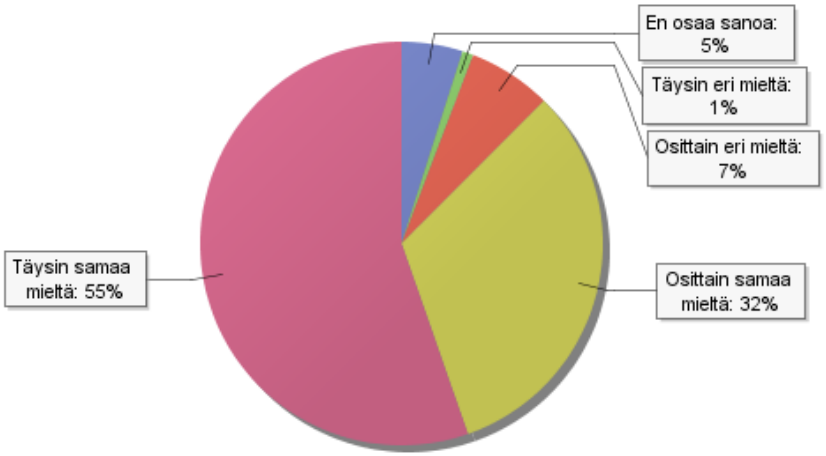
- pakko
- viestissä oli että se on pakko suorittaa
- Taisin saada asiasta sähköpostiviestin, en muista enää tarkkaan.
- oli pakko
- Halusin testata ja päivittää tietoni
- Eikös se ollut pakollinen?

11. Arvioi tietoturvakoulutusympäristön käytettävyyttä

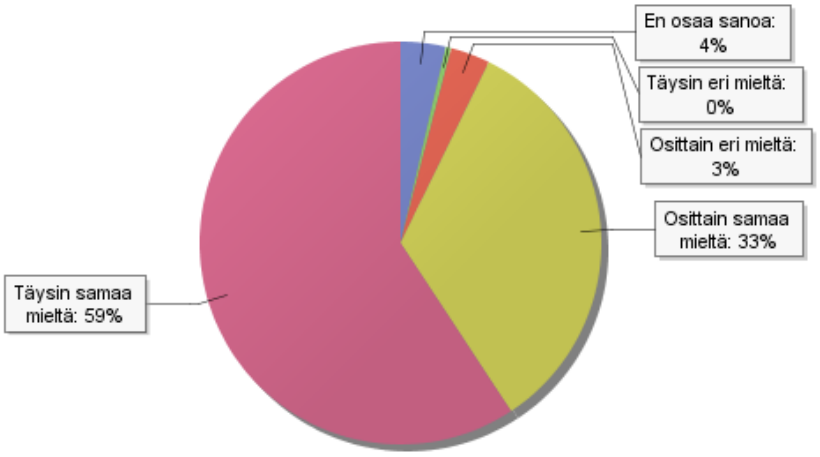
Tämän kysymysryhmän tavoitteena on selvittää tietoturvakoulutusympäristön käytettävyyttä

Vastaajien määrä: 224

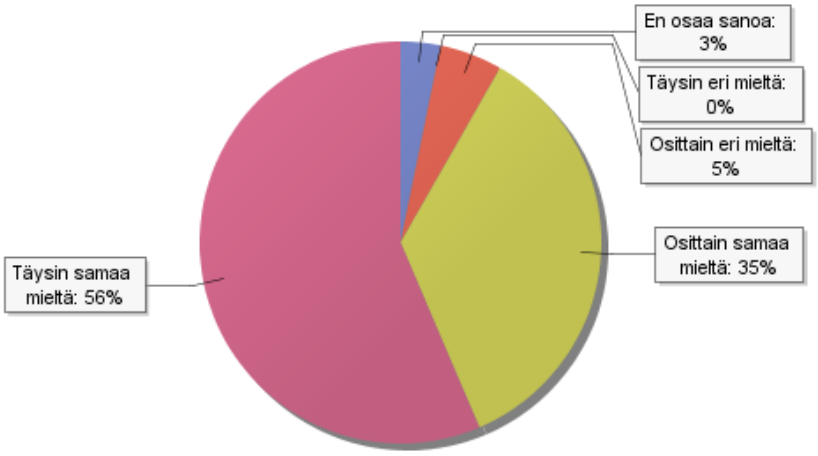
Koulutusympäristöön rekisteröityminen oli vaivatonta



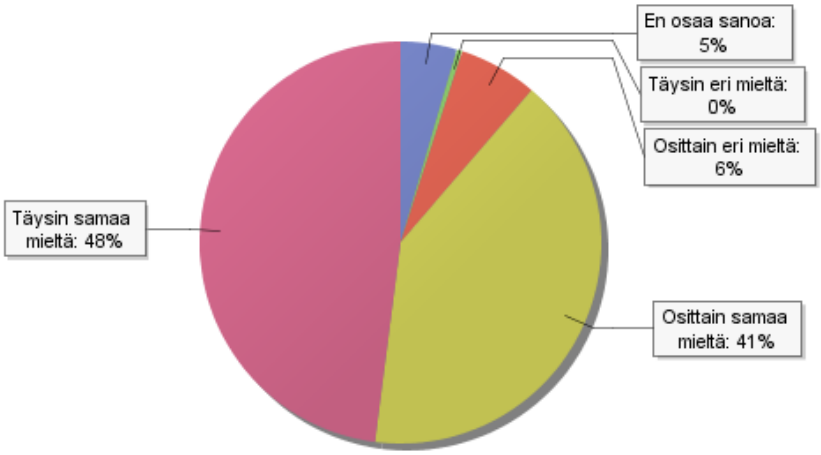
Koulutusympäristöön kirjautuminen oli vaivatonta



Koulutusympäristössä navigointi oli vaivatonta



Koulutusympäristön ohjeet löytyivät vaivattomasti

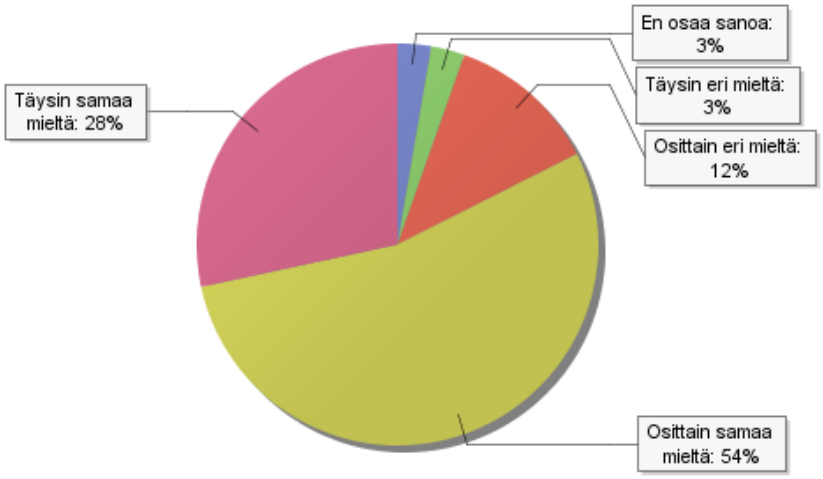


12. Arvioi tietoturvakoulutuksen sisältöä

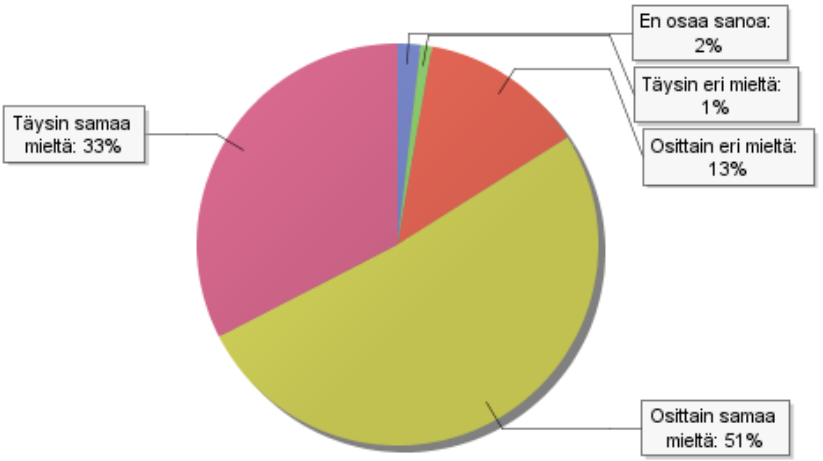
Tämän kysymysryhmän tavoitteena on arvioida tietoturvakoulutuksen materiaalin sisältöä.

Vastaajien määrä: 223

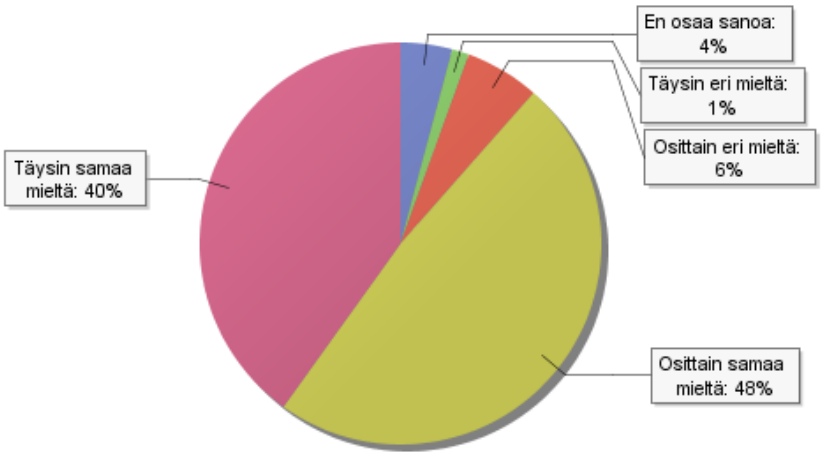
Koulutusmateriaali oli selkeää ja helppolukuista



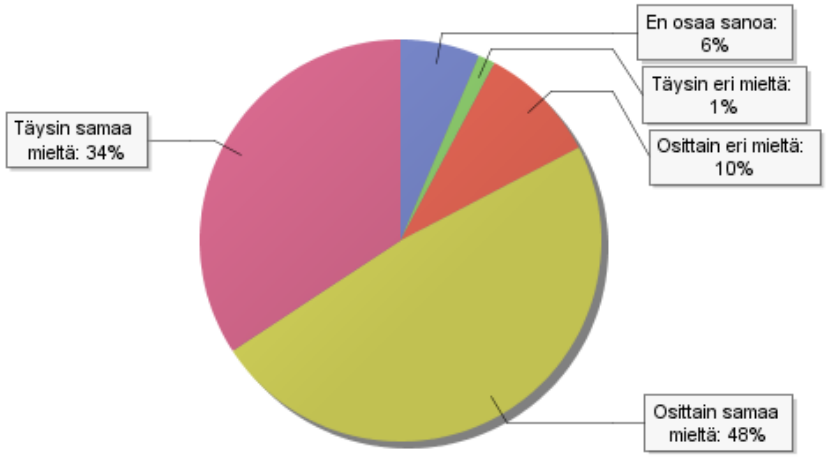
Ymmärsin koulutusmateriaalissa olevat käsitteet tai löysin niille tarvittaessa selityksen sanastosta



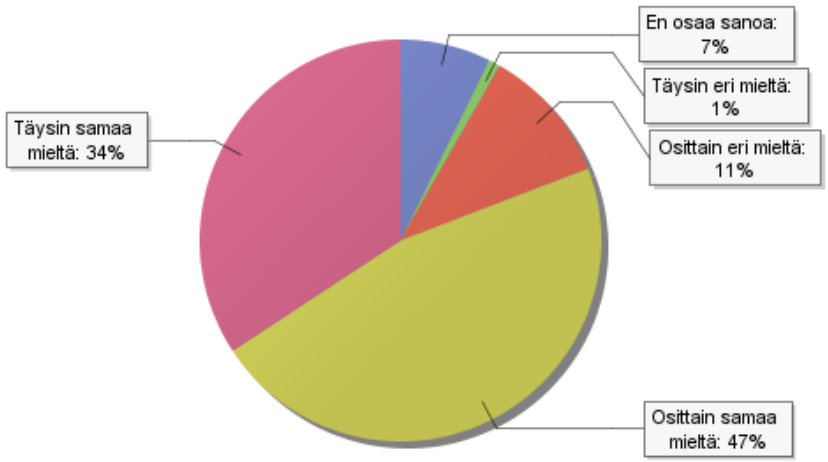
Koulutusmateriaalissa esiintyneet esimerkit auttoivat ymmärtämään käsiteltävän asian paremmin



Löysin koulutusmateriaalin teoriaosuudesta vastaukset alku- ja lopputestin kysymyksiin



Koulutusmateriaali ja opetusmenetelmät tukivat oppimistani

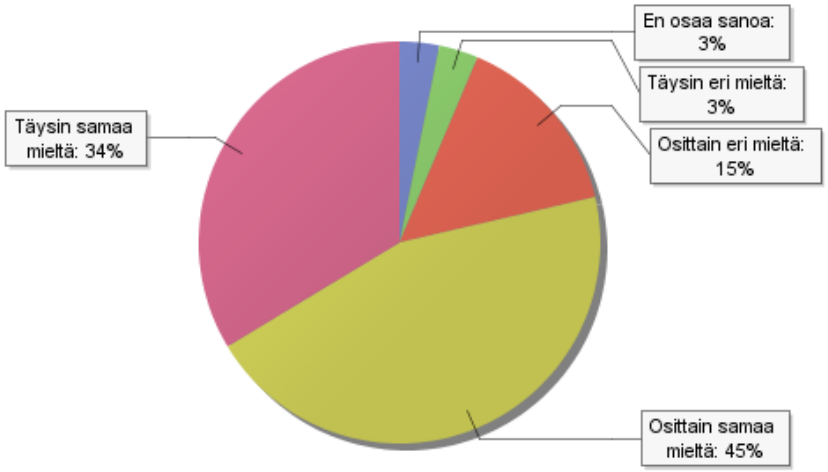


13. Asennoituminen tietoturvakoulutusta kohtaan

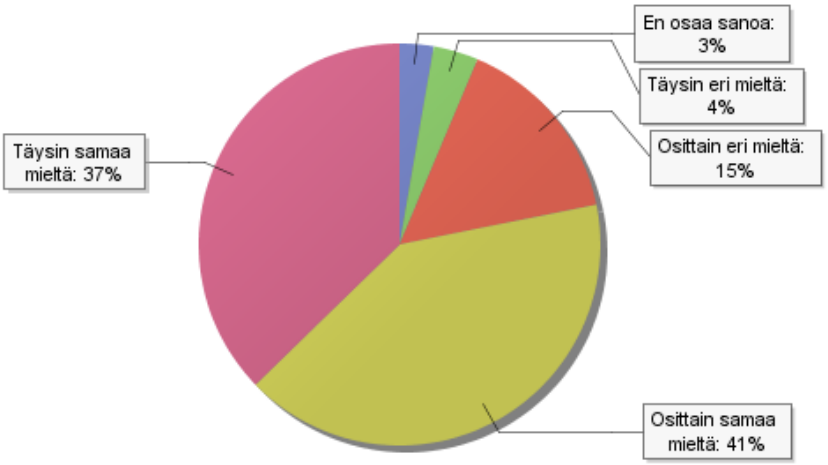
Tämän kysymysryhmän tavoitteena on arvioida koulutuksen tarkoituksenmukaisuutta ja henkilön motivaatiota koulutuksen suorittamiseen.

Vastaajien määrä: 223

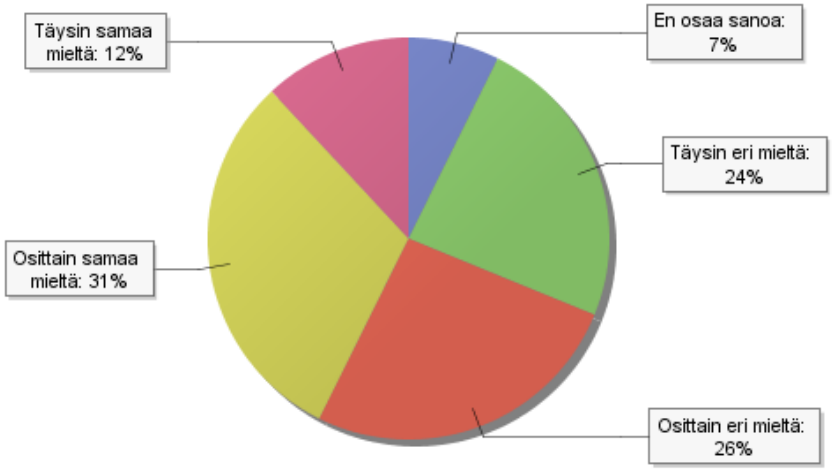
Olin motivoitunut koulutuksen suorittamiseen



Koulutus oli tarkoituksenmukaista työlleni



Minua kannustettiin ja sain palautetta koulutuksen suorittamisessa

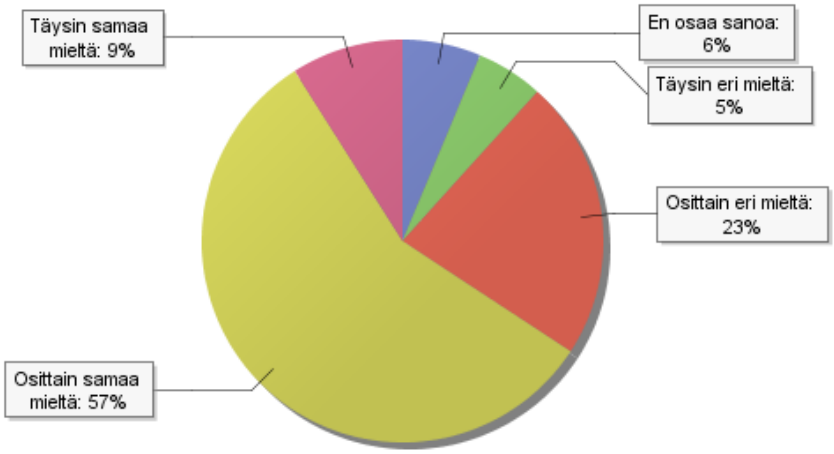


14. Arvioi tietoturvakoulutuksen vaikuttavuutta

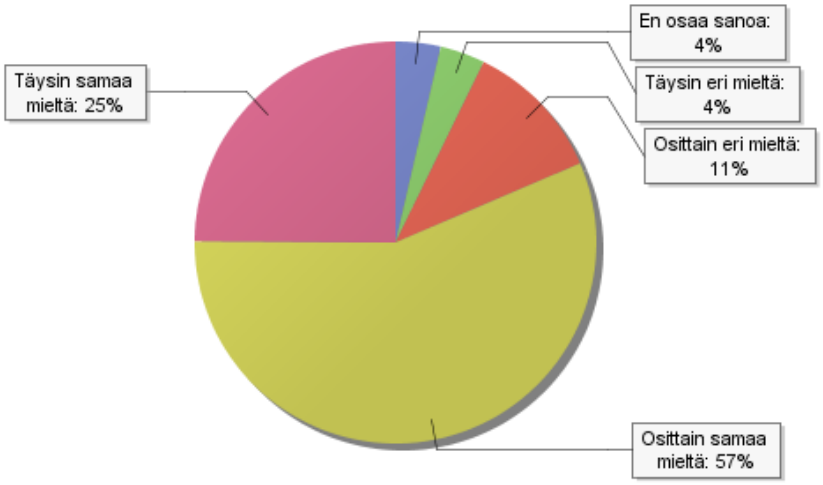
Tämän kysymysryhmän tavoitteena on arvioida koulutuksen vaikutusta oman osaamisen kehittymiseen ja työyhteisön toimintaan.

Vastaajien määrä: 224

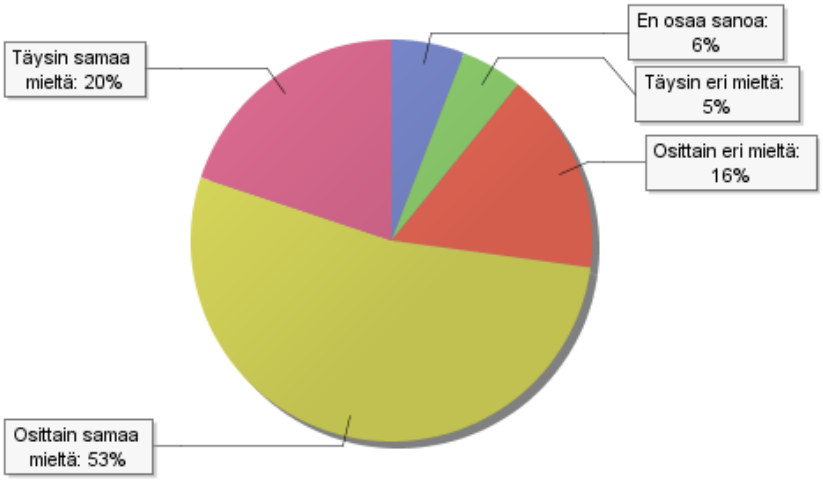
Koulutus vaikutti päivittäisiin tietoturvaan liittyviin toimintatapoihini



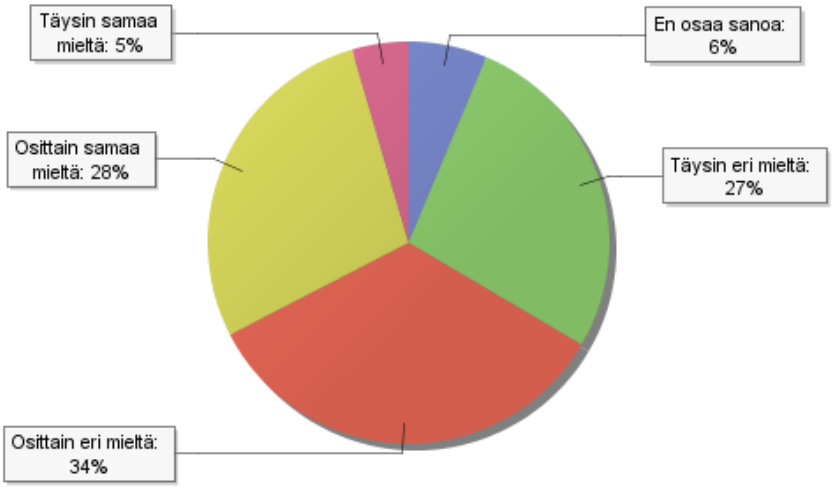
Koin oppineeni uutta tietoturvaan liittyvistä asioista



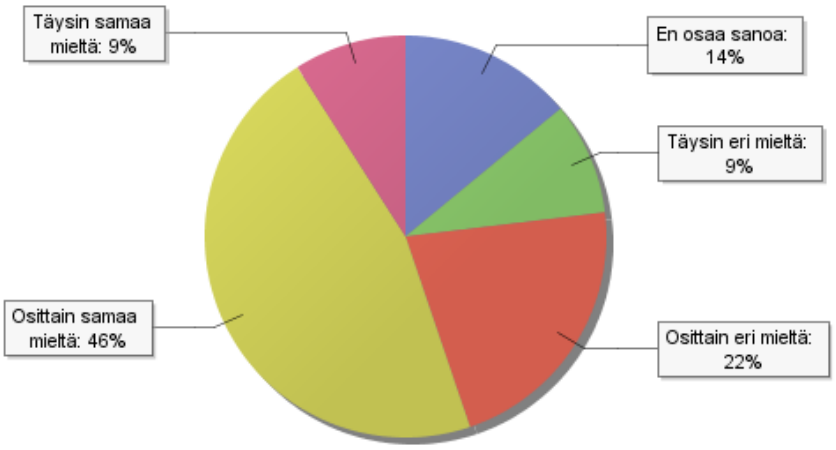
Koulutus edisti omaa tietoturvatietoisuuttani ja osaamiseni kehittyi koulutuksen myötä



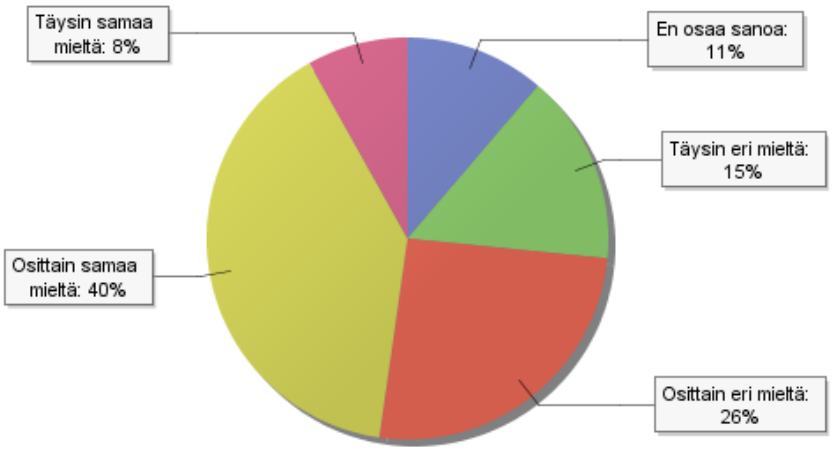
Työssäni on riittävästi aikaa kokeilla ja soveltaa uusia tietoturvakäytänteitä



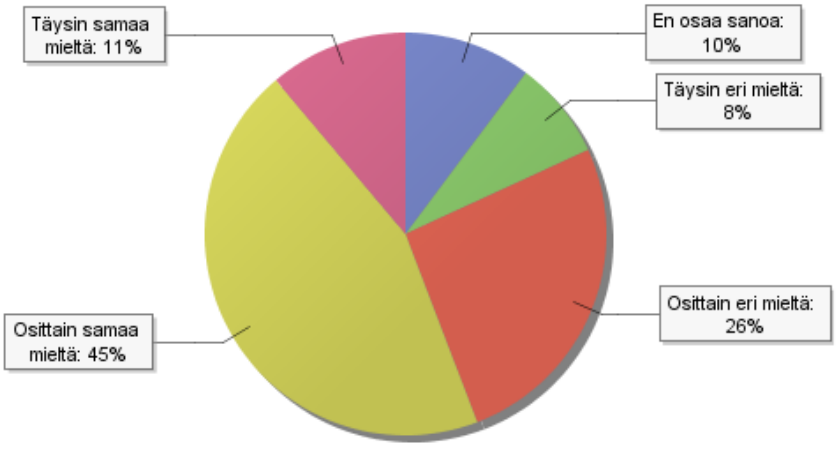
Koulutuksesta on ollut lisäarvoa työyhteisölleni ja sen tietoturvan kehittämiselle



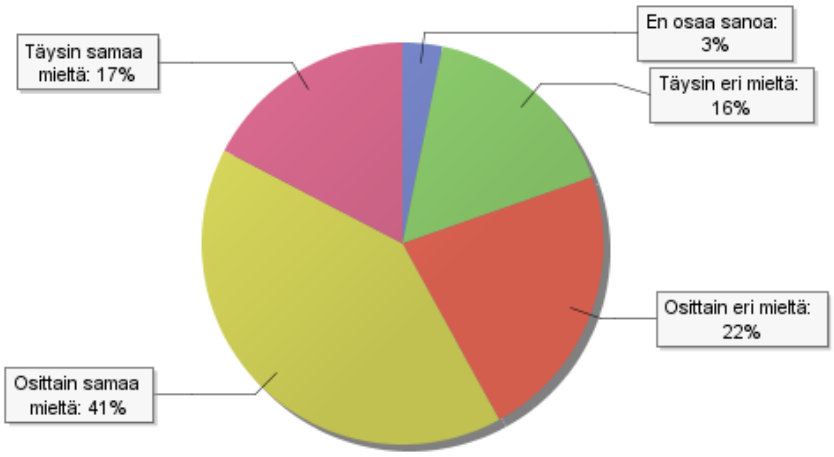
Koulutus toi lisää haasteita tietotekniikan käytön suhteen



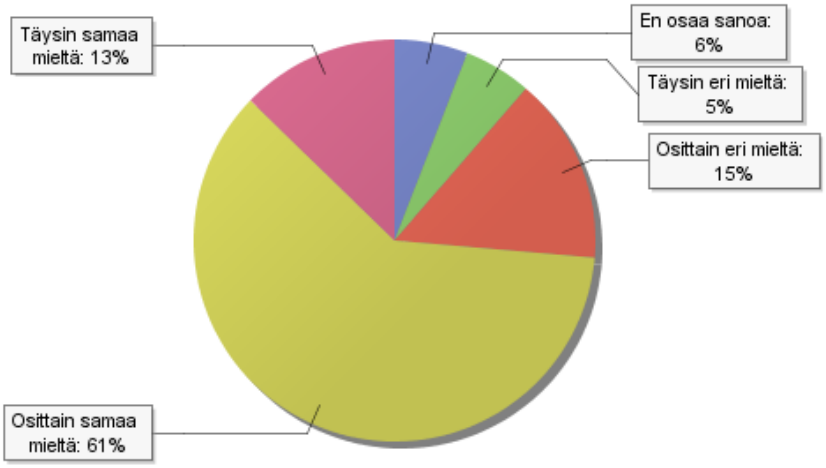
Koulutus toi uusia ajatuksia tai uhkakuvia esille työtäni ajatellen



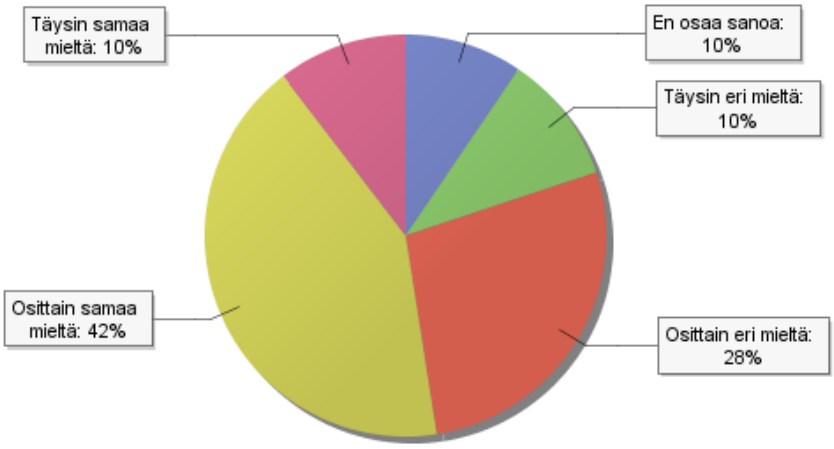
Salasanani hallintaan liittyvät käytänteet ovat muuttuneet tai kiinnitän niihin nykyään enemmän huomiota



Tunnistan nykyään paremmin tietoturvaan liittyviä epäkohtia tai uhkakuvia



Koulutuksen suoritettuani osaan perehdyttää uuden työntekijän tietoturva-asioihin



15. Tulisiko tietoturvakoulutusta järjestää säännöllisesti

Vastaajien määrä: 222

	Tulisiko tietoturvakoulutusta järjestää säännöllisesti
Kyllä	73,4%
Ei	0%
En osaa sanoa	26,6%

16. Kuinka usein tietoturvakoulutusta tulisi mielestäsi järjestää?

Vastaajien määrä: 222

	Kuinka usein tietoturvakoulutusta tulisi mielestäsi järjestää?
Kaksi kertaa vuodessa	1,8%
Kerran vuodessa	25,2%
Kerran kahdessa vuodessa	27%
Tarpeen mukaan	42,3%
Muu vaihtoehto, mikä?	3,6%

Avoimet vastaukset: Muu vaihtoehto, mikä?

- Muutaman vuoden välein, jotta asia pysyy muistissa. Kuitenkin aina uusille työntekijöille.
- Uusille työntekiöille ja viiden vuoden välein muille kertaukseksi
- 5 vuoden välein kertaus
- Koulutus jokaiselle uudelle työntekijälle 1-2 tuntia
- Ohjeistus Intra-sivustolla
- Joka kolmas vuosi tai erityisen tarpeen ilmaantuessa.
- Kerran vuodessa, ja aina uuden työntekijän aloittaessa.
- 4 vuoden välein

17. Millä tavoin toivoisit tietoturvakoulutusta järjestettävän tulevaisuudessa?

Vastaajien määrä: 223

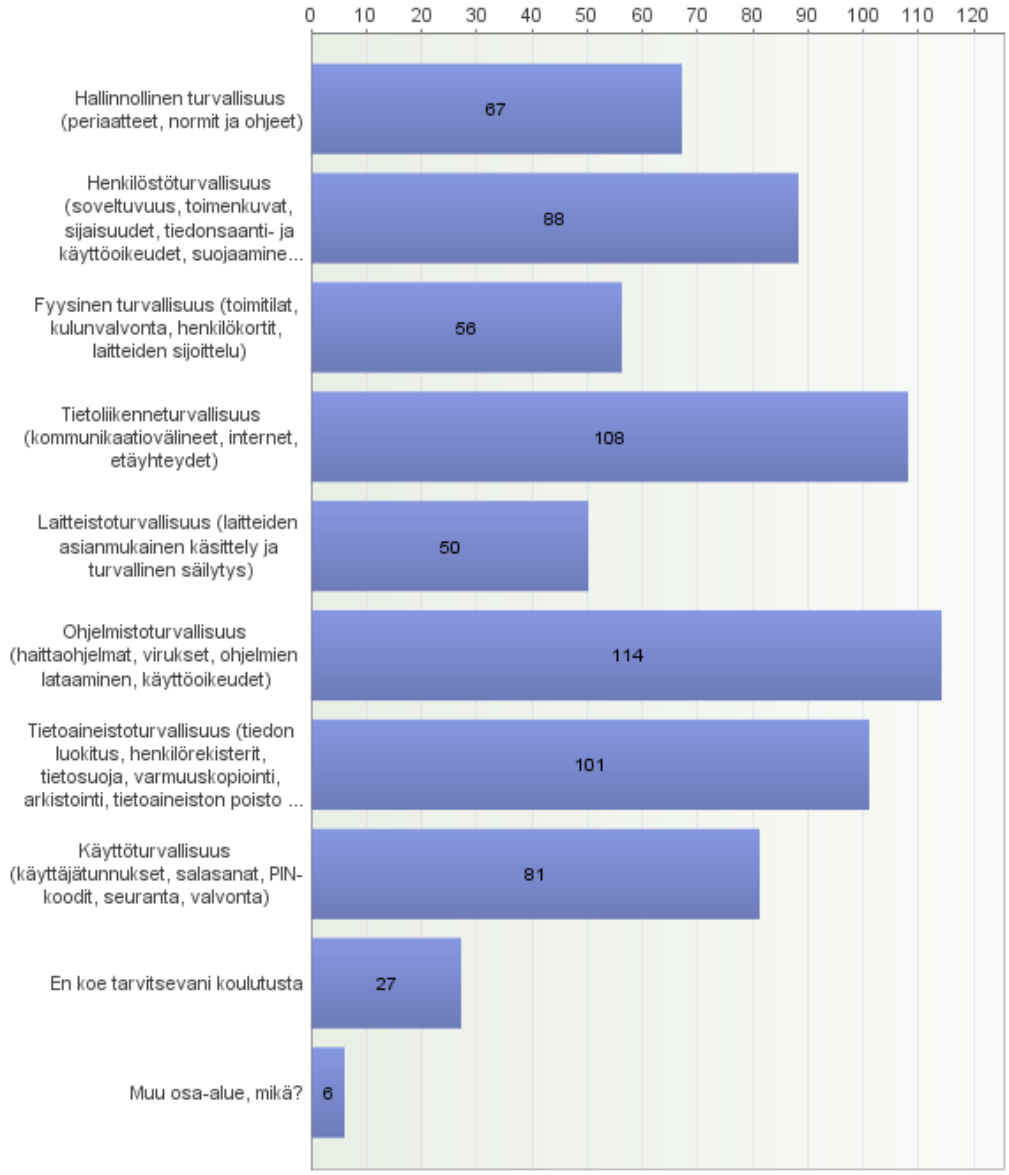
	Millä tavoin toivoisit tietoturvakoulutusta järjestettävän tulevaisuudessa?
Verkkokoulutus	53,8 %
Luennot	13 %
Verkkokoulutus ja luennot	34,1 %
Muu vaihtoehto, mikä?	1,8 %

Avoimet vastaukset: Muu vaihtoehto, mikä?

- Lähiopetus
- Tietourvaohjeistuksen säännöllinen päivittäminen Intrassa ja siitä viestittäminen työntekijöille sähköpostitse
- Lyncissä
- henkilökohtainen lyhyt opetus tietokoneella

18. Mihin tietoturvan osa-alueisiin toivoisit tulevaisuudessa koulutusta?

Vastaajien määrä: 220



Avoimet vastaukset: Muu osa-alue, mikä?

- tietojen järjestyksen ylläpito koneella
- kaikki yllä mainitut ovat tärkeitä näkökohtia
- Kaikkien käytössä olevien ohjelmien automaattinen päivitys lisää tietoturvallisuutta, ilman että päivitystä on jokaisen erikseen pyydettävä.
- en osaa sanoa
- Itse, seuraan muutenkin tietoturva-asioita, mutta koulutus on tosi tarpeellinen perus-käyttäjille
- Vanhojen kertausta ja uudet asiat, koska laitteet ja tekniikka kehittyy nopeasti

19. Minkälaista palautetta toivoisit koulutuksen suorittamisesta?

Vastaajien määrä: 31

- Lähinnä esimieheltä jonkinlaista huomiointia asian suhteen. Tulisi olo että asia on tärkeä kun siitä esimiehen kanssakin puhuttaisiin/käsiteltäisiin.
- Kahvitunnilla kyllä keskusteltiin, mutta ei missään virallisesti todettu, että hyvä homma, nyt me osataan.
- Ei aina netin kautta, en pidä näistä nettijutuista.
- Ei mitään.
- Sen, että on suorittanut hyväksytysti
- Verkkokoulutuksen jälkeen palaute kuinka työyhteisö / osasto pärjäsi.
- Olisi ollut kiva, jos esimies olis edes kuitannut saamansa tiedon, että olin suorittanut kurssin
- suoritusaika pitempi jotta voi valita kiireettömän ajankohdan töissä
- suoritus ok riittää
- Todistus riittää.
- Mikä kysymys tämä on? Koko henkilökunnalle järjestetään pakollinen netissä tehtävä monivalintatesti, josta puolet ei ymmärrä yhtään mitään, ei edes mitä testi käsittelee. Jos tietoturvasta tiesi vähänkään, testin läpäisi aineistoon perehtymättä. Jos taas tietoturvasta ei tiennyt mitään, koko homma tehtiin arpomalla tai työkaveri teki sen. Tuplatkaa testinläpäisseiden palkka, niin johan kiinnostaa.
- Keskustelua yhdessä siitä mitä tuli tehtyä
- En tarvi palautetta, näkihän sen Erkkikin kuinka monta pistettä siitä sai....
- Onko koulutuksen suorittanut henkilö ymmärtänyt asiat oikein.
- Nykyinen on oikein riittävä
- sähköinen palaute ja oma vastausprofiilit ovat riittävät
- hyväksytty/hylätty
- palautetta voisi tulla sähköpostilla
- Riittää, kun on saanut suoritettua koulutuksen.
- Koulutus oli hyvä ja tarpeellinen, mutta kuten aina käy niin tämäkin asia unohtuu tai vaipuu horrekseen mikäli sitä ei aika ajoin uusita.
- Loppukoe ja sen hyväksytty suorittaminen
- Ei palaute ole välttämätöntä kunhan itse tietää hyödyn.
- Tulostettava todistus oli hyvä.
- Lähiesimies antaisi palautteen ihan livenä. Pelkkä softan antama kiitos on turhan kliininen.
- Käsitteiden selventäminen.
- entinen käytäntö hyvä

20. Miten parantaisit koulutusta ja mitä tulevaisuudessa pitäisi tehdä?

Vastaajien määrä: 32

- Koulutuksessa pitäisi ottaa huomioon enemmän myös sitä todellisuutta, että monikaan ei juuri tiedä mitään tietoturvasta. Voisko olla joku yleispätevä paketti, jonka jokainen taho voisi liittää perehdytyskansioihin työpaikoilla, myös liikelaitokset, osakeyhtiöt.
- Olen yli 50 ja tietokoneet eivät ole "parhaat ystäväni", joten pitäisin nk yksinkertaista "kädestä pitäen opetusta" parhaana metodina. Meikäläisiä on paljon...
- joku oman alan henkilö puhumaan, että koskettaa...
- Verkkokoulutuksessa on hankalaa esittää kysymyksiä ja monet ei kehtaa jättää viestiä vaan olisi helpompi kysyä ja saada vastaus suoraan. Olen lähiopetuksen kannalla tai verkkokoulutus puheyhteydellä.
- Lyhyitä sessioita vaikka sitten useammin suoritettuna
- Monipuolinen luento käytännön esimerkkeineen.
- Koulutuksen jälkeen ydinasioita ja palautetta juuri meidän yksikkömme työssä olisi ollut hyvä käydä läpi henkilöstön yhteisenä koulutusteemana
- Selkeämmät kysymykset
- Tämän kurssin suorittaminen oli pakkopulla ja käytetty menetelmä (ohjelma) oppimi-

sen kannalta kehnohko. En oppinut juuri mitään uutta. Suoritin vain pakkopullan, mikä ei edistä myönteistä suhtautumista tietoturva-asioihin. Arvelen kuitenkin olevani aika "tietoturvallinen".
- Henkilöstöä tulisi kannustaa parantamaan tietoteknisiä valmiuksiaan ja taitojaan tukemalla nykyistä enemmän omaehtoista kouluttautumista kursseilla tai oppilaitoksissa. Nykyinen systeemi ei kannusta opiskelemaan.
- myös kaikille tilapäisille työntekijöille tarvitaan koulutusta (lomittajat ja kausityövoima)
- useampi tietokonealan kouluttaja voisi olla hyvä
- Nyt koulutus oli kai samanlainen sekä tietokoneisiin ja hallintoon pitemmälle perehtyneille että vasta aloittaville - osa toistosta oli turhauttavaa.
- Uudet käyttäjät, käyttäjätunnukset sulkeutuisivat, ellei ole suorittanut tietoturvaosiota, määrättyyn pvm mennessä esim. 1kk
- Pelkkä verkkokoulutus on siitä ikävä, että koulutuksen kuluessa herääviin kysymyksiin ei saa heti vastausta. Kysymyksiä ei tule esitettyä sitten mitään kautta ja joissain asioissa voi jäädä epätietoiseksi.
- Nykyisessä kyselyssä on muutama kysymys, jossa "oikea" vastaus riippuu siitä, miten kysymyksen tulkitsee. Kannattaisi päästä testikysymyksissä eroon tulkinnanvaraisuudesta. Jotain tietoturvallisuuskoulutusta voisi olla paikallaan järjestää myös pienryhmissä, jossa asioita voisi yhdessä tekemällä oppia.
  Pelkkä verkkokoulutus kun helposti jää yhden kerran asiaksi.
- Vanhemmat työntekijät eivät useinkaan ymmärrä tietotekniikasta hevon***. Koulutusta ei ole järjestetty tai jos järjestetään, siihen ei voi osallistua, kun ei saa hankkia sijaista. Aikoinaan, kun koulutus oli vielä mahdollista, koulutettiin järjestelmiä, jotka ovat poistuneet käytöstä jo aikaa. Valtaosa nuoremmista osaa ja ymmärtää tietotekniikasta sen verran, että nämä haistap…-"koulutukset" ovat silkkaa ajanhukkaa. Vanhemmille taas nämä ovat kuoleman paikkoja, kun jo sana tietoturvallisuus on käsittämätön. Mutta ihan kiva, että on vara haaskata kaupungin rahoja näiden suunnitteluun ja toteuttamiseen ja pakottaa työntekijät tekemään näitä omalla ajalla. Onpahan "koulutettu" porukkaa ja näyttää papereissa hyvältä.
- Tämä oli ihan hyvä juttu, mutta asioita voisi ehkä kertailla...
- Koulutus ei saa olla liian pitkä ja monimutkainen, on keskityttävä olennaiseen, muutoin ote repsahtaa ja se suoritetaan vain mahdollisimman nopeasti pois alta.
- Eritasoinen koulutus eri toimenkuvan omaaville työntekijöille (osastot)
- Minusta koulutus on asianmukainen jo nyt.
- nykyinen verkossa tapahtuva koulutus on hyvä
- Jokainen uusi työntekijä perehdyttää asiaa.
- koulutus on minusta riittävää
- Ehkä koulutusmateriaali voisi tulla aikaisemmin, mikäli sellaista on kirjallisena.
- Oman esimiehen kohdalla ei tullut mitään tietoa ko asiasta. Enkä edes tiedä miten omassa työyksikössäni koulutus suoritettiin. Palautteen käsittely työyksikön kanssa yhdessä olisi hyvä ja toivottava parannus. Olin etulyöntiasemassa koska olin mukana käynnistysvaiheessa, mutta jos en olisi ollut niin kysely olisi tullut ns. puun takaa.
- Kerran vuodessa esim. olisi ainakin muutaman kerran ja sitten tarpeen mukaan.
- Esimerkit ovat hyviä.

21. Muu palaute

Tässä voit vapaasti kommentoida niin tietoturvakoulutusta kuin tätä kyselyäkin.

Vastaajien määrä: 40

- Itselle koulutus sinänsä ei tuonut uutta asiaa, mutta on hyvä että koulutusta järjestetään. Voisiko koulutuksen uusijoilla olla vaikeampia tehtäviä, kuin ekakertalaisella? Se voisi lisätä kiinnostusta koulutukseen, kun joutuu jotain miettimään eikä vaan kertaamaan.
- Tein ensimmäisen kerran koulutuksen ja suoritin se ja sitten suoritusmerkintä oli kadonnut. Jouduin tekemään pakosta koulutuksen uudelleen , kaipa nyt osaan ;-) Ainakin tulostin todistuksen näkösälle.
- Kohdassa 14. olin monessa kohdin täysin eri mieltä, koska asiat olivat jo entuudestaan tuttuja, joten uutta ei paljoakaan tullut.
- Tietoturvakoulutus on tarpeellinen asia. Pitäisi kuitenkin muistaa, että kaikki käyttäjät

eivät ole "nörttejä" eivätkä välttämättä osaa kaikkia temppuja, joten opetus pitäisi olla sellaista, että välillä käytettäisiin rautalankaa... B)

- Koulutuksesta on sen verran aikaa, etten kykene muistamaan materiaaliin liittyviä yksityiskohtia kovin tarkasti. Suuri osa asiasta oli joka tapauksessa jossain määrin tuttua, eikä materiaalin silmäilyyn ja testin tekemiseen kulunut kovin paljon aikaa. Koulutuksen suorittaminen ei juuri rasittanut, mutta ei myöskään tarjonnut paljoakaan uutta työn kannalta.
- Nyt koulutus oli vähän läpihuutojuttu
- Tästä kyselystä - fonttikoko hieman suuremmaksi, muuten ihan ookoo.
- Selkeitä!
- Monivalintakysymysten vastausten järjestys oli poikkeava, yleensä en osaa sanoa on keskellä.
- kysely ihan ok, koulutus voisi olla hyvä, vaikkapa halvallakin
- Tietoturvasta ja eri teemoista vois laittaa tietoiskuja? Esim. Lanssiin i- tyyliin - muistatahan että... ja tietoa löytyy linkistä alla....
- Koulutuksen suorittamisesta on jo sen verran aikaa, että en oikein hyvin muistanut sitä miten se meni. Mutta eiköhän vastaukset suunnilleen pidä paikkansa :)
- Kuulee monesti sanottavan, että pitäisi olla vain yksi salasana, jolla pääsee kaikkiin, ohjelmiin, mihin on oikeudet. Ovien sulkemisesta ja esim. kannettavien salauksesta kuulee vieläkin sanottavan, että miksi pitää olla niin monta salasanaa, kuka näitäkin tarvitsee ja julkisia asioitahan käsittelemme??? ASENNE KOHDALLEEN KAIKILLE!
- Tämä kysely tuli niin pitkän ajan kuluttua ko. koulutuksesta, että en oikein muista millainen se rakenteeltaan oli.
- Tämän kyselyn olisi voinut tehdä vähän aikaisemmin kun asiat oli vielä tuoreena muistissa
- Pyydettiin palautetta ja sitä annettiin. Ei henkilökohtainen hyökkäys, mutta alalla on aika pirusti hommia ilman tällaisia joutavanpäiväisyyksiäkin.
- Tietoturvakoulutukset ovat tärkeitä, vanhan jo tiedossakin olevan tiedon tärkeys korostuu, tietoturva-asiat eivät ole koskaan liikaa esillä.
- Prosessin toteutuksesta on kulunut jo sen verran aikaa, että sen olen jättänyt taka-alalle. Koulutus oli ns. pakollinen ja kuuluukin olla. Koulutus (verkossa toteutettu) oli kovin massiivinen ja vuosittain tai tiheämmin raskas toteuttaa. Miten vaihtuva väki huomioidaan ja millä tavalla uudet työntekijät velvoitetaan suorittamaan koulutuksen -seuranta?
- Onkohan tarpeen vaihtaa niin usein salasanoja kuin organisaatiossa nykyään pakotetaan ????
- Negatiivinen suhtautumiseni asiaan johtui täysin siitä, että muutama päivä ennen koulutusajan loppua tuli käsky tehdä se. Ja kun kyse oli vielä vuoden kiireisimmästä ajasta, niin harmitus oli aika korkealla ja muutama kirosana pääsi. Asiahan oli ihan hyvä ja tarpeellinen, mutta tietoa sen tekemisestä oli kyllä hyvin piiloteltu jossain ES-Sissä...
- Monet pitivät kyselyä hankalana ja kiusallisena ja jotkut jopa toivoivat jonkun muun suorittavan sen puolestaan. Ihmiset jotka käyttävät vähän tietokonetta on vaikea omaksua edes perusasioita, kuten tallentamista ja siirtymistä toiselle sivulle.
- Kyselyyn vastaaminen tosi hankalaa, koska muistissa ei ole mitään koskien kyseistä tietoturvakoulutusta. Ainoastaan hajanainen muistikuva, että jotain taisi joskus olla.
- Koulutuksen suorittamisesta on kulunut niin paljon aikaa, että vaikea muistaa koulutusaineiston laatua ja sujuvuutta.
- Koulutuksesta on jo niin kauan, että tuskin muistin mistä oli kysymys. Siksi useimmat vastaukset niin negatiivisia, valitettavasti.
- kysely asiallinen ja selkeä vastata
  Tällainen kysely olisi ollut paikallaan jo aiemmin, koska koulutuksestani on yli vuosi. Ja anteeksi vaan, mutta nyt tuli aikapula, enkä ehdi vastaamaan kaikkiin! Matka edessä!
- aivan mielenkiintoinen
- Tämä kysely olisi pitänyt tehdä jo heti kun täyttöaika kyselyyn päättyi. Ei tahtonut enää muistaa yksityiskohtia.
- Kysely olisi pitänyt tehdä melko nopeasti koulutuksen päättymisen jälkeen. Ihan ei tarkalleen muista miten koulutus meni mutta ymmärrän tämän kyselyn ajankohdan nyt.
- Kysely oli selkeä ja sopivan pituinen, ei vienyt liikaa aikaa (onneksi).
- Tietoturvakoulutuksesta on niin pitkä aika tähän kyselyyn, että siitä ei muista juuri

mitään. Siksi on vaikea vastata kaikkiin kysymyksiin.

- Koulutus hyvä, mutta minulla oli osaaminen jo ennen koulutusta
- Tämä kysely olisi pitänyt toteuttaa jo 2012 vuoden alussa, koska eihän nyt enää meinannut muistaa...
- Jatkuvassa tietotekniikan uudistumisessa pitää olla valveutunut.
- Koulutuksesta on jo jonkinverran aikaa, joten osa siihen liittyvästä koulutusmenetelmästä on jo unohtunut.
- hei en ole enää työnjohtajan asemassa joten tämä tietoturvajuttu on sikäli tarpeeton etten työssäni tarvitse enää tietokonetta .
- salasanojen määrää helpottaa ja vähentää kaikesta tietoturvasta huolimatta!
- Joissakin rasti ruutuun kysymyksissä oli useampia väittämiä samassa, Vaikea päättää kumpaan vastaa