Tampereen ammattikorkeakoulu

TIETOTURVA- JA TIETOSUOJATUTKIMUS ORGANISAATIOSSA

Juha Manninen

OPINNÄYTETYÖ
Toukokuu 2019

Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tieto- ja viestintätekniikka
Tietoliikennetekniikka ja tietoverkot

MANNINEN, JUHA:
Tietoturva- ja tietosuojatutkimus organisaatiossa

Opinnäytetyö 36 sivua, joista liitteitä 3 sivua
Huhtikuu 2019

Opinnäytetyönä toteutettiin tietoturva- ja tietosuoja-aiheinen tutkimus julkishallinnon organisaatiolle. Työn tavoitteena oli tutkia organisaatiossa havaittuja tietoturva- ja tietosuojariskejä ja ongelmia. Tutkimuksen tulosten avulla mietittiin parannusehdotuksia organisaation tietoturvan ja tietosuojan parantamiseksi. Tutkimuksessa tiedon keräämiseen käytettiin kyselylomaketta. Kyselylomake lähetettiin organisaation henkilöstölle. Kyselylomakkeella kartoitettiin organisaation työntekijöiden ja esimiesten itse työssään kohtaamia tietoturva- ja tietosuojaongelmia. Kysely koostui monivalintakysymyksistä sekä tarkentavista avoimista kysymyksistä. Tutkimus kohdistettiin vain osaan organisaatiota ja kyselyn vastaajiksi valittiin tietyn suuruinen satunnaisotos.

Kyselyyn vastasi lopulta hieman alle puolet valitusta otoksesta. Kyselyn tuloksia analysoitiin ja mietittiin erilaisia kehityskohteita organisaation tietoturvan ja tietosuojan parantamiseksi. Tulosten avulla huomattiin valtaosan vastaajista suhtautuvan tietoturvaan ja tietosuojaan sekä niiden tilaan organisaatiossa positiivisesti. Suurin osa kyselyn tuloksista esille nousseista tietoturva- ja tietosuojaongelmista liittyivät henkilöstön huolimattomuuteen ja mahdolliseen välinpitämättömyyteen. Merkittävimmäksi parannusehdotukseksi organisaation tietoturvan ja tietosuojan kannalta määritettiin tietoturva- ja tietosuoja-asioiden tärkeyden painotus henkilöstölle ja mahdollisesti tarkempi perehdytys näissä asioissa.

Asiasanat: tietoturva, tietosuoja, organisaatio

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Information and Communications Technology
Telecommunications and networks

MANNINEN, JUHA:
Cyber security and data protection study in an organization

Bachelor's thesis 36 pages, appendices 3 pages
April 2019

The objective of this study was to research and analyze cyber security and data protection threats and problems in a public organization. The results of the research were used for identifying the weaknesses of the organization with cyber security and data protection and suggest ways to improve them. The data were collected from the employees and superiors of the organization themselves with a questionnaire. The questionnaire consisted of multiple choice questions and also some open more specific open-ended questions. The research was focused only on a part of the organization. There was also a random sample selected to take part in the inquiry.

Less than half of the random sample answered the questionnaire. The majority of the participants believed that cybersecurity and data protection are taken care of well in the organization. There were also some risks and threats, which stood out among the rest. Most of them had something to do with personnel of the organization not paying enough attention or maybe being careless, when dealing with cyber security and data protection. The improvement that was suggested was simply to emphasize the importance of cyber security and data protection to the personnel. Also giving detailed information to new employees about cyber security and data protection.

Key words: cyber security, data protection, organization

SISÄLLYS

LYHENTEET JA TERMIT

DoS	Palvelunestohyökkäys
DDoS	Hajautettu palvelunestohyökkäys
GDPR	EU:n yleinen tietosuoja-asetus
Social engineering	Sosiaalinen manipulointi
Tarkistussumma	Tietotekniikassa käytetty tarkistuskoodaustapa
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johto-ryhmä
VPN	Virtuaalinen erillisverkko

1 JOHDANTO

Yhteiskunnan muuttuminen yhä tietokeskeisemmäksi on korostanut tietoturvan merkitystä entisestään ja tietoturvallisuus onkin noussut tärkeäksi osaksi turvallisuutta. Tietoverkkojen kautta tapahtuva rikollisuus ja muu harmin aiheuttaminen on tuonut mukanaan paljon uusia uhkia. Uudenlaisia tietoturvauhkia tulee koko ajan lisää ja siksi on tärkeää, että jokaisella on edes jonkinlainen käsitys tietoturvasta, sillä tietoturvauhkilta suojautumisessa tärkeimpänä tekijänä on lopulta käyttäjä itse.

Yritysten ja organisaatioiden kannalta tietoturvan ja tietosuojan merkitys on myös kasvanut merkittävästi. Mahdollisten tietoturvapoikkeamien raportointi ja henkilöstön kouluttaminen ovat tärkeässä asemassa, kun puhutaan organisaation tietoturvallisuuden ylläpitämisestä ja parantamisesta.

Tässä opinnäytetyössä toteutettiin tietoturva ja tietosuoja aiheinen tutkimus eräälle julkishallinnon organisaatiolle. Tutkimuksen tarkoituksena on kartoittaa kyseisen organisaation henkilöstön työssään kohtaamia tietoturva- ja tietosuojariskejä. Tutkimus toteutettiin organisaation henkilöstölle lähetettävällä kyselylomakkeella. Kyselyn tulosten avulla pohditaan mahdollisia kehityskohteita tietoturvan parantamiseksi organisaatiossa. Jotta tutkimuksen työmäärä saatiin pidettyä kohtuullisena, tutkimus rajattiin vain osaan tätä organisaatiota. Lisäksi kyselyä varten valittiin tietynsuuruinen otosjoukko.

2 TIETOTURVA

Tietoturva on käsitteenä laaja, mutta sen voidaan katsoa tarkoittavan kaikkien tietojen, tietojärjestelmien ja tietoliikenteen turvaamista. Tietoturvan merkitys on nykypäivänä suuressa roolissa. Tietoturvaan kohdistuu monenlaisia uhkia ja niitä tulee jatkuvasti lisää. Tietoturvan ylläpitämiseen käytettävien toimenpiteiden on pysyttävä ajan tasalla uusien uhkien kanssa. Tietoturvaan ajatellaan usein liittyvät erilaiset tietotekniset uhat, kuten tietokonevirukset. Tietoturvaan kuuluu kuitenkin muitakin osa-alueita kuin vain teknisiin toimenpiteisiin liittyvät ratkaisut. Seuraavasta luettelosta nähdään tietoturvan osa-alueet. (tietojesiturvaksi.)

- Hallinnollinen tietoturva
- Fyysinen tietoturva
- Laitteistoturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineiston turvallisuus
- Tietoliikenneturvallisuus
- Henkilöstöturvallisuus
- Käyttöturvallisuus

Edellä olevassa listassa on lueteltu tietoturvan osa-alueet. Tietoturvaa voidaan määritellä myös eri tavalla. Usein tietoturvaa määriteltäessä sen katsotaan jakautuvan tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen.

2.1 Tiedon luottamuksellisuus

Tiedon luottamuksellisuuden tarkoituksena on estää pääsy tietoihin niiltä, joilla ei ole siihen valtuuksia. Tiedon luottamuksellisuudesta hyvänä esimerkkinä ovat kaikenlaiset järjestelmät, jotka vaativat käyttäjäntunnuksen ja salasanan. Esimerkiksi sähköpostin salasana on henkilökohtainen ja sen antaminen toiselle rikkoo tiedon luottamuksellisuutta. Jokainen käyttäjä voi parantaa tiedon luottamuksellisuutta. Esimerkiksi valitsemalla itselleen hyviä ja tehokkaita salasanoja, huolehtimalla tiedon turvallisesta hävittämisestä, sekä tiedostojen metatietojen poistamisesta. (Yksityisyydensuoja.)

2.2 Tiedon eheys

Tiedon eheyden tarkoitus on varmistaa tiedon muuttumattomuus. Tiedon muuttumisella eheyden yhteydessä tarkoitetaan nimenomaan tahallista tietojen muuttamista esimerkiksi hyökkäyksen yhteydessä. Tiedon eheyttä voidaan ylläpitää tarkistamalla tiedon oikeellisuus aina kuin mahdollista, mikä on osa tiedon eheyttä. Tiedon oikeellisuus voidaan tarkistaa esimerkiksi tiedoston tarkistussumman avulla. Tarkistussumman luomiseen käytetään kryptograafista tiivistefunktiota, jolloin sen muuttumattomuus voidaan taata. Tarkistussumman tarkoituksena on, että jokainen tiiviste on erilainen. Samaa tiivistearvoa ei myöskään ole tarkoitus saada toiselle kohteelle. Tarkistussummasta ei myöskään voi päätellä alkuperäistä lähdettä. (Yksityisyydensuoja.)

2.3 Tiedon saatavuus

Tiedon saatavuuden tarkoitus on, että vain oikeuden omaavat henkilöt pääsevät tietoihin käsiksi. Asiakirjojen pitää olla helposti saatavilla, niille keille tieto kuuluu. Tiedon saatavuutta on helppo jokaisen käyttäjän parantaa. Tietojen varmuuskopiointi ja niiden suojaaminen haittaohjelmilta ovat hyviä tapoja parantaa tietojen saatavuutta. (Yksityisyydensuoja.)

2.4 Tiedon kiistämättömyys ja todennus

Tiedon luottamuksellisuuden, eheyden ja saatavuuden lisäksi tietoturvan käsitettä voidaan myös laajentaa kiistämättömyydellä, tunnistuksella ja todennuksella. Kiistämättömyydellä tarkoitetaan, että jotkin tapahtumat voidaan jälkikäteen todistaa jonkin käyttäjän tekemäksi. Todennuksella tietojärjestelmän käyttäjä todistetaan valtuutetuksi käyttäjäksi. (tietojesiturvaksi.)

2.5 Tietosuoja

Tietosuoja on osa tietoturvaa, jolla pyritään henkilötietojen turvaamiseen. Tietosuoja perustuu lakiin, ja sillä on tarkoitus määrittää milloin ja miten henkilötietoja voidaan käsitellä. Tietoturva on tietosuojan toteuttamisen keino. Sen tarkoitus on suojata tietoaineisto ja tietojärjestelmät. (tietosuojavaltuutetun toimisto.)

2.5.1 GDPR

GDPR eli General Data Protection Regulation (yleinen tietosuoja-asetus) on 25.5.2018 voimaan astunut henkilötietojen käsittelyä sääntelevä laki. GDPR:n avulla pyritään antamaan parempi suoja henkilötiedoilla ja enemmän tapoja hallita tietojen käsittelyä. GDPR on voimassa kaikissa EU-maissa. (tietosuojavaltuutetun toimisto.)

3 TIETOTURVA ORGANISAATIOSSA

Nykypäivän yhteiskunnasta on tullut todella tietokeskeinen. Tietojärjestelmiä on useita ja tietoa liikkuu todella paljon. Nämä kaikki tietysti edelleen korostavat tietoturvan merkitystä. Tietoturva on välttämätöntä organisaatioiden toiminnalle. Tietoturva koskettaa jokaista organisaation jäsentä. Tietoturvasta huolehtiminen ei kuulu pelkästään IT- ja tietoturva-ammattilaisille.

3.1 Tietoturvan ja tietosuojan vaatimukset

Monissa organisaatioissa ja yrityksissä on tiettyjä vaatimuksia ja standardeja, joita niiden tietoturvapolitiikat noudattavat. Tässä työssä tehtävä tutkimuksen kohdeorganisaation tietoturvavaatimukset pohjautuvat ISO/IEC 27001 standardiin. Myös Euroopan tietosuojaneuvoston soveltamisohjeita käytetään. Organisaation tietoturvallisuutta ohjaavat lisäksi myös VAHTI eli julkisen hallinnon digitaalisen turvallisuuden johtoryhmän ohjeet sekä JUHTA eli julkisen hallinnon tietohallinnon neuvottelukunnan JHS-suositukset. (tietoturva- ja tietosuojapolitiikka.)

Kohdeorganisaation tietoturvan ja tietosuojan toimintaa ohjeistetaan myös lainsäädännön kautta. Tästä esimerkkejä ovat seuraavat säädökset.

- EU:n yleinen tietosuoja-asetus 2016/679
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Henkilötietolaki (523/1999)
- Laki yksityisyyden suojasta työelämässä (477/2001)
- Tietoyhteiskuntakaari (917/2014)
- Yhteiskunnan turvallisuusstrategia (2017)
- Valmiuslaki (1552/2011)
- Laki kansanvälisistä tietoturvallisuusvelvoitteista (588/2004)

3.2 Tietoturvapoikkeama

Tietoturvapoikkeama on tapahtuma, jonka seurauksena organisaation vastuulla olevien tietojen tietoturvallisuus on tai saattaa olla vaarantunut. Tällaiset poikkeamat voivat esimerkiksi johtaa tietojen tuhoutumiseen tai häviämiseen. Kun tietoturvapoikkeamia tapahtuu, niihin on tärkeää reagoida nopeasti. Poikkeamien dokumentointi ja analysointi on myös tärkeää, jotta voidaan löytää mahdollisia kehityskohteita. Voidaan esimerkiksi selvittää, mistä tietoturvallisuuden osa-alueesta henkilöstö saattaisi tarvita lisää koulutusta tai ohjeistusta. Henkilötietoihin kohdistuva poikkeamaa kutsutaan tietosuojapoikkeamaksi. (Tietoturvapoikkeamien tunnistaminen.)

3.2.1 Tietoturvaloukkaus

Henkilötietojen tietoturvaloukkaus on tapahtuma, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi

- hävinnyt tiedonsiirtoväline, kuten USB-tikku
- varastettu tietokone
- hakkerointi
- haittaohjelmatartunta
- kyberhyökkäys
- tulipalo datakeskuksessa

Tietoturvaloukkauksesta voi olla organisaatiolle paljon haittaa, sillä siitä voi esimerkiksi menettää henkilötietojen valvomiskyvyn. (tietosuojavaltuutetun toimisto.)

4 TIETOTURVAN TOTEUTTAMINEN

Tietoturvan toteuttamisella tarkoitetaan niitä teknisiä toimenpiteitä, joiden avulla tietoturvaa toteutetaan ja ylläpidetään. Tietoturvan toteuttamiseen on monia eri tapoja ja välineitä kuten virustentorjuntaohjelmat sekä salasanat.

4.1 Virusturva ja palomuuri

Virustorjuntaohjelmilla pyritään torjumaan erilaisia haittaohjelmia, kuten viruksilta, troijalaisilta tai madoilta. Haittaohjelmia on monia erilaisia ja niitä voidaan luokitella esimerkiksi sen mukaan, mitä ne tekevät tai miten ne leviävät. Kaikki haittaohjelmat kuitenkin pyrkivät jollain tasolla tekemään vahinkoa. Virustorjuntaohjelmia voi käyttää tarkistamaan tiedostoja, muistitikkuja tai vaikkapa kovalevyjä virusten varalta. Virustorjuntaohjelmien päivittäminen on myös tärkeää, sillä uudenlaisia haittaohjelmia ilmestyy nopealla tahdilla, ja virustorjuntaohjelmien on pysyttävä ajan tasalla. F-Securen tutkimusjohtaja Mikko Hyppönen kertoi vuonna 2012, että haittaohjelmat Stuxnet ja DuQu kerkesivät olla aktiivisina yli vuoden ja haittaohjelma Flame jopa kaksi vuotta, ennen kuin tietoturvayhtiöt tunnistivat ne. (Yksityisyydensuoja.)

Palomuuri on toisenlainen tapa suojata tietokonetta ulkopuolelta tulevilta hyökkäyksiltä. Palomuuri on järjestelmä, joka on toteutettu joko ohjelmisto- tai laitteistopohjaisesti, ja jonka tarkoituksena on valvoa verkkojen välillä, sekä estää asiaton pääsy esimerkiksi lähiverkkoon. Yritysten ja organisaatioiden verkoissa on usein monia palomuureja. (Yksityisyydensuoja.)

4.2 Salasanat

Käyttäjätunnus-salasanapari on paljon käytetty tapa henkilön todentamiseen sekä tunnistamiseen erilaisissa tietojärjestelmissä. Salana on melko yksinkertainen mutta toimiva ratkaisu varmistaa, että vain oikeat henkilöt pääsevät käsiksi suojattuun tietoon. Vaikka salasanat ovatkin monesti toimiva ratkaisu, ei niitä ole

mahdoton murtaa. Salasanan selvittämiseen on useita tapoja, joista helpoin on yksinkertaisesti vain arvata se. Tästä syystä on tärkeää olla käyttämättä helposti arvattavia salasanoja. Helposti arvattavia salasanoja on esimerkiksi käyttäjän tietoihin liittyvät salasanat, kuten esimerkiksi syntymäpäivän käyttäminen salasanana. Lisäksi kannattaa välttää käyttämästä yleisiä salasanoja, kuten ”1234” tai ”qwerty” tai vastaavia. (yksityisyydensuoja).

Toinen tehokas tapa salasanan selvittämiseen on sen murtaminen väsytystekniikalla (engl. brute force). Tämä tekniikka perustuu siihen, että käydään kaikki mahdolliset vaihtoehdot läpi. Tämä tekniikka tosin vie usein paljon aikaa salasanasta riippuen. Usein luullaan. että monimutkainen salasana ja runsas erikoismerkkien käyttö suojaa parhaiten, mutta todellisuudessa salasanan pituus on tärkeämpää. Erityisesti brute force tekniikkaa vastaan pitkä salasana on todella hyvä, sillä se pidentää laskenta-aikaa. Alla olevassa taulukossa vertaillaan salasanaa, jossa on käytetty vain pieniä kirjaimia, sekä salasanaa, jossa on käytetty kaikki näppäimistön merkkejä. Taulukosta nähdään, että esimerkiksi 12-merkkinen salasa, jossa on käytetty ainoastaan pieniä kirjaimia, on parempi, kuin 8-merkkinen, jossa on käytetty kaikki näppäimistön merkkejä. Pitkä ja yksinkertainen salasana on siis turvallisempi ja suojaa paremmin, kuin lyhyt ja monimutkainen salasana. (yksityisyydensuoja).

Taulukko 1. Salasanan merkkien määrä ja käytetyt merkit (Yksityisyydensuoja salasanat)

Pituus	Vain pienet kirjaimet (29)	Kaikki näppäimistön merkit (107)
6	594 823 321	1 500 730 351 849
7	17 249 876 309	160 578 147 647 843
8	500 246 412 961	17 181 861 798 319 201
9	14 507 145 975 869	1 838 459 212 420 154 507
10	420 707 233 300 201	196 715 135 728 956 532 249
11	12 200 509 765 705 829	21 048 519 522 998 348 950 643
12	353 814 783 205 469 041	2 252 191 588 960 823 337 718 801
13	10 260 628 712 958 602 189	240 984 500 018 808 097 135 911 707
14	297 558 232 675 799 463 481	25 785 341 502 012 466 393 542 552 649
15	8 629 188 747 598 184 440 949	2 759 031 540 715 333 904 109 053 133 443

4.3 Etätyö ja kannettavat laitteet

Etätyö tarjoaa työntekijälle mahdollisuuden tehdä työtä muuallakin kuin vain työpaikallaan. Etätyön avulla työntekijä ei ole sidonnainen yhteen työympäristöön ja työpisteeseen, vaan töitä voi tehdä esimerkiksi kotoa käsin. Etätyö tuo kuitenkin mukanaan myös omia tietosuojaan liittyviä asioita, joista pitää huolehtia. Etätyöympäristössä ei pääse hyödyntämään työpaikan tietoturvamekanismeja, joten se saattaa rajoittaa työtehtävien määrää. Työpisteen pitäminen puhtaana työasioista, työasioista puhuminen ulkopuolisten kuullen ja it-työvälineistä huolehtiminen korostuvat etätyössä.

Etätyötä tehdessä on myös tärkeää käyttää suojattua ja luotettavaa verkkoa. Esimerkiksi oman langattoman lähiverkkonsa tietoturvaa kannattaa suojata salasanalla. Etätyössä yhteyden muodostamiseen yrityksen tai organisaation verkkoon käytetään VPN-yhteyttä. Salatun VPN:n käyttäminen ehkäisee tietoliikenteen kuuntelua. (Viestintävirasto Kyberturvallisuuskeskus, 2015.)

5 ORGANISAATION TIETOTURVAUHKIA

Organisaatioihin ja yrityksiin tietoturvauhkia on paljon erilaisia ja niiden tunnistaminen ja oikea reagointi niihin ovat organisaation tietoturvallisuuden kannalta tärkeää.

5.1 Yleisimpiä tietoturvauhkia organisaatioissa

Kaikissa tai varmaankin melkein kaikissa organisaatioissa kohdataan jonkin asteisia tietoturvauhkia. Kuvassa 1 on viestintäviraston kyberturvallisuuskeskuksen julkaisemat top 5 tietoturvauhat ja ratkaisut organisaatioissa vuodelta 2017.

KUVA 1. Organisaatioiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017 (Viestintävirasto Kyberturvallisuus 2018)

Tässä opinnäytetyössä tehtävä tutkimus ja siihen kuuluva kysely liittyvät myös näihin samoihin asioihin kuin yllä olevassa taulukossa. Alla on esitelty muutamia organisaatioiden tietoturvauhkia hieman tarkemmin.

5.1.1 Palvelunestohyökkäys

Palvelunestohyökkäys eli Denial of Service (DoS) tarkoittaa verkkohyökkäystä, jolla pyritään estämään jonkin verkkosivuston tai palvelun käyttö. Palvelunestohyökkäyksen toteuttamiseen on erilaisia menetelmiä, mutta yleisin tapa on kohdistaa verkkosivustoon/palveluun niin paljon liikennettä, että asiakkaiden palvelu ei ole enää mahdollista. Voidaan puhua myös hajautetusta palvelunestohyökäyksestä eli Distributed Denial of Service (DDoS). Tämä tarkoittaa, että hyökkäys tulee useista lähteistä, käyttäen esimerkiksi bottiverkkoa. (Viestintävirasto Kyberturvallisuuskeskus 2016.)

Palvelunestohyökkäyksellä ei oikeastaan vaikuteta tiedon eheyteen ja luottamuksellisuuteen, sillä itse palvelun sisälle ei hyökätä. Palvelunestohyökkäys keskittyy nimenomaan tiedon saatavuuden vaikeuttamiseen. Palvelunestohyökäysten toteuttaminen internetissä ei ole mitenkään vaikeaa ja niitä on vaikeita estää.

5.1.2 Tietojenkalastelu ja sosiaalinen manipulointi

Tietojen kalastelulla eli verkkourkinnalla pyritään saamaan luottamuksellisia tietoja esiintymällä tahona, joka olisi siihen oikeutettu. Yleensä tietoa, jota yritetään urkkia, ovat henkilötiedot, tilitiedot ja salasanat. Tietojen kalasteluun käytetään yleensä sähköpostiviestejä. Lähetetään jonkin palveluntarjoajan nimissä viestiä asiakkaille ja kysellään asiakkaan tietoja.

Microsoftin pilvessä toimivan Office 365 sähköpostin kautta tapahtuvat kalastelut ovat erittäin yleisiä. Useita suomalaisia yritysten johtajia ja työntekijöitä joutui hyökkäysten kohteeksi kevään 2018 aikana. Tietojen kalastelun osaltakin on tärkeää käyttää resursseja sen torjuntaan, sekä kouluttaa henkilöstöä. Kalastelut kohdistuvat usein yritysten ja organisaatioiden johtoryhmän jäseniin (kyberturvallisuuskeskus 2019)

Social engineering eli sosiaalinen manipulointi tarkoittaa, että rikolliset yrittävät huijaamalla tai harhauttamalla saada ihmisiä antamaan tietoa heille. Sosiaalisessa manipuloinnissa merkittävässä osassa on ihmisten hyväuskoisuus ja se,

miten rikolliset hyödyntävät sitä. Kohde yritetään saada luottamaan hyökkääjään. Yleensä luottamusta voidaan yrittää saada esiintymällä jonakin luotettavana tahona, kuten pankkina. Huijaussivustot voivat usein olla ulkonäöltään täysin identtisiä oikeaan sivustoon, mutta yleensä sivuston pystyy erottamaan huijaukseksi osoiterivin avulla. (kyberhygieniaopas.)

5.1.3 Käyttäjät

Suurin tietoturvariski yritykselle/organisaatiolle on sen omat työntekijät. Vastuu tietoturvasta on lopulta melkein aina itse käyttäjillä. Tietoturvaohjelmat ja erilaiset sovellutukset auttavat parantamaan tietoturvaa tiettyyn pisteeseen asti, mutta käyttäjien pitää olla myös perillä asioista. Tekniset tietoturvaratkaisut eivät välttämättä estä ihmisten tekemiä virheitä.

Tässäkin opinnäytetyössä tehtävä tutkimus tutkii nimenomaan kohdeorganisaation työntekijöiden kohtaamia tietoturvariskejä omassa työssään. Monet näistä riskeistä ovat itse työntekijöiden aiheuttamia, olkoon ne sitten tahallisia tai tahattomia. Jotta organisaation tietoturva olisi hyvällä pohjalla, on tietoturvaan liittyvien asioiden perehdytys työntekijöille oltava kunnossa.

6 TUTKIMUS

Tässä opinnäytetyössä tutkimuksen aiheena oli tutkia organisaatiossa kohdattuja tietoturva- ja tietosuojauhkia. Tutkimuksessa käytettiin tiedon keräämiseen kyselomaketta, jolla kerättiin kohdeorganisaation henkilöstön kokemuksia erilaisista tietoturva- ja tietosuojauhkista.

6.1 Tutkimusmenetelmä

Kyselytutkimus on yleinen tutkimusmenetelmä, jolla kerätään tietoa vastaajajoukolta kysymysten avulla. Kysymykset voivat olla monivalintakysymyksiä tai avoimia kysymyksiä. Kyselytutkimuksella saa kerättyä paljon tietoa laajastakin kohderyhmästä. Kysely on myös melko helppo ja tehokas menetelmä. Kyselytutkimuksen huono puoli on, että tulokset voivat olla pinnallisia eivätkä välttämättä vastaa siihen, mitä oltiin tutkimassa. Kyselyssä on tärkeää muodostaa kysymykset vastaajien kannalta ymmärrettäviksi. Kyselytutkimus valittiin tässä opinnäytetyössä tehtävään tietoturvatutkimukseen tutkimusmenetelmäksi, koska se tuntui helpoimmalta ja resurssien puitteissa järkevimmältä tavalta tutkia kyseistä asiaa.

6.2 Tutkimuksen toteuttaminen

Tässä opinnäytetyössä tehtävässä tutkimuksessa tiedon keräämiseen käytettiin siis kyselomaketta. Kyselylomakkeen sisältö muodostettiin, niin että se kattoi mahdollisimman hyvin tutkittavaa asiaa, ja että sillä saataisiin vastaajien näkemykset esiin. Toisaalta kyselyyn käytettävän vastausajan oli pysyttävä kohtuullisena. Kyselyn lopullisen version arvioitu vastausaika oli noin 10-30 minuuttia. Kysely koostui 28 kysymyksestä, joista muutama ensimmäinen oli vastaajan taustatietoihin liittyviä kysymyksiä. Loput kysymykset liittyivät henkilöstön työyhteisössä kohdattuihin tietoturva – ja suojaongelmiin ja riskeihin. Näissä kysymyksissä oli vastausvaihtoehdot kyllä, ei ja en osaa sanoa. Kysymykset oli lisäksi

lajiteltu muutaman kysymyksen ryhmiin, niin että samaan aiheeseen liittyvät kysymykset olivat yhdessä. Jokaisen ryhmän lopussa oli avoin vastauskenttä, johon vastaaja voi tarkentaa sen ryhmän kysymysten vastauksiaan.

6.3 Kohderyhmä

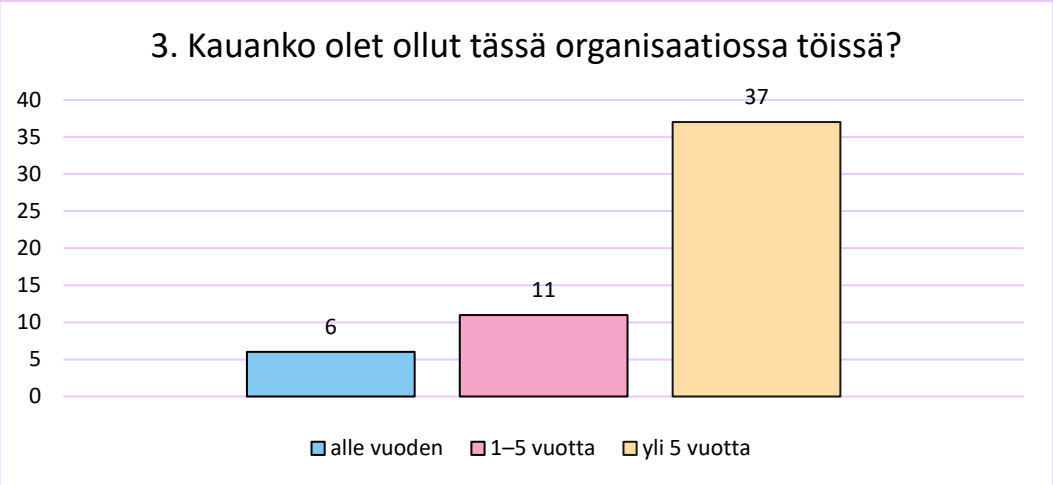
Kuten jo aiemmin on mainittu, tässä opinnäytetyössä tehty tietoturva- ja tietosuoja aiheinen tutkimus tehtiin julkishallinnon organisaatiolle. Tutkimus rajattiin vain erääseen osaan tätä organisaatiota. Tutkimuksessa käytetty kysely lähetettiin 100 työntekijälle ja 25 esimiehelle, jotka valittiin satunnaisesti.

7 TUTKIMUKSEN TULOKSET

Kyselyyn vastasi lopulta 45 työntekijää ja 10 esimiestä alkuperäisestä 100 työntekijän ja 25 esimiehen otoksesta. Tulosten läpikäyntiä varten tulokset on jaoteltu samoihin kysymysten ryhmiin, miten ne kyselyssä esiintyivät.

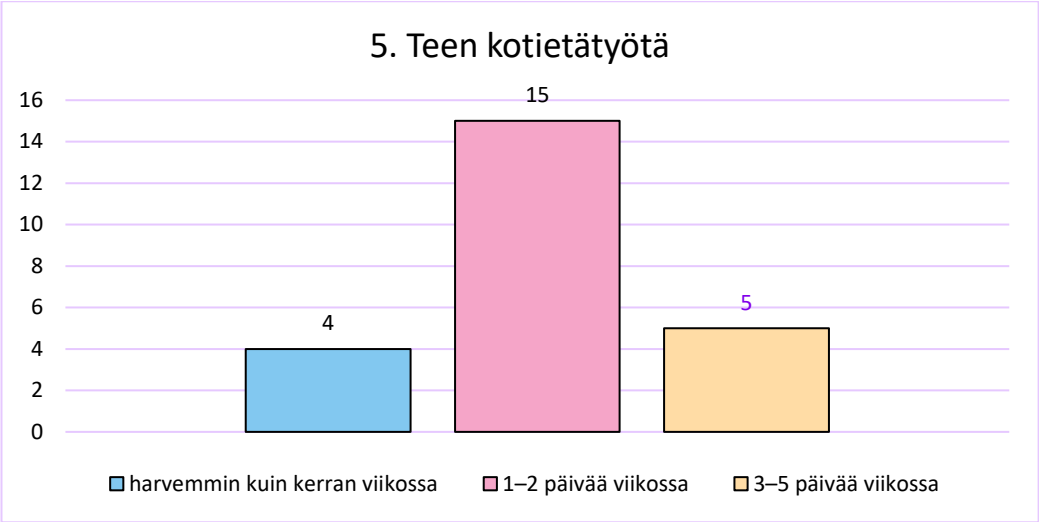
7.1 Kysymykset 1-5

Alkupään kysymyksillä kartoitettiin hieman taustatietoja vastaajasta. Kuten jo aiemmin todettiin, kyselyyn vastasi 45 työntekijää ja 10 esimiestä. Kyselyyn vastanneet jaoteltiin myös sen mukaan, kuinka paljon kokemusta heillä on työskentelystä organisaatiossa. Kyselyyn vastanneista 9 oli määräaikaisessa ja 44 vakituisessa työsuhteessa. Lisäksi kuviosta 2 nähdään vastaajien työkokemuksen jakauma työvuosien mukaan.



KUVIO 1. kysymyksen 3. "kauanko olet ollut tässä organisaatiossa töissä?**"** vastausjakauma

Osa kysymyksistä liittyivät kotietätyön riskeihin ja siksi oli tärkeää, että kyselyyn saatiin myös vastauksia sellaisilta henkilöiltä, jotka tekevät kotietätyötä. Vastaajista 25 ilmoitti tekevänsä kotietätyötä. Kotietätyötä tekeville esitettiin jatkokysymys, jossa kysyttiin, kuinka usein kyseinen henkilö tekee kotietätyötä.



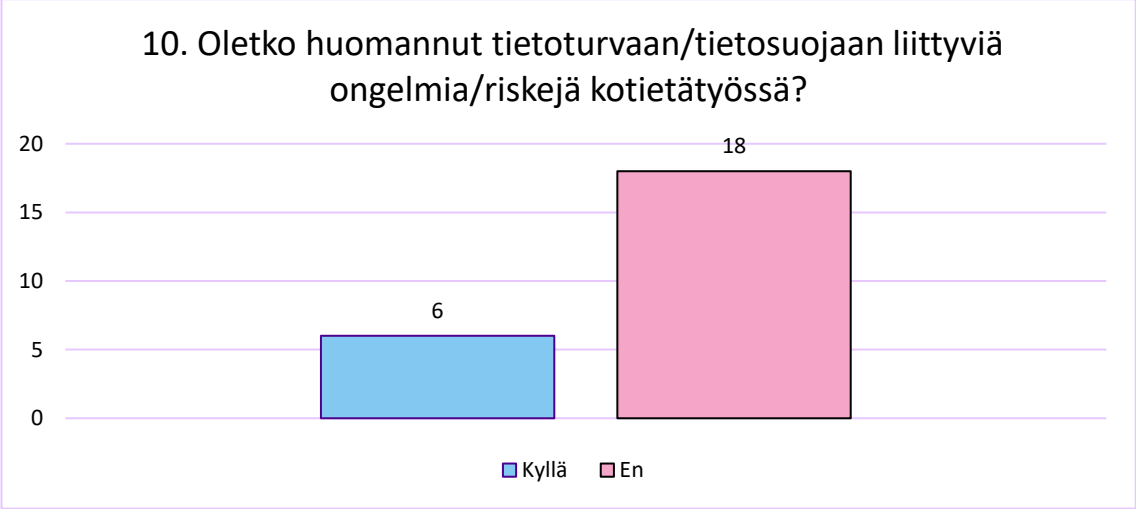
KUVIO 2. Kysymyksen 5 jatkokohdan ”teen kotietätyötä” vastausjakauma.

7.2 Kysymykset 6-10

Näillä kysymyksillä kartoitettiin hieman vastaajien yleistä tieto tasoa tietoturva- ja tietosuoja-asioissa kohdeorganisaatiossa. Lisäksi myös tutkitaan hieman eri tietoturvaan ja tietosuojaan liittyvien ohjeistusten riittävyyttä. Kuviosta 1 nähdään kysymysten 6-9 vastausjakaumat. Vastauksista nähdään, että melko iso osa vastanneista (23) oli huomannut jonkinlaisia tietoturvaan/tietosuojaan liittyviä ongelmia työssään. Mutta suurimman osan vastanneista mielestä organisaatiossa kuitenkin huolehditaan tarpeeksi tietoturvasta sekä tietosuojasta. Myös ohjeistus ja tietoturva- ja tietosuoja-asioiden perehdytys on ollut riittävää suurimmalle osalle vastanneista.

KUVIO 3. Kysymysten 6-9 vastausjakaumat

Tähän ryhmään kuului lisäksi vielä kysymys 10. Kysymys koski kotietätyötä, joten sen vastausjoukko oli pienempi, ja siksi esitetään sen vastausjakauma erikseen kuviossa 2.



KUVIO 4. kysymyksen 10. "Oletko huomannut tietoturvaan/tietosuojaan liittyviä ongelmia/riskejä kotietätyössä?" vastausjakauma

Kysymysten 6-11 vapaasti vastattavaan avoimeen kohtaan saatiin myös jonkin verran vastauksia, joista alla on muutamia esimerkkejä. Avoimista vastauksista nousivat esille avointen työtilojen mukanaan tuomat riskit ja se miten yhteisille tulostimille tulostettuja asiakkaiden henkilötietoja sisältäviä papereita unohdetaan noutaa. Lisäksi esille nousi se, miten tietoturva- ja tietosuoja-asioihin suhtaudutaan eri lailla nykyään kuin ennen.

- ”Perehdytyksessä painotettava enemmän asian vakavuutta ja oman työn vastuuta tietoturva- ja tietosuoja asioissa. ”

- ” Olen huomannut riskejä, mutta mielestäni pystynyt niitä hyvin välttämään. Kotietätyössä oma työhuoneeni on kaukana huoneista, joissa mahdollisesti muita on.

- ”Riskinä olen huomannut toimiston kopiokoneelle jääneitä asiakkaiden asiapapereita. Esim. siivooja tai huoltomies voi ne nähdä.”

- ” Kotietätyössä tietosuojariski kasvaa, mikäli ei ole erillistä työhuonetta.”

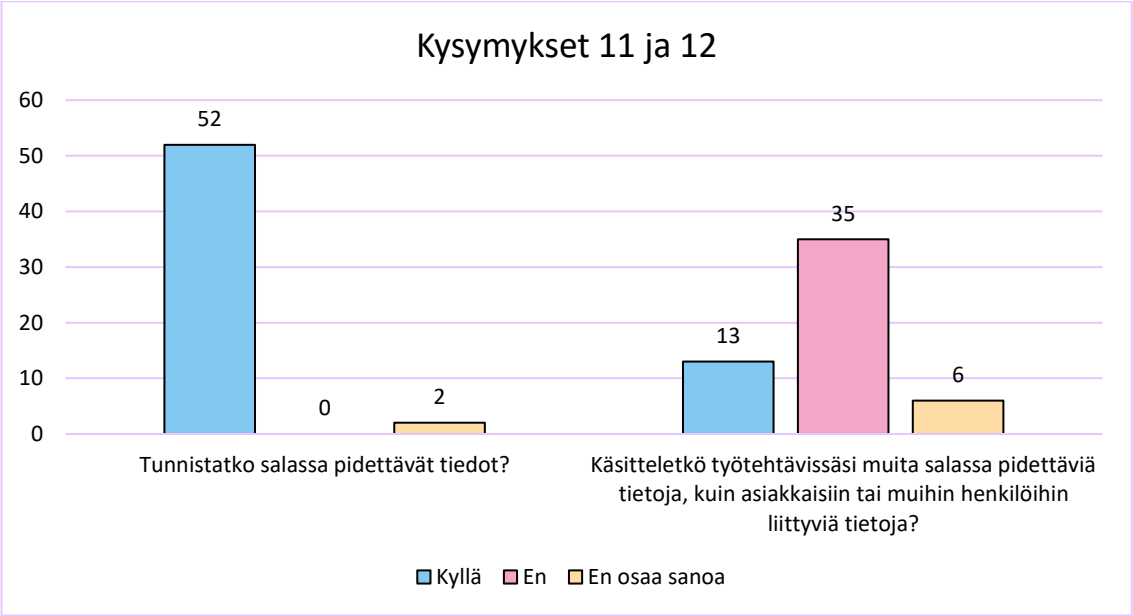
- ” aloittaessani näihin asioihin ei juurikaan kiinnitetty huomiota, tai huomattavasti vähemmän kuin nykyään. Riskit olivat huomattavasti pienemmät. Ja näin vanhempana, kun on joutunut myöhemmällä iällä opettelemaan, niin tietoturva-asioiden sisäistäminen ei ole ihan helppoa.”

- ”Avotiloissa kuulee, kun työkaverit puhuvat asiakkaiden asioista puhelimitse esim. asiakkaiden tai yhteistyökumppaneiden kanssa.”

- ” Ei varsinaisesti riskejä mutta olen ollut epävarma juuri nettiyhteyksistä onko varmasti luotettavia kotona yms. Mutta kyse on enemmänkin omasta tietämättömyydestä kun riskistä.”

7.3 Kysymykset 11-12

Kysymykset 11 ja 12 liittyivät salassa pidettäviin tietoihin ja kuviosta 3 nähdään näiden kysymysten vastausjakaumat. Tulosten mukaan lähes kaikki vastanneista tunnistavat salassa pidättävät tiedot. Suurin osa vastanneista ei käsittele työsään muita salassa pidettäviä tietoja, kuin asiakkaiden tai muiden henkilöiden henkilötietoja.



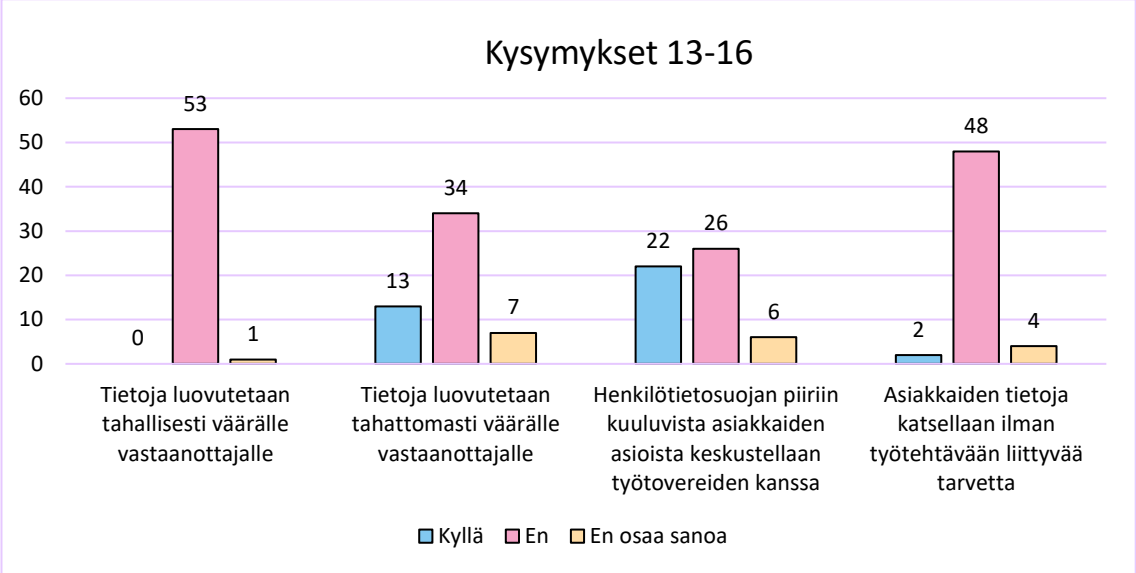
KUVIO 5. Kysymysten 11 ja 12 vastausjakaumat

Alla vielä yksi esimerkki kysymyksiä 11 ja 12 tarkentavan avoimeen kysymykseen tulleesta vastauksesta.

- ”Luulen tunnistavani salassa pidettävät tiedot. Toisaalta se, mitä tietoja voi muille viranomaisille välittää, saattaa olla joskus hieman epäselvää ja tarkistettava esim. esimieheltä.”

7.4 Kysymykset 13-16

Tässä kohtaa kyselyä siirryttiin kysymyksiin, joilla selvitettiin organisaation henkilöstön itse työssään kohtaamia tietoturva- ja tietosuojariskejä. Kysymykset 13-16 liittyvät kaikki jollain tavalla asiakkaiden henkilötietojen vaarantumiseen. Kuviosta 4 nähdään kysymysten 13-16 vastausjakaumat. Vastauksista huomataan, että kukaan vastaajista ei ollut havainnut tahallista tietojen luovutusta väärälle vastaanottajalle, mutta tahatonta puolestaan oli havainnut noin kolmasosa vastaajista. Lisäksi asiakkaiden tietojen puhumista työtovereiden kanssa oli havainnut jopa 22 vastaajaa.



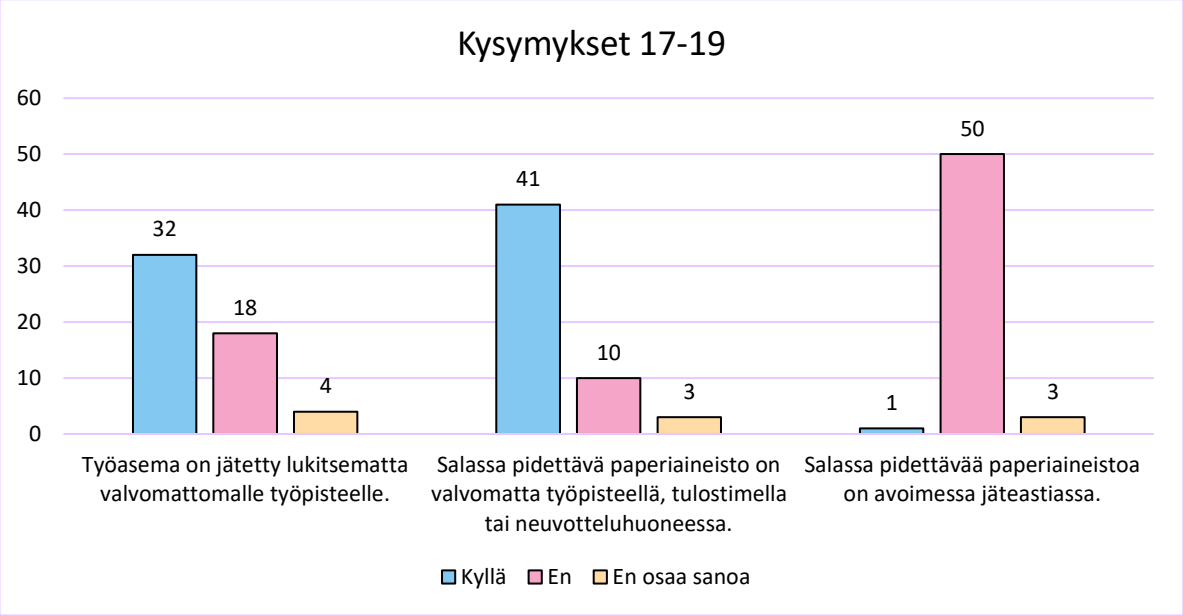
KUVIO 6. Kysymysten 13 - 16 vastausjakaumat

Avoimeen kohtaan saatiin myös esimerkiksi seuraavanlaisia vastauksia.

> -” Keskustelu liittyy työtehtäviin, kun kysytään neuvoa ja pyydetään toista henkilöä katsomaan tapausta.”
>
> -” huolehditaan mielestäni hienosti siitä, että asiakkaan tietoja ei luovuteta kenellekään ilman valtakirjaa/asiakkaan suostumusta.”
>
> -” Tietoja luovutetaan tahattomasti väärälle vastaanottajalle on minusta huolestuttavalla tasolla. Sen takia perehdytystä enemmän ja asian vakavuuden painottamista.”

7.5 kysymykset 17-19

Kysymykset 17-19 liittyvät vahvasti siihen, että jotakin mahdollisesti salaista tietoa, kuten esimerkiksi asiakkaiden henkilötietoja on näkyvillä. Kuviosta 5 nähdään kysymysten 17-19 vastausjakaumat. Vastauksista nähdään, että suurin osa vastaajista on huomannut työaseman, joka on jätetty lukitsematta valvomattomalle työpisteelle ja lisäksi, että salassa pidettävää paperiaineistoa on valvomatta työpisteellä, tulostimella tai neuvotteluhuoneessa.



KUVIO 7. Kysymysten 17-19 vastausjakaumat

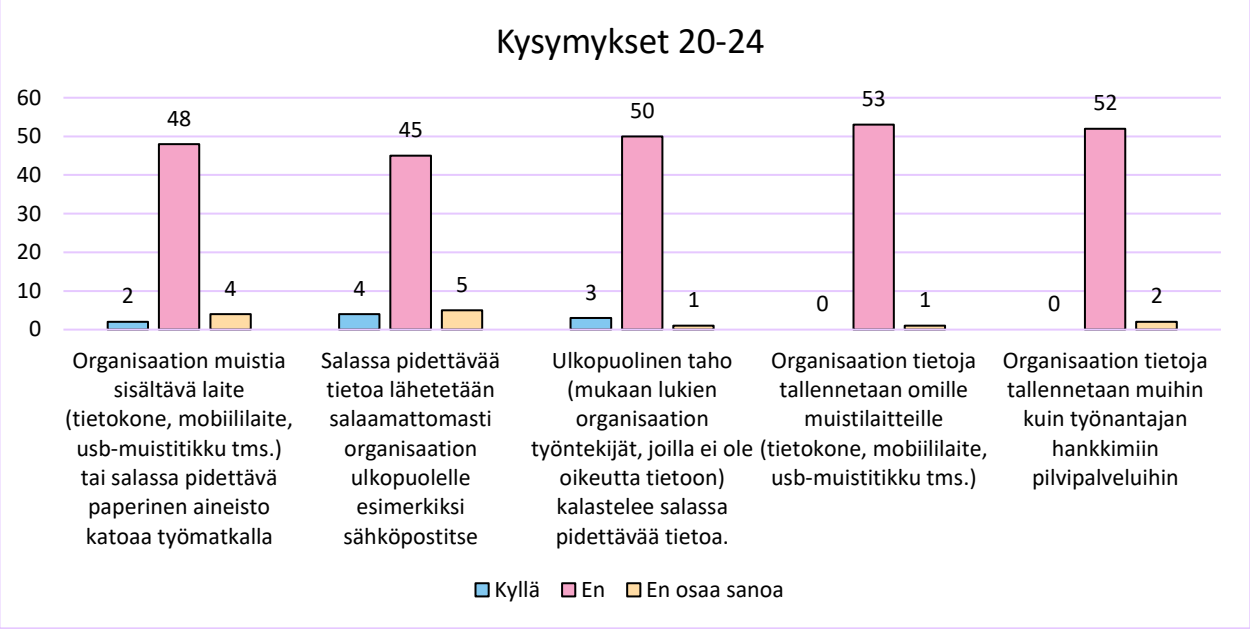
Avoimeen vastauskohtaan vastattiin seuraavanlaisesti. Niistä esille nousivat jo aiemmissa vastauksissa ilmenneet avotoimistojen mukanaan tuomat riskit, sekä työaseman lukitsematta jättäminen.

> -”Avokonttoreissa haasteen tekee juuri tämä, että helposti unohdetaan ettei haittaisi oman porukan keskuudessa, jos työasema ei ole lukittuna tai paperiaineistoa tulostimella. Itse uskon että aina parempi olla varovainen kuin liian luottavainen käsiteltävien aineistojen kanssa.”

> -”Itsekin syyllistyn joskus siihen, että työasema jää lukitsematta, jos nopeasti kipaisen hakemassa tulosteet. Tässä olisi itsellä parannettavaa. Tulostimella on aina toisinaan tulosteita. Nykyisin kyllä vähemmän kuin aikaisemmin”

7.6 kysymykset 20-24

Kysymykset 20-24 liittyvät vielä erilaisiin riskeihin, jota henkilöstö on työssään mahdollisesti kohdannut. Kuviosta 6 nähdään kysymysten 20-24 vastausjakaumat. Vastauksista huomataan, että kaikissa valtaosa vastaajista ei ole huomannut mitään kyseisitä riskeistä työssään.



KUVIO 8. Kysymysten 20 – 24 vastausjakaumat

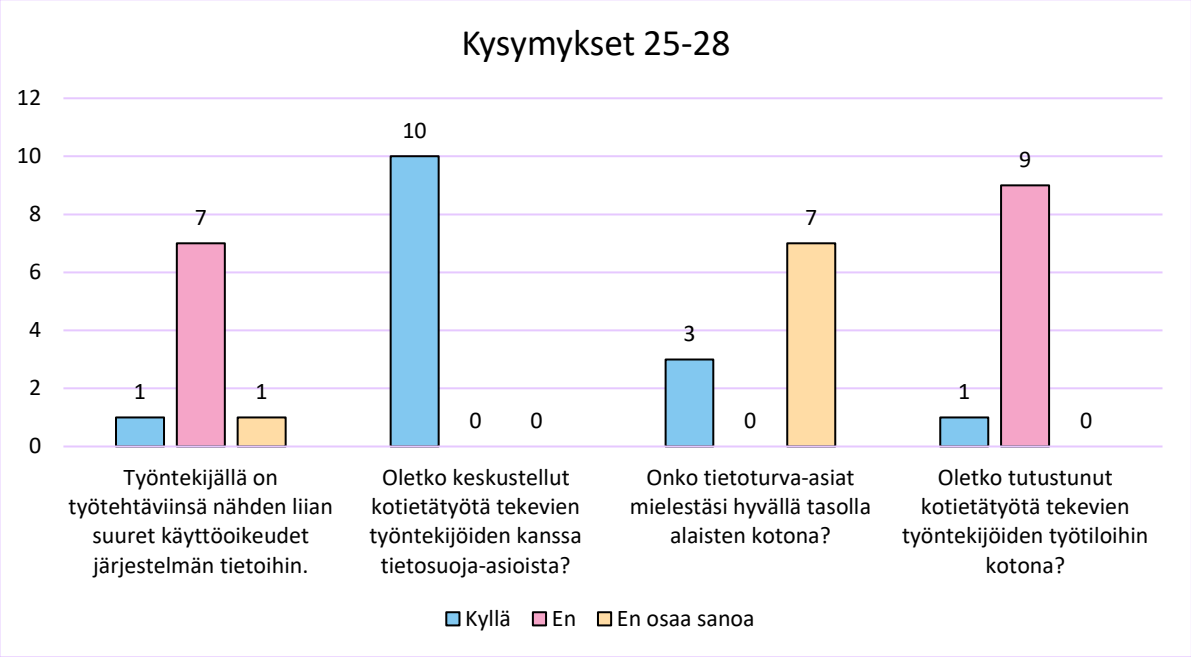
Alla on vielä esimerkki eräästä avoimesta vastauksesta.

> -” Käytän henkilökohtaisia laitteita erikseen enkä liitä niitä koskaan työkoneeseen.”

> -”Ulkopuolinen taho, kuten yhteistyökumppanit saattavat pyytää salassa pidettäviä tietoja. Sen takia on erittäin tärkeää, että on henkilöitä, joilla on osaamista mitä tietoja saa ja missäkin puitteissa luovuttaa ulkopuoliselle taholle ja aina tällaiset pyynnöt menisivät näiden ihmisten kautta, jotta tietosuoja rikkomuksilta vältyttäisiin.”

7.7 kysymykset 25-28

Kysymykset 25-28 vastasi pelkästään kyselyssä mukana olleet esimiehet. Kuvi-osta 7 nähdään kysymysten 25-28 vastausjakaumat.



KUVIO 9. Kysymysten 25-28 vastausjakaumat

”-Kotietätyötä tekevien työolosuhteita ei käydä tarkistamassa, joten niiden val-vonta on hankalaa. Kotietätyö myös lisääntyy jatkuvasti, joten tietosuoja siinä mielessä on riski.”

8 TULOSTEN YHTEENVETO

Useissa tapauksissa organisaation suurin tietoturvallisuutta uhkaava tekijä on sen työntekijät. Tämä tutkimus painottuikin selvittämään tarkemmin tietoturva- ja tietosuojauhkia ja niiden syitä. Valtaosa kyselyyn vastanneista tuntui suhtautuvan tietoturvaan ja tietosuojaan, sekä niiden tilaan kohdeorganisaatiossa melko positiivisesti. 81,5% vastaajista oli sitä mieltä, että kohdeorganisaatiossa huolehditaan tarpeeksi tietoturvasta ja tietosuojasta. Kohdeorganisaatiossa kiinnitettään nykyään selvästi enemmän huomiota tietoturva- ja tietosuoja-asioihin. Toki jonkinlaisia poikkeuksiakin löytyi, sillä 42,6% vastaajista ilmoitti havainneensa jonkinlaisia tietoturvaan tai tietosuojaan liittyviä ongelmia tai riskejä työssään. Isoimmaksi tietoturvaa ja tietosuojaa vaarantavaksi tekijäksi nousi yksinkertaisesti tahaton huolimattomuus ja ehkä joissakin tapauksissa välinpitämättömyys. Esimerkkeinä tästä tietokoneen lukitseminen ja työpisteen puhtaana pitäminen salassa pidettävää tietoa sisältävistä papereista on tärkeää tietoturvan ja tietosuojan kannalta.

8.1 Parannusehdotuksia tulosten perusteella

Mitään merkittäviä muutoksia kohdeorganisaation tietoturvaan on vaikea tehdä tämän kyselyn tulosten perusteella. Joitakin pieniä muutoksia voi toki tehdä. Isoimpana asiana voisi painottaa tietoturvan ja tiesuojan merkitystä henkilöstölle ja sitä, kuinka niistä huolehtiminen kuuluu kaikille. Asiakkaiden henkilötietoja käsitellessä tulee olla tarkkana. Niistä puhumista työtovereiden kanssa olisi hyvä tehdä harkiten varsinkin, jos paikalla on muita mahdollisia ulkopuolisia. Henkilötietoja sisältävien asiakirjojen kanssa on myös oltava tarkkana. Näitä asioita voisi tuoda enemmän esille perehdytyksessä uusille työntekijöille.

Vastausten perusteella joillekin pidempään organisaatiossa olleille tietoturva asioiden sisäistäminen voi olla hankalaa, koska tietoturvan merkitys on viime vuosina kasvanut, eikä ollut niin ajankohtaista heidän aloittaessaan työt. Kotietätyöhön liittyvät tietoturva-asia tuntuvat olevan kohdallaan. Kaikki kyselyyn vastanneet esimiehet ovat puhuneet tietosuoja-asioista kotietätyötä tekevien kanssa.

Alaistensa kotietätyötiloihin oli tutustunut vain 1 vastanneista esimiehistä, mutta ei tälle kyllä varmaan ole tarvettakaan. Kotietätyötilojen tarkistaminen tuskin parantaisi kotietätyön tietoturvaa ja tietosuojaa, jos samat asiat voidaan hoitaa keskustelemalla asiasta. Tarvittaessa esimiehet voivat käydä tarkistamassa työntekijöidensä kotietätyötilat Avoimista vastauksista ilmeni myös joitakin yksittäisiä asioita, mutta niiden perustella on vaikea tehdä mitään johtopäätöksiä, koska vastaajia oli sen verran vähän.

8.2 Pohdinta

Tutkimuksen tarkoituksena oli selvittää sitä, minkälaisia tietoturvaan ja tietosuojaan liittyviä riskejä, tai ongelmia kohdeorganisaatiossa kohdataan. Näihin pyrittiin myös selvittämään syitä. Joitakin aiemmin esitettyjä ongelmia nousikin esille kyselyn tulosten perusteella. Lisäksi vastauksista ilmeni myös muitakin asioita, mutta näiden perusteella on vaikeaa tehdä isoja johtopäätöksiä, sillä sen saattoi tuoda esille vain yksittäinen vastaaja. Tämän perusteella ei voi tietää sitä, onko kyseinen asia isokin ongelma kohdeorganisaatiossa vai onko se vain yksittäisen vastaajan mielipide. Jos koetaan tarpeelliseksi, niin kyseylä voidaan tulevaisuudessa toteuttaa uudestaan laajemmalla vastaajajoukolla ja hieman muokaten kysymyksiä selvittämään tarkemmin tietoturva- ja tietosuoja ongelmien syitä.

LÄHTEET

Kyberturvallisuuskeskus. 2019 Office 365 -sähköpostin tietojenkalastelu ja tietomurrot erittäin yleisiä – havaitse, suojaudu, tiedota!. Luettu 27.2.2019 https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota

Organisaation sisäinen ohjeistus. Tietoturvan ja tietosuojan lainsäädännön vaatimukset. Luettu 7.4.2019

Organisaation sisäinen ohjeistus. Tietoturva- ja tietosuojapolitiikka. Luettu 28.3.2019

Organisaation sisäinen ohjeistus. Tietoturvapoikkeamien tunnistaminen. Luettu 9.4.2019

Tietojesiturvaksi. Tietoturvan osa-alueet. Luettu 12.2.2019 https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvan-osa-alueet

Tietojesiturvaksi. Tietoturvallisuuden peruskäsitteitä. Luettu 24.1.2019 https://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoturvallisuuden-peruskasitteita

Tietosuojavaltuutetun toimisto. gdpr. Luettu 24.1.2019 https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. Tietosuoja. Luettu 24.1.2019 https://tietosuoja.fi/tietosuoja

Tietosuojavaltuutetun toimisto. Tietoturvaloukkaukset. Luettu 9.4.2019 https://tietosuoja.fi/tietoturvaloukkaukset

Viestintävirasto. Kyberturvallisuuskeskus. 2015. Laita etätyön tietoturva kuntoon. Luettu 3.4.2019 https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/10/ttn201510071118.html

Viestintävirasto. Kyberturvallisuuskeskus. 2016. Palvelunestohyökkäykset ovat internetin arkipäivää. Luettu 5.2.2019 https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/04/ttn201604291231.html

Viestintävirasto. Kyberturvallisuus. 2018. Organisaatioiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017. Luettu 5.2.2019. https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801161310.html

Yksityisyydensuoja. Oikeudellisuuden tarkistaminen. Luettu 27.4.2019 https://www.yksityisyydensuoja.fi/oikeellisuuden-tarkistaminen

Yksityisyydensuoja. Salasanat. Luettu 2.4.2019 https://www.yksityisyydensuoja.fi/salasanat

Yksityisyydensuoja. Tietoturva. Luettu. 24.1.2019 https://www.yksityisyydensuoja.fi/tietoturva

Yksityisyydensuoja. Virusturva ja palomuuri. Luettu 3.4.2019. https://www.yksityisyydensuoja.fi/virusturva-ja-palomuuri

LIITTEET

Liite 1. Kyselylomake

1(3)

Taustatiedot (kaikille)

1.Oletko

-työntekijä

-esimies

2. Mihin osaan organisaatiota kuulut?

3. Kauanko olet ollut tässä organisaatiossa töissä?

- alle vuoden
- 1–5 vuotta
- yli 5 vuotta

4. Onko työsuhteesi

- Määräaikainen?
- Vakituinen?

5. Teetkö kotietätyötä

- Kyllä
- En

Kyllä-vastanneille

Teen kotietätyötä

harvemmin kuin kerran viikossa

1–2 päivää viikossa

3–5 päivää viikossa

Kaikille

Kyllä En En osaa sanoa

6. Oletko huomannut tietoturvaan/tietosuojaan liittyviä ongelmia/riskejä työssäsi?

7. Huolehditaanko tässä organisaatiossa mielestäsi tarpeeksi tietoturvasta ja -suojasta?

8. Onko henkilötietojen käsittelyä koskeva ohjeistus riittävä?

9. Saitko riittävästi tietoa tietoturva- ja tietosuoja-asioista aloittaessasi työn tässä organisaatiossa?

10. Oletko huomannut tietoturvaan/tietosuojaan liittyviä ongelmia/riskejä kotietätyössä?

Kyllä en tee kotietätöitä

Tähän voit halutessasi tarkentaa viiden edeltävän kysymyksen vastauksia (6-10)

Kaikille Kylllä En En osaa sanoa

11. Tunnistatko salassa pidettävät tiedot?

12. Käsitteletkö työtehtävissäsi muita salassa pidettäviä tietoja, kuin asiakkaisiin tai muihin henkilöihin liittyviä tietoja?

Tähän voit halutessasi tarkentaa kahden edeltävän kysymyksen vastauksia (11-12)

Kaikille

Oletko kohdannut seuraavia tilanteita työyhteisössäsi? Kyllä En En osaa sanoa

13. Tietoja luovutetaan tahallisesti väärälle vastaanottajalle

14. Tietoja luovutetaan tahattomasti väärälle vastaanottajalle

15. Henkilötietosuojan piiriin kuuluvista asiakkaiden asioista keskustellaan työtovereiden kanssa

16. Asiakkaiden tietoja katsellaan ilman työtehtävään liittyvää tarvetta

Tähän voit halutessasi tarkentaa neljän edellisen kysymyksen vastauksia (13-16)

17. Työasema on jätetty lukitsematta valvomattomalle työpisteelle.

18. Salassa pidettävä paperiaineisto on valvomatta työpisteellä, tulostimella tai neuvotteluhuoneessa.

19. Salassa pidettävää paperiaineistoa on avoimessa jäteastiassa.

Tähän voit halutessasi tarkentaa kolmen edellisen kysymyksen vastauksia (17-19)

20. Organisaation muistia sisältävä laite (tietokone, mobiililaite, usb-muistitikku tms.) tai salassa pidettävä paperinen aineisto katoaa työmatkalla
21. Salassa pidettävää tietoa lähetetään salaamattomasti organisaation ulkopuolelle esimerkiksi sähköpostitse
22. Ulkopuolinen taho (mukaan lukien organisaation työntekijät, joilla ei ole oikeutta tietoon) kalastelee salassa pidettävää tietoa.
23. Organisaation tietoja tallennetaan omille muistilaitteille (tietokone, mobiililaite, usb-muistitikku tms.)
24. Organisaation tietoja tallennetaan muihin kuin työnantajan hankkimiin pilvipalveluihin

Tähän voit halutessasi tarkentaa viiden edellisen kysymyksen vastauksia (20-24)

Vain esimiehille

Kyllä En

25. Työntekijällä on työtehtäviinsä nähden liian suuret käyttöoikeudet järjestelmän tietoihin.
26. Oletko keskustellut kotietätyötä tekevien työntekijöiden kanssa tietosuoja-asioista?
27. Onko tietoturva-asiat mielestäsi hyvällä tasolla alaisten kotona?
28. Oletko tutustunut kotietätyötä tekevien työntekijöiden työtiloihin kotona?

Tähän voit halutessasi tarkentaa neljän edellisen kysymyksen vastauksia (25-28)